# **General Comments**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **General Comments** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Introduction**  Australia is pleased to provide this response to the question posed by the CWG-Internet in CL-13/68. That letter asked Member States to provide their positions on what actions have been undertaken by governments in relation to the international internet-related public policy issues identified in Annex 1 to Resolution 1305 (Council 2009). Accordingly, this response sets out the actions that the Australian Government is taking on a number of these identified issues. Where appropriate the Australian Government position on the issue more generally is also set out. Australia consulted widely both within and outside the Australian Government in the preparation of this response.  Australian internet related policy seeks to foster and reward innovation, drive productivity and empower individuals, while maintaining trust and confidence in Australia’s digital economy and the online environment.  A common theme throughout this response is that while government plays an important role in responding to the range of issues identified - to provide the policy and legal frameworks, essential infrastructure and critical services - it cannot work alone. Effective responses require partnerships and shared responsibility through the active engagement and participation of the private sector, non-government bodies and citizens or in enabling them to respond to these issues within their own areas of expertise. Australia believes that developing a network of multi-stakeholder partnerships is central in ensuring a whole‑of‑nation approach to the development of internet policy. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | **1) What actions have been undertaken or to be undertaken by governments in relations to each of the international Internet-related public policy issues identified in Annex 1 to Resolution 1305 (adopted by Council 2009 at the seventh Plenary Meeting)?”**  The Bulgarian government has undertaken and implemented a policy which resulted in unprecedented (and almost not followed in other countries) growth of Internet penetration, affordability, and quality of the service. The relevant information is contained in Information document № 7, [presented](http://www.itu.int/md/S10-PP-INF-0007/en) by the MTITC to the ITU Plenipotentiary Conference in 2010 (Guadalajara, Mexico).  Bulgaria has waived any licensing or registration regime for the Internet service providers since 1999. Under the Law for Electronic Communications the Government neither exercises control nor deals with the Internet names and addresses.  ISOC-Bulgaria, having been part of the last 14 years of negotiations, and sometimes legal arguments between all interested parties in the country, believes that such a policy has proven to be very successful for the general development of the Internet sector in the country.  **2) What is the ITU’s role to support governments in their activities around Internet-related public policy issues?**  Internet-related public policy issues are within the sovereignty of each country which are also ITU member states. Therefore, it’s up to the member states to decide to what extent to involve various internet-related organizations and co-operate with them.  **3) Which international organizations/forums are the most adequate to receive support from the governments on the Internet-related public policy issues?**  The most adequate organizations have been recognized by the ITU in the Internet resolutions from PP-10, and they are IETF, ICANN, ISOC, W3C, which provide their public forums several times a year. Also, the Internet Governance Forum should receive a more substantial support from governments. |
|  | Canada [(INF/30)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0030/en) | Canada is pleased to submit this contribution to inform the discussion of the Council Working Group on Internet-related public policy issues.  Canada supports an open, multistakeholder approach to Internet governance. The Internet has grown, and continues to thrive, under this governance model. lt is an arrangement that has been successful in promoting global competition, innovation, social development and economic growth.  Existing arrangements are effective because they enable inclusive participation of stakeholders from across the global Internet community, including governments, to collectively develop bottom-up policies and to make decisions based on consensus.  At the national level, governments play an important role with respect to the development of national Internet-related public policy and enforcement frameworks (e.g. rural and remote broadband access, competitive marketplace frameworks, adoption/use, intellectual property, etc.)  At the international level, governments are one of many stakeholders, among a large community of global Internet users, participating in the decision-making process. This includes a broad representation of the technical internet community, civil society, academia and businesses. While some lead on particular issues, all groups have the opportunity to contribute their unique perspectives and strengths to decision-making. Within the technical community, governments have an appropriate and effective venue for advancing their public policy views and shanng their concerns.  This open and multistakeholder structure of decision-making is effective because it is robust and flexible. Arising issues can be dealt with quickly, and with input from the entire community This process is ideally suited and complementary to the rapid pace of innovation and growth of the Internet.  In conclusion, inclusive multistakeholder participation in decision-making processes ensures the continued stability, security and interoperability of the Internet. This approach acknowledges the importance of collaboration from the entire community of global Internet users, including governments. lt is essential for the sound development of the Internet as a tool that all world citizens have equal access to. |
|  | Czech Republic [(INF/8)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0008/en) | Public policy issues pertaining to the Internet and identified in Annex 1 to Resolution 1305 belong among many ones that are observed by the Czech Republic.  Relevant legal standards are being issued in accordance to valid EU legislation.  For all aspects (internationalized domain names, security, capacity building, children protection etc.) there are relevant departments and responsible parties. Not only in the government (i.e. ministries) but also at specialized agencies that cooperate with the government.  There are many other stakeholders like public and private bodies that are involved in these matters and cooperate among themselves and with the state administration as well.  There are also non profit organizations that actively develop their own projects and cooperate with similar international organizations. Such projects are focused on the promotion of safer use of the Internet, education of children, parents, teachers etc. They involve lectures, educative videos, books, publicity campaigns, TV programs, PC and mobile applications for consumers etc. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | Please note, that Denmark supports the opening of the Council Working Group on Internet-related public policy issues to participation from all relevant stakeholders. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **Introduction**  The Internet has revolutionized the world around us by changing the political, social, economic and cultural landscape of our societies as an omnipotent and ubiquitous phenomenon. Considering the fact that India has a population of over 17% of the world, the Indian government, therefore, should play a pivotal role in global Internet cooperation; in formulating frameworks for such cooperation and building a roadmap for future Internet governance challenges.  World Summit of Information Society (WSIS) has extensively dealt with its various aspects Internet Governance and has defined and recognized the roles of various stakeholders including the Governments in formulating International Public Policy and overall governance of Internet and management of its critical resources. The role of the Government in formulating Internet related public policies, in the context of current global issue of Internet governance can better be understood by asking the following relevant questions:   1. **What should be the scope or terms of references of Internet Governance be?** 2. **Who are its various stakeholders/ performer/ actors for different levels of work in the multilayered and multi-player scenario of the Internet ecosystem?** 3. **How are the various stakeholders’ roles defined and how can their functions be coordinated and harmonized to dovetail their mutual roles towards a common goal and objectives?** 4. **Who would formulate the high level principles to enable the Stakeholders/ actors/ performers to perform their roles in a coordinated and harmonized way towards a common cause of Internet Governance?** 5. **Finally which should be the Authority at the global level which will formulate the high level public policies relating to Internet?**   Today, Internet is ubiquitous and plays a critical role in socio-economic development, as a medium of learning and service provisioning involving all types of stakeholders namely the Government, Private Sector, Civil Society, Individuals, International bodies and Inter-Governmental Organizations.  Hence, it is essential to secure the Internet System in general and to protect the integrity of communication, data and information content in particular. It is also important to address the threats arising out of the misuse of the Internet. In this regard, the Government and the community of governments besides other stakeholders have a role to play in their sphere of activities.  However, the functioning of the various stakeholders and the rules/principles/ guiding norms being adopted or to be adopted by the stakeholders while working for/ contributing to the development and shaping of the Internet eco-system as a whole is a complex and contentious exercise in which it really becomes difficult to visualize and precisely determine the roles and scope of various stakeholders/ actors.  Fortunately, a lot of work has been done in this direction. In 2005, the World Summit for Information Society after long and detailed deliberations adopted the Tunis Agenda which covered the various aspects of Internet, including definition of Internet Governance **[Para 34]** and also identified the roles of various stakeholders **[Para 35]** such as that of the Government, Private sector, Civil society, Intergovernmental organization and International organizations in shaping and developing the entire Internet System.  The governance of Internet as well as the governance on Internet (users) involves a holistic involvement of all stakeholders/ actors and India believes that the Government has certainly a prime mover role to play in this regard. This is especially true in many developing and least developed countries where the necessary institutions may not be sufficiently evolved or perhaps not even exist. This paper sets out the India’s view, arguing that the issue should be considered in a broad context. The different roles of the Indian government are to empower Internet users, ensure a fair and consistent domestic legal framework, and foster a robust global Internet infrastructure. Governments need to be active players in the Internet governance process with other stakeholders and build partnerships in order to achieve public policy goals and to secure the economic and social benefits of its citizens through the Internet as envisaged in Para 29,35, 61,68 and 69 of the Tunis Agenda. Government should be represented in decision-making forums but they would undertake consultations at their respective national levels with all stakeholders including private industry, civil society, academia and the technical community while formulating their positions.  -----  **Conclusions**  The success of the Internet can be attributed to its openness. As such, Indian government has a responsibility to maintain a secure, open and free character of the global Internet. The Indian government plays a central and crucial role in providing open access to the Internet, guaranteeing internet freedom, and securing the rule of law online. This responsibility exists at the national level, but given the borderless, global nature of the Internet, the Internet governance is also very much a global issue. It is both a domestic and a foreign policy subject. Indian government has an obligation to ensure its strategic security in the cyber domain. It also has an important role in furthering internet freedom, along with civil society, the private sector and academia. We feel that global Internet Governance and international management of internet should be multilateral, transparent, democratic and representative with full involvement of governments and other stakeholders. The institutions that regulate and administer the Internet need to be internationalized. In this regard it can be stated that governments should engage with all the stakeholders to work in a synergetic manner to achieve the objectives of a robust, secure, capable Internet which can help in the overall growth of the economy, knowledge and convenience of mankind at global levels.  Policy framework on the Internet governance at the international level must involve all the governments of various nations through mutual consultation and negotiation. In this regard, governments also need to involve all their stakeholders in their consultation processes. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Introduction:**  The Internet has developed through participation of multi-stakeholders. Therefore, for further development of the Internet, the government of Japan believes that the multi-stakeholder approach, including not only the Member States of ITU but also participation from private sector, civil society, technical and academic communities, and other intergovernmental and international organizations, is the best way to consider the international Internet-related public policy issues.  In addition, free flow of information is indispensable so that all users can enjoy the maximum benefits of the Internet, and the Internet can continue to contribute to social and economic development. Therefore, Japan considers that free flow of information should be ensured to address international Internet-related public policy issues.  To deal with the issues on the Internet, the government of Japan thinks that observing the following points is important:   * To respect voluntary actions made by each stakeholder, such as establishing voluntary guidelines and promoting collaboration among businesses * To establish frameworks to promote each stakeholder’s voluntary actions under the cooperation of government and the private sector etc.   To advance those measures, the following principles should be observed:   * No excessive intervention by governments; * To ensure free flow of information; and * Not to lead to regulations on contents and infringement of privacy   One of the outstanding characteristics of the Internet is its 'borderlessness', which gives extraordinary ability to the Internet. We support the open and bottom-up multi-stakeholder model so that the Internet continues to evolve and equally connects every corner of the world.  If intergovernmental organizations and/or national governments have “too much” influence to the public policy and technical development by means of international treaties and/or national laws/regulations, the speed of growth and development of the Internet would be seriously ruined. Governments need to avoid such kind of situation, and encourage to support private sector initiatives.  Based on that, governments should continuously support voluntary actions by multi-stakeholders including the private sector.  For example, governments could share best practices on examples made by governments to support each stakeholder’s voluntary actions.  The government of Japan is pleased to have the opportunity to respond to the CWG Internet Questionnaire. We support a multi-stakeholder approach, so we made our input following stakeholders consultation around in Japan. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | The independent national institution regulating the communications sector in **Lithuania** is the Communications Regulatory Authority of the Republic of Lithuania (RRT). One of the main purposes of RRT is promotion of competition in electronic communications and postal sectors. RRT implements the national policies and strategies established by the Government of Lithuania in the field of electronic communications. The policy development, including internet-related public policy, is the priority of the Government. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | ***Methodology applied by Moroccan Regulatory agency to measure THE QUALITY OF mobile SERVICE TO REQUEST TO THE WORKS OF "Specialized Group in identifying questions of public policy related to the Internet" CWG-Internet***  In accordance with the actual regulation, the National Telecommunication Regulatory Agency (ANRT) is in charge of monitoring and supervising the quality of telecommunication services (QOS). To achieve this task, ANRT undertakes QOS measurement campaigns through national territory in order to test and evaluate the quality of service received by end users.  Thus, ANRT conducts measurement campaigns following a defined set of parametres . These parameters are intended to check the accessibility of the service, its continuity, its availability and its reliability. They concern both voice (failure rate, cutoff rate, success rate ...) and data transmission (reception rate, transmission rate, error rate data ...) and aim to ensure the level of QoS provided to customers.  Each campaign is conducted on the basis of a significant (number of tests, geographic zones, services, timing ...) in order to ensure the representativeness of measurements and relevance of results. Measurements are performed in intuitive and random way, according to a protocol of measures adopted by ANRT in conjunction with the mobile service suppliers (operators).  Following the campaigns carried out, ANRT transmit the results of measuring tests to operators. In case that the observed QOS is degraded, the mobile service supplier is requested about parameters of quality of its service, and asked to take necessary adjustment actions to improve  its service quality.  Rigorous flow-up is undertaken by the technical services of ANRT to check the implementation of adjustment actions through the realization of measurement campaigns on the ground in order to assess the efficiency of these actions.  In terms of mobile Internet, ANRT assess the quality of service of UMTS/HSDPA networks of both Itissalat Al-Maghrib and Medi Telecom operators and CDMA2000/EVDO network of WANA CORPORATE operator. This assessment is set out to learn about the mobile Internet accessibility, the connection delay, the connection rate and throughput for transmission and reception. These indicators are:   * The average downlink throughput; * The maximum downlink throughput; * The average uplink throughput; * The maximum uplink throughput;   The measured indicators are carried out by using smartphones and computers (PC) covering mobile internet (data 3G) of three operators Itissalat Al-Maghrib (IAM), Medi Telecom (MdT) and Wana Corporate ( and performed on a sample of cities, airports and tourist and offshore areas.  Results of these campaigns are published on the website of the ANRT. Each one of the concerned operators is entered for the implementation of necessary adjustments actions to solve the abnormalities observed in its 3G network. |
|  | Norway [(INF/35)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0035/en) | When it comes to addressing international Internet public policy issues we would like to emphasize that Norway supports the model of multistakeholder cooperation where all stakeholders can participate and address the various issues. Norway believes that this way of addressing Internet Governance is essential to ensure that Internet continues to be a major factor to economic growth, social and cultural development and keeping the Internet secure and open. We acknowledge the role of all stakeholders, as referred in WSIS Tunis Agenda paragraphs 29 and 35. We also believe that multistakeholder processes have shown to provide the flexibility and global scalability required to address Internet Policy challenges as stated in the OECD’s Internet Policy-making Principles.  We would like to address some of the topics listed in the Council Resolution 1305 Annex 1. |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | Poland wishes to thank the CWG Internet Chairman for opening this valuable public consultation on the Res. 1305. In response to that Poland reached out for the national sector and compiled this contribution with a view to share some of the finest examples of the Res. 1305 Annex 1 output.  We received a number of multistakeholder comments on that call, which all show that the openness of the Internet policy-making forums has intensively been looked for and that there are a lot of inputs that can enrich the discussion on the way forward for the Internet.  **NOTE:** Some of the contributions go beyond the Res. 1305 timespan i.e. before 2009 when the resolution and the Annex 1 Public Policy issues were adopted. Nevertheless a decision was taken not to crop them out so that the line of continuous commitment from some of the contributors was clearly seen.  **Contributors:** Ministry of Administration and Digitization (MAC), Office of Electronic Communications (UKE), Ministry of the Interior, Internal Security Agency (ABW), Research and Academy Computer Network (NASK), Poznań Supercomputing and Networking Centre (PCSS), Warsaw Technical University, Polish Chamber for Electronic Communication (PIKE). |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | Indeed, MICT considers that Internet’s success and major role in the socio-economic developments worldwide is due to its multi-stakeholders nature and cooperative approach. Governments, service providers, businesses, researches and academia have contributed, all in their respective roles and responsibilities, to this achievement.  ITU has contributed also significantly to Internet growth through the development of global telecommunications standards. It resulted in the impressive list of accomplishments listed in ITU’s Council Resolution 1305, Annex 1. To that regards, MiCT welcomes ITU focus on the international perspective of Internet related public policy issues, as opposed to technical policies implementation and/or day to day operation of the Internet.  -------  More globally, MICT supports ITU activities in all these areas at regional and international level. In that perspective, ITU should be the global platform to debate, discuss and agree on approaches and mechanisms related to Internet public policies which can foster great progress at a regional and international level. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Introduction**  Since 2000, the Government of Rwanda (GoR) embarked on a 20 year journey through her Vision 2020 aiming at transforming Rwanda into a middle-income country from her agrarian economy to an information-rich, knowledge-based economy by 2020. The GoR strongly believes that Information and Communication Technologies (ICTs) can enable Rwanda leap-frog the key stages of industrialization. As such, GoR has integrated ICTs, through the National Information and Communication Infrastructure (NICI) process, as a key driver for socio-economic development to fast track Rwanda’s economic transformation, and consistently strives to align the country’s development agenda to global trends in order to be competitive. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**   1. Name or create an entity within the UN system to enable governments, on an equal footing, to carry out their roles and responsibilities in international public policy issues pertaining to the Internet, but not in the day-to-day technical and operational matters that do not impact on international public policy issues. 2. Develop clear mechanisms and processes within the entity to address how issues are introduced, studied, agreed, disseminated, adopted and implemented. 3. Participate in mechanisms for development of international public policy, and ensure that national public policy is consistent with international policy. |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | **Preface**  Sudan has identified the need to revise the multi-stakeholders bottom-up model to provide a fair deployment usage of Internet service and resources with no single control over the global network services and traffic.  In developing countries the role of governments is the key assuring national welfare. This paper arguing that the issue should be considered in a formal organization like ITU. ITU as UN agency is will recognizance and trusted globally to provide strategic management model for the global networks.  **Background**  Internet is without any doubt is the fastest and most effective means of communication making it possible to reach a great number of people in the world. This fact makes the issues related to Internet a global issue and should be undertake under this capacity. The current management model which called the multi-stakeholder model was failed to prove it’s transparently because few organizations with significant power control the overall process. A part of the Internet community can be punished by limiting their rights to global accessibility to Internet just because their administration has a different political view. This is not acceptable according to the human rights principles.  Tunis Agenda (Art. 35, 69) mentioned very clear the role of governments in the multi-stakeholder process of Internet governance: they have rights and responsibilities, on an equal footing, for international public policy related to the Internet, though not in day-to-day technical and operational matters.  In the national level, in Sudan, we endeavor to maintain our community benefit from Internet under the undusted sanction imposed by the US. And we are collaborating with ITU and other fair agencies to undertake action to develop our ICT sector.  ­------  **Conclusion**  With the current management model governments have been unable to undertake their role even this structure affect the country sovereignty. This is primarily due to the fact that the mechanism needed to enable this role, defined in the Tunis Agenda as “enhanced cooperation”, and has never been realized. This has been infertile by those who currently control the Internet or the organization in [favor](javascript:void(0)) of the controller. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | It is our view that stakeholders in business, civil society, the Internet technical communities, governments and academic institutions make significant contributions to the development of the internet.  The global Internet governance should continue to develop. The current model with multistakeholder cooperation in various forums for the governance and management of critical Internet resources, the domain name system and IP-addresses, should be preserved and strengthened. Sweden is of the opinion that increased government influence at the expense of the influence of other stakeholders would be a disincentive for the innovation and entrepreneurship that is the driving force for development of the Internet. Increased government influence would lead to increased politicization of technical decisions and bureaucratising established decision-making.  We have seen through the years that the multistakeholder model of governing the internet helps to transform the economy globally, regionally and locally and make it stronger. It also promotes the ability of people to exercise their freedoms and express their democratic aspirations.  Our support for the multistakeholder model is rooted in our firm belief that this is the only model that will continue to generate technological developments and solutions for the future and preserving the Internet's open nature.  Sweden sees a need for a continuous debate among all stakeholders on a range of public policy issues, including   * Safeguarding the open character of the internet, * Promoting net neutrality and limitations of intermediary responsibility, * Securing and promoting human rights, in particular freedom of expression online, * Sharing policies and best practices on improving accessibility and affordability in ICT’s, network resilience and reliability, * Protection of privacy and the free flow of information, * Promoting an open and enabling online business and trading environment * Ensuring that the role of the Internet and ICTs is fully recognized and used to reduce poverty, empower the poor and generate sustainable development. |
|  | Ukraine [(INF/15)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0015/en) | In reply to the ITU letter of 22 November 2013 No CL-13/168, the Administration of Communication of Ukraine informs that the following measures are taken on the Internet-related international public policy issues stipulated in the Annex 1 of Council Resolution 1305:   * Ukraine registered its own Cyrillic zone and received national “.УКР” Cyrillic domain in the Internet. Since August 2013 Ukrainian public authorities began to register their own information resources in the “.УКР” domain. Registration of domain names for owners of trademarks, trade names and other intellectual property rights will be the next step; * technical information protection system operates in Ukraine to provide information protection and includes a set of organizational structures united by goals and objectives for information protection engineering activities, as well as relevant legal, material and technical basis. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | The UK government supports a multi-stakeholder approach to Internet governance issues both in a national and international context. The UK government is a firm believer that the ITU Council Working Group on Internet Public Policy Issues should be open up to all relevant stakeholders who wish to participate, where we believe it would bring greater depth in discussions and output of the group moving forward.  For this reason, the UK looks forward to the open consultation which the Council Working Group has agreed will take place immediately after this consultation. By allowing all stakeholders to participate, we believe that the second conversation will provide a much richer and more informative set of responses from a range of perspectives. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | The Internet is an essential tool for innovation, economic growth, and social discourse. Given the diversity and complexity of Internet policy issues, it is counterproductive to narrowly prescribe roles and responsibilities to distinct stakeholders, including governments. We believe a flexible approach that leverages existing multistakeholder institutions and other cooperative venues would lead to a better outcome. This approach will ensure that all considerations are taken into account, encourage broader participation, and facilitate more creative problem solving. All stakeholders have an interest in realizing the goal of an open, interoperable, secure and reliable cyberspace by developing international Internet-related policy in a collaborative manner.  We acknowledge that paragraph 35 of the WSIS Tunis Agenda defines roles for the various stakeholders including states (governments), the private sector, civil society, intergovernmental and international organizations. The United States believes that Paragraph 35 must be read as a whole in the context of the broader Tunis Agenda and the discussions leading up to it, and that the necessity of engagement by the private sector, civil society, intergovernmental and international organizations is paramount. The United States’ understanding of these particular roles is informed by our democratic process and our commitment to multistakeholder Internet policymaking and governance. Governments must continue to work in concert with industry, civil society, technical and academic experts, and others to advise on what is technically and commercially feasible to ensure the Internet continues to scale, and evolve.  Unilateral efforts by governments to regulate technical and operational aspects of the Internet or to foster the development of an indigenous ICT sector by imposing discriminatory local rules serves only to hinder the kind of investment, innovation, and competition that created today’s Internet. Such efforts will also inhibit industry growth and creativity and broader economic development.  Within the U.S. we are committed to using a multistakeholder approach to address Internet policy issues that ensures transparency, fair process, and accountability.  This multistakeholder approach allows policymakers to work amongst the international community to find attainable solutions to the unique challenges, particularly those challenges associated with access, content, and capacity.  In addition, policymakers make it a priority to promote and protect the free flow of information online. As a priority the U.S. holds that Internet users should be able to send and receive content of their choice with limited interference, consistent with international human rights norms and conventions.  Best outcomes are achieved through the active involvement of stakeholders from industry, civil society, the technical community, and academia. With full participation by all relevant and interested stakeholders, we are less likely to adopt policies and regulations that inhibit innovation and restrict the rights of free expression. Through multistakeholder collaboration, we are more likely to grow economies, catalyse opportunities, and invigorate social discourse.  Below, we provide additional detail on existing or potential governmental activities in relation to each of the International Internet-related public policy issues identified in Annex 1 of Resolution 1305. |

# **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Multilingualisation of the internet including Internationalised (multilingual) Domain Names**  The multilingualisation of the internet will allow users to use the internet in different languages and scripts, which will assist in making the internet more culturally diverse. The ability to access and produce content in different in their own language will offer all internet users more choices in their avenues for communication, and help them to benefit from the opportunities that the internet provides.  Governments have a role in supporting the progress of this important policy issue.  The Australian Government is a strong supporter of ICANN’s multi-stakeholder approach to internet-related policy development, and its ongoing work to introduce internationalised domain names (IDNs) into the Domain Name System. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | Most web sites in the Republic of Belarus are registered in domain zone .by, information is mostly presented in one or both national languages of the Republic of Belarus (Belarusian and Russian).  During 2013 active negotiations with ICANN were held and it’s expected that Cyrillic domain zone .БЕЛ will be launched in 2014. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | In terms of IDNs, Botswana adheres to the ‘latin alphabets’. Currently the .bw registry supports IDN’s but as a country it is not yet implemented. Until such a time when there is a demand for IDN’s that is when it will be considered.  Botswana encourages the development of local content in local languages and this will further be promoted through the utilisation Universal and Service Fund (USF), which about to be established. Local content would ensure that Batswana have access to meaningful and relevant online content hence promoting usage of the internet. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | The Bulgarian Government has contributed to the ICANN IDN Fast Track process: thanks partly to the unsuccessful bid to obtain Cyrillic IDN ccTLD for Bulgaria, the ICANN policy was changed. As a result of that change Bulgaria, Greece, and other interested countries have the opportunity to appeal for review of the first objection. Furthermore, the ICANN IDN program has proven to be working both in the Fast Track, and in the new gTLD part. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  Denmark has actively supported the IDN policy making process and decisions in ICANN. We also support the European initiatives to implement IDN variants for Bulgaria and Greece. Presently there is no demand on a national level for any Danish IDN’s. Both Greenland and the Fareo Islands have been delegated their own 2-character ISO 3166-1 top-level domain. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * A request has been submitted to ICANN to have the Iraqi Arabic domain name ( عراق .) and the procedures are at their final stages. * Encouraging the design of Iraqi websites with more than one language. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  Governmental Advisory Committee (GAC) in ICANN has contributed from the perspective of universal connectivity, security/stability, robust development, transparency and non-discriminatory in order to facilitate the implementation of internationalized domain names through advising IDN ccTLD Policies and so on.  At this stage, 26 IDN ccTLDs are delegated into the root zone.  **Actions to be undertaken by governments**  Governments should continuously contribute from the perspective of universal connectivity, security/stability, robust development, transparency and non-discriminatory through participating in ICANN/GAC for further implementation of internationalized domain names.  And also, governments are encouraged to be boosters of IDNs by using IDNs for their own websites etc.  Multilingualization of the Internet has been well developed by R&D, establishment of standards and formulation of policies led by private-sector-based initiatives so these initiatives should be maintained.  But still now, there are not enough applications for IDNs. So all stakeholders including governments are encouraged to promote IDN-aware applications. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | 1. **Multilingualization of the Internet Including Internationalized Domain Names**   The issues of Internationalized Domain Names in Korea is mentioned in ‘section Ⅲ – Domain’ in this summary report. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | * **Management of Internet resources, including domain names and addresses** (issuses 1, 2, 3 in Annex 1)   RRT is authorized to issue permissions regarding the use of the name of Lithuania in the second level domain name before the top-level domain “lt”. The authorizations ensure that the name of Lithuania is used in an appropriate manner and encourage a proper representation of Lithuania on the Internet.  Lithuania, represented by RRT, is a member of the Government Advisory Committee (GAC), an advisory body to the Board of Directors of the Internet Corporation for Assigned Names and Numbers (ICANN), the organization which performs the administration of the Internet protocol addresses, domain name system and Internet root servers. The main function of GAC is to advise ICANN on public policy issues.  Lithuania attaches great importance to a multistakeholder dialogue in internet governance and organised the 2010 Internet Governance Forum meeting in Vilnius, Lithuania. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  With regard to the first public policy issue we inform you that the Government Decision No 765 from 05.07.2006 on the Republic of Moldova official web page was adopted. According to this decision, the information posted on the country official web page should be presented/published into three languages: the official state language, English and Russian, and can be translated into other languages if necessary. Also, the Government Decision No 188 regarding official public administration web pages from 03.04.2012 has extended the provisions of the aforementioned Decision. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**   1. **Internationalized Domain Names**   The [Root-Zone](http://www.iana.org/domains/root) was limited to ASCII (American Standard Code for Information Interchange) characters. However, the introduction of Internationalized Domain Names (IDNs) has given to the Internet users the opportunity to access domain names in their own language. Through two new processes, recently allowed by ICANN:   * IDN Fast Track Process: The ICANN Board, at its annual meeting in Seoul, South Korea in October 2009, has enabled countries and territories that use languages based on scripts other than Latin,to submit requests to ICANN for IDN ccTLDs representing their respective country or territory names in local scripts other than ASCII characters. (Ex: **المغرب, امارات**). * New generic Top-Level Domains (new gTLDs): ICANN has approved, at its 41th meeting in Singapore in June 2011, the new gTLD program, giving the possibility of applying for new TLD domain names that represents geographic locations, communities, trades, etc. This program has also allowed the addition into the root zone of IDN gTLDs, based on scripts other than Latin, such as Chinese, Arabic, Cyrillic, etc. ICANN has received 116 applications for IDN new gTLDs (Ex: **كوم**, **欧莱雅**, **شبكة** ‘already delegated by ICANN’).  1. **IDN ccTLD Fast Track Process/ Delegation of the IDN ccTLD “المغرب.“**   Through the IDN ccTLD Fast Track process, the National Telecommunication Regulatory Agency (ANRT), with the support of Moroccan government, had initiated in 2010 the application procedure for delegating the Arabic ccTLD "المغرب.".  Thus, the Board of ICANN has approved in April 2011, the delegation of the Arabic ccTLD "المغرب." To the ANRT (the Administrator of the ASCII ccTLD: “.ma”).  The Agency will prepare the naming policy and Registration phases for "المغرب" domain names, notably in accordance with international standards and practices and with the involvement of the local main stakeholders, and through an online public consultation.  Knowing that the most Internet users are generally more comfortable to use Internet services through their native language, it is necessary to make names and content on the Internet available in non-Latin based scripts to a large number of users. Thus, the introduction of the Arabic domain names under "المغرب" could help to promote the development of Arabic online content in Morocco. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | **POLICY AND REGULATION: Multilingualization of the Internet, International Internet Connectivity,**  **International public policy issues pertaining to the Internet and the management of Internet resources.**  InternetNZ, the New Zealand Domain name registrar, has actively supported the introduction and implementation of Internationalised Domain Names through the International Corporation of Assigned Names and Numbers (ICANN). The .nz domain introduced the use of macrons in 2010 to allow for Maori language strings.  International Internet Connectivity in New Zealand is managed on a fully commercial basis between private providers. The New Zealand Government does not regulate international Internet Connections.  The New Zealand Government participates in the discussions on international management of Internet resources, including domain names and addresses through regular attendance at the International Corporation for Assigned Names and Numbers (ICANN) Governmental Advisory Committee meetings, and through discussions with the New Zealand Domain Name Registrar.  New Zealand also has an annual multistakeholder conference, Nethui, which brings together internet stakeholders across New Zealand to discuss internet public policy issues. This event is based on the format of multi-stakeholder collaboration successfully introduced by the global Internet Governance Forum (IGF)  We support continued discussions in international fora regarding the process towards enhanced cooperation on Internet governance. We encourage the ITU to support developing countries to build capability so they can effectively participate on an equal footing, in multistakeholder discussions regarding international public policy issues pertaining to the Internet, as detailed in PP. Resolution 102 (Rev. Guadalajara, 2010). |
|  | Norway [(INF/35)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0035/en) | **Multilingualization of the Internet including Internationalized (multilingual) Domain names**  To address multilingualization of the Domain Name System (DNS), Norway has worked through ICANN’s Governmental Advisory Committed supporting the policy development process called “ccTLD Fast Track” which ended up with a successful introduction of several new ccTLDs in various scripts. Norway will continue to participate in the policy processes to enable introduction of both IDN ccTLDs and new IDN gTLDs. |
|  | Oman (TRA) [(INF/10)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0010/en) | TRA launched (عمان.), which is (.oman) Arabic IDN. TRA also accredited three local registrars. The number of registered (.oman) Arabic IDN domain names has increased.  Also, TRA starts lead a campaign about (Arabic content in the internet) in 2014. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  Regarding the two languages of Paraguay the Spanish and Guaraní are widely used in Paraguay, i.e. the Polytechnic School of the National University of Asunción has developed applications in the native language called Guarani. Domains have also been registered in Guarani language, such as: [www.yagua.com](http://www.yagua.com), [www.yayogua.com.py](http://www.yayogua.com.py), [www.guaranirenda.com](http://www.guaranirenda.com), [www.tocorre.com](http://www.tocorre.com) and more, plus content sites in Guarani. For more information please see National Computing Centre, [www.cnc.una.py](http://www.cnc.una.py). Also we can mention that Paraguay instituted a Language Policies Secretariat [www.spl.gov.py](http://www.spl.gov.py). |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**   1. **NASK[[1]](#footnote-1) (Research and Academy Computer Network)**   **Introduction of IDNs** (2003) enabling the use of Polish language symbols in domain naming. Apart from substantial extension of naming register it provides facilities for ethnic minorities to register Internet domains using their mother tongue. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  A Memorandum of Understanding was signed between Portugal and Brazil in October 2009 to increase the multilingualization of the Internet namely in Portuguese (1) the integration of the search on the open access scientific information repositories of both countries (RCAAP); (2) the realization of an annual Portugal-Brazil conference on open access; (3) the joint development of resources for the computational processing of the Portuguese language extending the extensive resources made available for the European variant of Portuguese through the Linguateca project; (4) the development of a joint project for measuring the Web content in Portuguese; (5) the joint development of Web Archives namely on Science, Technology and Education Content.  The Portuguese Web Archives is a public institutional project for developing and providing access to archives of Web content in subdomains of the ccTLD.pt periodically recorded, several times a year. This project already assures a large number of snapshots of the evolution of the Web content in subdomains of the ccTLD .pt and goes back several years as the content available in the World Internet Archives was acquired to be provided in the Portuguese Web Archives. The project is member of the International Internet Preservation Consortium (IIPC). |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | From 2010, the Russian Federation has cyrillic country code top-level domain .РФ. As of January 2014, more than 808 thousand domain names were registered in the ccTLD .РФ.  Domain «.ru» is a leader in its popularity between other national domains, followed by «.com» и «.net».  According to W3Techs as of March 2013, Russian language became second highest widely-spread language in the Internet (by total number of documents/pages detected globally by web crawler which automatically identified language as «Russian»).  Efforts are under way to provide and develop national identity, enhance Russian-language audience in Internet and promote Internet functionality for the benefits of older people. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**   1. Support development of local content in local languages and scripts. 2. Develop international public policies addressing multilingualization issues such as email and search engines.   **Actions which have been undertaken by Governments**  A. Local content is a national and regional issue and many governments have programs in place to support development. |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | After the completion of the restructuring of the Sudanese ccTLD architecture, NIC should endeavor all government agencies to activate IDN on their portals. Also SIS shall encourage all website under .SD domain to activate the Arabic domain. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  There is a virtuous circle where infrastructure development, growth of local content and lower access prices feed each other. Market demand for local language content is driven by improved access, faster networks (for example, through the establishment of national Internet exchange points) and political support for broad, inclusive use of ICTs in the general public. Stakeholder groups should be aware of the “content divide” where much of the world’s content is unavailable to local population. Each stakeholder group can act in their sphere in support to the development of local content. There are useful suggestions available for how this can be done from the OECD, among others.[[2]](#footnote-2)  Internationalized domain names, IDN, are important to making domains available in local languages and scripts. ICANN is central to facilitate this through cooperation of all stakeholders, including governments through the Governmental Advisory Committee, GAC. Regional and Local Internet Registries, RIR and LIR, as well as international organizations can have a role in promoting the use of IDN as available. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | Since March 2004 it is possible to register internationalised domain names corresponding to the Swiss official languages under the country code Top Level Domain (ccTLD) .ch  <http://www.bakom.admin.ch/org/grundlagen/00563/00564/00681/index.html?lang=fr> |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | Since 2008, the UK, through its representative on the ICANN Governmental Advisory Committee, has been involved in discussions at the GAC on an agreed coordinated government line to the ICANN Board on the issue of multilingual domain names. ICANN has made arrangements for domain names to be multilingual and there are now a number of non-Latin script domain names with work continuing to release more. Many of the new gTLDs introduced this year use a non-Latin script, and 116 such applications have been made for strings using languages including Cyrillic, Arabic and Chinese. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  A logical starting place for promoting the development of local language content is for governments to encourage the development of services, applications, and websites in local languages, especially by maximizing the potential of their country code top-level domains (ccTLDs) to serve as venues for local content. Governments can also support research on improved automated translation methods as well as initiatives to scan and digitize key historical and educational materials. Most importantly, by establishing an enabling environment that encourages innovators and entrepreneurs to develop local digital content, governments can empower their citizens to take the lead on multilingualization efforts. Each of these activities can help increase the amount of locally relevant and accessible content available online. Another key consideration is the development of locally relevant content—creating the on-line value that pulls demand onto the expanding Internet. The rapidly evolving market of cloud services, portable, personal devices and advanced software applications will power a new generation of local content as more citizens gain access to the Internet at affordable cost.  The Internet Corporation for Assigned Names and Numbers (ICANN) is continuing to facilitate the development of non-English content and the broader availability of Internationalized Domain Names (IDNs) through the introduction of ccTLDs as well as and generic top level domains (gTLDs) in non-ASCII scripts. Beginning in 2010, countries and territories that use languages based on non-Latin scripts had the ability to request top-level domains that reflect their country’s name in its local script through ICANN’s Fast Track IDN ccTLD process, which was developed jointly by the Governmental Advisory Committee (GAC) and the Country Code Names Supporting Organization (ccNSO). At this time there roughly 40 IDN ccTLDs have been entered into the root. A longer term IDN ccTLD policy is nearing completion.  Further, many of the first new gTLDs that have been introduced into the root of the Internet this year are IDNs, and 116 such applications have been made for strings using languages including Cyrillic, Arabic and Chinese. Governments have contributed to the development of the policies that have facilitated the introduction of IDN top level domains through their participation in the GAC.  UNESCO has primary responsibility for supporting multilingualism on the Internet, within the UN System. Governments can work through UNESCO to develop policies to promote linguistic diversity, creation of local language content, access to multilingual digital resources, use of ICTs for the preservation of languages, and cooperation with other entities seeking to promote online multilingualization. UNESCO and ICANN have also entered into a Memorandum of Understanding (MOU) to support the introduction of IDNs and to collaborate in enhancing capabilities for countries, particularly developing countries, to actively participate in building an inclusive multilingual Internet. Also of note, the Internet Society (ISOC), the OECD, and UNESCO have partnered to promote content, and to highlight the important role Internet infrastructure plays in enabling content. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | * Currently no actions |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Multilingualization of the Internet Including Internationalized (multilingual) Domain Names**  There is currently no Policy on multilingualization of Domain Names in Zambia.  However, the registry software currently implemented in Zambia is capable of handling IDNs as and when the requirement is deemed necessary. |

# **International Internet Connectivity**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | It's necessary to stimulate development of interconnection points for backbone providers, responsible for international traffic, peering points and data centers. Special attention should be given to cost reduction of Tier-1 services. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | Botswana has connectivity to the East Africa Submarine Cable System (EASSy) and West Africa Cable System (WACs) in order to secure sufficient international broadband capacity for the country. The country finalised its National Broadband Strategy by end of 2013. The Strategy will assist in the coordinated rollout of broadband infrastructure and services.  The challenge as Botswana is that as a landlocked country it is very expensive to transit neighbouring States to be able to reach the shores. |
|  | Brazil [(INF/38)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0038/en) | **International Internet connectivity**  Brazil has deployed Internet Exchange Points, as part of a strategy to improve quality, increase connectivity and resilience of the Internet and reduce the costs of international interconnections. As of January 2014, Brazil operates, through the Internet Steering Committee (CGI.br), 25 IXPs located in major cities throughout the country. These IXPs jointly exchange total peak daily traffic in excess of 350 Gbps. The following website is the reference for information on IXPs in Brazil: <http://www.ptt.br/localidades/atuais/>.  Furthermore, Brazil has actively participated in ITU efforts to raise awareness of this very relevant issue, both at the World Conference on International Telecommunications (WCIT-12) and the World Telecommunication/ICT Policy Forum (WTPF-13). Based on its national experience, Brazil has promoted the view that enabling the interconnection of international, national and regional networks through IXPs is an effective way to improve international internet connectivity. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | Without licensing regime, Internet Service Providers were able to compete with each other, and reach levels of prices, which make the Internet in the country accessible and affordable for everyone. Bulgaria rates # 1 in the EU in fast speed Internet (*ITU, The World in 2013* - *ICT Facts and Figures)*. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **International Internet Connectivity** In the Danish eGovernment Strategy for 2011-2015, the government has set a number of benchmarks focusing on investment and development of the digital infrastructure that is secure and robust enough to meet future requirements. The digital strategy benchmarks are both set to promote the supply and the demand for high speed broadband (NGA).  The government has an ambitious broadband target that all households and businesses should have access to a broadband connection of minimum 100 Mbps download and 30 Mbps upload by 2020.  On 13 March 2013, the government furthermore launched 22 specific initiatives to promote the development and improvement of the framework conditions for the telecommunications companies' investments in broadband infrastructure in Denmark and promote the municipalities’ opportunities of providing better coverage requirements through public procurement of high speed broadband in areas where there is currently poor coverage.  The government is also working on an initiative to develop a more detailed broadband mapping to replace the now annual survey based on data from telecommunications companies. In general, there have been considerable investments in broadband infrastructure in Denmark. This has contributed to a well-developed broadband infrastructure. For example,approx. 81 pct. of all Danish households and businesses have access to a broadband connection with a download speed of 30 Mbps, and we are in the top 3 among OECD countries in terms of the number of broadband connections per 100 inhabitants.  Finally, in December 2012 the government has set up a growth team consisting of high level public and private experts, which will hand over recommendations to the government on how to promote the access and usage of broadband infrastructure to an even greater extend. The growth team is expected to submit its recommendations to the government in early 2014. The government will make a growth plan to address the growth team's recommendations. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **The development of standards for Internet**  The government needs to play due role in coordinating the creation of open standards on an international scale. The government is an affected party in many areas of standardization. The government should supplement the efforts by participating in the standards making process, facilitate or coordinate standardization with existing organizations especially the ITU, ISO, IEEE or any other standard setting organization to create a regime of open standards in order to minimise the possible use of Standard Essential Patents resulting in affordable equipment pricing. The government organization can play a major role in creating and supporting open standards as against consortium or propriety standards |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Establishing many international gateways IGWs on the Iraqi land and sea ports. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  International Internet Connectivity is based on negotiated deals between operators.  **Actions to be undertaken by governments**  International Internet Connectivity should continuously be decided by negotiated deals between operators as before. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | 1. **International Internet Connectivity** 2. **Backbone Networks**   ***IX (Internet eXchange)***  These days the internet is used as a medium for distributing vast amounts of information and connecting diverse users. To achieve this, there must be direct and indirect connection among ISP (Internet Service Providers) to provide connection services. As internet use has increased, a number of ISP is created. It caused to increase line cost due to the excessive investment and traffic. In this regard, in order to ensure efficient networking, the IX (Internet eXchange) has appeared.  The IX is an internet interworking service for efficient traffic communication between ISPs. For the purpose of connecting ISPs, each provider interfaces its lines to major IX NOCs (Network Operations Center) so that line costs are lowered and network paths provided. Looking at the IX operations in Korea:  ∙ the KTIX is connected to 18 ISPs and 2 IXs (total connection capacity approx. 1,804Gbps),  ∙ the DIX is connected to 30 ISPs and 2 IXs (total connection capacity approx. 1,500Gbps),  ∙ the SKBIX is connected to 12 ISPs and 3 IXs (total connection capacity approx. 1,795Gbps),  ∙ the KINX is connected to 15 ISPs and one IX (total connection capacity approx. 371Gbps), and  ∙ the 6NGIX, which operates on a nonprofit basis for IPv6-based traffic exchange, is connected to 5 ISPs (total connection capacity approx. 4Gbps).  ***Commercial Internet Networks***  A total of 119 Korean Internet commercial services, including Kornet (KT), Boranet (LG U+), B-Net (SK Broadband), Sejongnet (Sejong Telecom) and Dreammax (Dreamline), receive IP addresses from KISA(Korea Internet & Security Agency), responsible for Korean internet resources, and provide services such as leased lines and high-speed connectivity for institutions and individuals using the Internet.  KORNET is a domestic infrastructure network for internet connection. This high-speed information network is short for the ‘KORea-telecom-interNET’. From June 1994 until now, KORNET has installed 2.5G~10Gbps high-speed networks in over 90 locations across the country, and built over 20 international lines including the 140Gbps line connecting with the US and provided service. BORANET is the internet communication network of LG U+. It launched a service to lease internet lines for enterprises in October 1994, and then extended the service to home users. It also provides high-speed internet customers with triple-play service, i.e. voice, internet and broadcasting. B-Net is the internet network of SK Broadband. It launched commercial service in April 1999, introduced Korea’s first IPTV service (Btv) in July 2006. Currently over 130 are accommodating subscriber section traffic around the country, and B-Net is connected to numerous foreign and major Korean service providers to provide high-quality internet service.   1. **Subscriber Networks**   ***Fixed Line Networks***  Korea completed its government-led BcN(Broadband Convergence Network) project in 2010, six years after it commenced in 2004. The number of BcN subscribers using a connection faster than 50Mbps now exceeds 14.82 million, over achieving the original goal of 12 million by more than 20%. The BcN project has enabled practically all cities, towns and rural communities to use 50M~100Mbps FTTH and HFC-based broadband Internet services. For small farming and fishing villages with fewer than 50 households, for which access to broadband Internet service was not commercially practical, the farming and fishing village broadband subscriber network promotion project has been operated since 2010. The FTTH-based broadband networks were implemented for about 38% (5,002) of 13,217 villages in total by December 2012. Also, the Giga Internet project, which was launched in 2009, will offer the Giga Internet which is10 times faster than BcN, offering speeds between 100Mbps and 1Gbps. Aiming at more than 90% of Giga coverage across the country by 2017, Korea is now developing and demonstrating technologies for enhancing next-generation subscriber networks, such as Giga Wi-Fi, 10GE-PON and the RF Overlay-based Giga Internet.  ***Wireless Networks***  As smartphones and tablet PCs have vastly consumed, the connection to the internet has become common from anywhere and at any and all times. To handle excessive traffic in WMAN networks like WCDMA or LTE, domestic mobile carriers are actively installing Wi-Fi Aps (Access Point). To date, the three mobile carriers in Korea have installed more than 400,000 APs, and general users are increasingly installing Wi-Fi APs in their homes or offices to reduce costs and ensure faster connection. According to a March 2013 study released by IDC, Wi-Fi services of global carriers are forecast to record about USD 4.2 trillion of sales in 2013.  As APs have proliferated, excessive installation of APs caused signal interference and deteriorating transmission speed. To address this, starting in 2012, the government has been inducing the three major domestic carriers to jointly install APs in public places so that more than 2,000 APs have been installed across the country, and by the end of 2013 an additional 2,000 APs will be installed in heavy traffic areas and inner city areas around the country so that the public can have better access to the Internet.  Traffic per LTE subscriber in Korea is 1.6 times that of WCDMA subscribers, and data traffic is increasing rapidly as the number of LTE subscribers is increasing sharply. So expansion of the LTE bandwidth is being actively discussed. Unlike 3G, LTE transmission speed will improve proportionally as bandwidth is increased. In other words, if the current 10MHz width of LTE is increased to 20MHz or more, the transmission speed of LTE will be doubled. The government finished auctioning the LTE spectrum in the 1.8GHz and 2.6GHz band in August 2013, but when and how to allocate the spectrum adjacent to the 1.8GHz band owned by KT has become a heated issue. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | *Please refer to Section 1.* |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) In October 2010, Government agreed to an “Open Access Policy” being applied for the operation of undersea cable landing stations in Mauritius with a view to further stimulating competition in the ICT sector. This led to the possibility of purchase of Indefeasible Right of Use (IRU) by International Long Distance (ILD) operators in Mauritius from members of the SAFE consortium, resulting in a drastic decrease of up to 44% in the price International Private Lease Circuit (IPLC) lines.  (b) In April 2012, the ICT Authority of Mauritius approved the Reference Cross-Connection Offer that Mauritius Telecom Ltd would provide to duly licensed operators, with a view to allowing other consortium members of the SAFE cable to establish operations in Mauritius and offer IPLC at whosesale level. Subsequently, Belgacom Ltd (a member of SAFE Consortium) established a Mauritian branch and started its operation, leading to a reduction of up to 52% in the price of IPLC. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **International Internet Connectivity. Contributing to capacity building for Internet governance in developing countries. Developmental aspects of the Internet.**  ,,Digital Moldova 2020" Strategy was approved by the Government Decision No 857 on October 31, 2013. The strategy aims to create conditions through minimum state intervention, but with maximum effect for information society development, focusing efforts on three pillars:   * Pillar I: Access and infrastructure- Enlarging access and connectivity through wide optimized ICT infrastructure, with free uniform and non-discriminatory access to everyone. * Pillar II: Digital content and electronic services- Promoting digital content and services generating; * Pillar III: - Capacities and utilization- Strengthening literacy and digital content skills to enable innovation and usage stimulation.   The main purpose of this Strategy is to create the premises for developing a secured digital environment and to increase the confidence within it. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **International Internet Connectivity (Kingdom of Morocco)**  The Internet traffic volumes are increasing significantly, globally generated by services that require more and more bandwidth and a high sensitivity to latency. Therefore, it is widely recognized to optimize Internet Connectivity, notably by enabling the interconnection of networks through **Internet Exchange Points** (IXPs), which will be an effective way to improve international internet connectivity and to reduce the related costs.  Recognizing these challenges, the NCIT (National Council of the Information Technology), established by a decree and chaired by the Head of the Moroccan Government, has recommended the establishment of a national internet exchange point.  Thus, the Ministry in charge of the new technologies (Ministry of the Industry, trade, Investment and the Digital Economy), the National telecommunication Regulatory Agency of the kingdom of Morocco (ANRT) and other relevant national departments, are currently preparing the general framework for the establishment and the management of a national IXP, notably, the administrative and legal aspects. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 1.* |
|  | Oman (TRA) [(INF/10)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0010/en) | No activity, however, TRA ongoing study for the establishment of Internet Exchange Point IXP. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **International Internet Connectivity**  Connectivity in Paraguay is usually a bilateral agreement between the provider of Internet access service in Paraguay and a carrier service at the neighboring country (since Paraguay is a landlocked country). The administration of Paraguay and its peers at international forums are holding talks on the coordination of frequencies, roaming voice / data exchange and compensation of Internet data traffic. Paraguay was the one of the main driver of: ITU CMTI RESOLUTION PLEN / 1 (DUBAI, 2012) Special measures in favor of developing landlocked countries and small island developing States for access to international fiber optic networks. |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **International Internet Connectivity**   1. **NASK**   NASK’s international Internet connectivity is run mainly by means of purchasing services from international connectivity operators and through the DECIX (Internet exchange point based in Frankfurt).  Inter-operator cooperation is also carried out by way of offering services to companies based out of Poland.   1. **PCSS**[[3]](#footnote-3) **(Poznań Supercomputing and Networking Centre)**   Managing, developing and operating of the **Polish Optical Internet PIONIER[[4]](#footnote-4)**, a nationwide broadband optical network that represents a base for research and development in the area of information technology and telecommunications, computing sciences (grids, etc.), applications and services for the Information Society. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **International Internet Connectivity**  Portugal, through ANACOM (as the NRA) has been directly involved in the work undertaken by BEREC (before ERG), in particular on the evolution of IP interconnection at European level on a competitive perspective and, more recently, in the broader context of 'net neutrality' (see, for example, <http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/1130-an-assessment-of-ip-interconnection-in-the-context-of-net-neutrality>). Previously, within the participation in BEREC (ERG), ANACOM had leaned on IP interconnection in the context of the transition from PSTN to NGN (see ERG (07) 09, "ERG (08) 26 ERG Report on IP interconnection" and "ERG Common Statement NGN IP-IC Core". Many of the key points raised for IP/network connectivity are still at the heart of the current debate over network neutrality, i.e. the separation of network and application layers, "best effort" versus quality of service (QoS) and guaranteed service and also the charging principles used.  Moreover, at the level of access and Interconnection, Portugal considers that the establishment of national IXPs are helpful for developing countries to reduce international internet connectivity costs and improve and deepen the national internet experience.  Accordingly, Portugal highlights the experiences of several countries in Africa, Asia and South America as a valuable source for identifying the lessons learned and best practice in establishing regional and national interconnectivity.  At the transmission level, Portuguese operators are participating in a number of consortiums for the development and exploitation of submarine cables which are a key infrastructure for connecting Europe, Americas, Africa and Asia fostering reliable connectivity at competitive prices.  Please, see map: <http://www.submarinecablemap.com> |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Fostering growth of the number of interconnection points of backbone networks carrying Internet traffic, Internet exchange points, data centres, considering connectivity criteria for traffic exchange points or backbone networks. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **International Internet Connectivity**  **Rwanda Internet Exchange Point**    A Rwanda Internet Exchange Point (RINEX) was put in place by local network operators and ISPs. Another important point is that a Virtual Landing Point (VLP) is being built to help local ISPs and Network operators acquire submarine capacity that can be redistributed in their respective networks. Currently, all ISPs are connected to RINEX.  RINEX which is currently managed by Rwanda ICT association (RICTA), a neutral body, enables domestic traffic to remain local, and improvement of efficiency of international bandwidth utilization. It also helps to develop local contents and web hosting, attracts International content providers to locate their servers in Rwanda and promotes Internet broadband access and cost affordability.  **Connectivity to submarine cables**  Rwanda is currently connected to three international submarine fibre optic cable systems for Internet connection such as the East Africa Submarine Cable System (EASSY), The East African Marine Systems (TEAMS) and SEACOM through local telecommunication companies and ISPs.  This connectivity drastically increased the gateway capacity up to 5Gbps.  The Rwanda connectivity to three different cables and gateways through Mombasa and Dar es Salam routes increased the reliability and availability of the Internet in Rwanda. The international Internet bandwidth price decreased compared to the satellite Internet connectivity up to twenty times (from USD 2500/Mbps to USD 125/Mbps).  **Source:** (Lishan Adam, n.d.)  **Figure 1:** The undersea fibre optic links to the countries of East Africa. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**   1. Support mechanisms and strategies to ensure that national traffic remains local or regional. 2. Enact national and regional regulation supporting profitable but moderate connection charges. 3. Develop international public policies fostering affordable global connectivity, thereby facilitating improved and equitable access for all.   **Actions which have been undertaken by Governments**   1. A number of countries are undertaking relevant national and regional programs regarding local traffic. 2. A number of countries are implementing national regulation to support bilateral agreements between operators to ensure affordable connection charges. |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | MSC establish the SIXP in order to utilize the usage of the International Internet Connectivity. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **International Internet Connectivity**  Key issues to be addressed by low- and middle-income countries include the establishment of economic policies and regulations that enable competition on a level market playing field with predictability and accountability, leading to better infrastructure, lower prices and increased international exchange. The fourteen principles agreed in the OECD Communiqué on Principles for Internet Policy-Making can be useful in this respect[[5]](#footnote-5), as can the policy and regulatory best practices developed by the Alliance for Affordable Internet[[6]](#footnote-6)  IPv6 is one important issue since some new Internet users will not be able to get an IPv4 address and every service that aim to reach all users’ needs to be available by IPv6. Sweden have actively promoted the transition to IPv6 on a local, regional, national and international level. Sweden have been active on the international level within RIPE as well as within the ITU IPv6 group. We have made guidelines available in English to be able to spread them through ITU and other fora to support the uptake of IPv6. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | The Swiss Telecommunications Act states in Article 4 that anyone providing a telecommunications service must notify the Federal Office of Communications (the Office) of this. The Office registers telecommunications service providers who have notified  Article 3 of the Ordinance on Telecommunications Services states that foreign providers of international telecommunications services which entrust the termination of their connections in Switzerland to other providers which have notified their services are exempted from the obligation to notify. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | The UK believes that today’s international telecommunication services, including international Internet connectivity, should be provided on the basis of private sector commercial arrangements, and should not be driven by bilateral agreements between Administrations.  The UK also acknowledges the role that Internet Exchange Points (IXPs) both in the local and regional sense can play in reducing the costs of Internet connectivity in developing countries. IXPs are a viable option to lower costs by avoiding the cost of international links and physically connecting regional ISPs. As a consequence, this increases traffic in developing countries, giving incentives to both local ISPs and international ISPs to host on their servers. It also provides a major incentive in the procuring and delivery of local content to the benefit of the local community and businesses alike. The UK strongly supports the liberalisation of telecommunication markets in order to maximise the benefits of open competitive markets. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **International Internet Connectivity**  Governments have an essential role to play in enabling the development of broadband networks to facilitate international Internet connectivity. The most effective way to expand networks and improve access in developing countries is by establishing competitive markets with transparent and consistent regulatory systems to attract private capital, as well as by adopting measures designed to lower – rather than increase – the cost of broadband services for end users. Crucial infrastructure for improving international connectivity includes competitive landing stations and terrestrial access points that allow numerous entities to provide service and attract international investors seeking to extend fiber networks. Attempts to finance infrastructure deployment by mandating payments between service providers will lead to demand distortions and could effectively restrict availability of Internet services and content.  There are a variety of resources available to assist governments seeking to improve international Internet connectivity, including within ITU-D where there are numerous efforts focused on broadband deployment. The World Bank, the Inter-American Development Bank, and other regional development banks can help fund improvement in connectivity by identifying additional ways to further investment in broadband infrastructure and by providing best practices and means of technical assistance. Additionally, many nations offer bilateral assistance; for example, the U.S. government’s Global Broadband and Innovations program provides technical assistance in establishing national broadband plans and reforming universal service programs. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | * Availability of international connectivity through different transport providers and IP ports with geographic redundancy. * Installation, operation and availability of capacity in fiber optic submarine cables. * Satellite capacity and transmission. * Presence and connectivity at regional and international Internet Exchange Points (IXPs). * IPv6 Native connectivity with almost all carriers and transit providers. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **International Internet Connectivity**  International internet connectivity has been increased by Liquid Telecom, Zamtel and Fibrecom (ZESCO). This has increased the number of international fibre gateways to the under sea cables on east and west coast of Africa. |

# **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Internationally, the global internet governance framework is based on a multi-stakeholder model, which brings together representatives from government, civil society, industry, non-government organisations, academia, and industry. Within this framework, stakeholders have different roles and responsibilities and it is difficult for any one group, including governments, to exercise undue influence in policy development.  The multi-stakeholder model has encouraged economic growth and innovation by maximising access – anyone anywhere can invent new applications, develop content, or create hardware or other standard-based technology and connect it with the global network. These arrangements underpin features that are crucial to the internet’s success – its global nature, openness and dynamism – and ensure that it remains a global platform for economic and social innovation and development.  Governments have wide experience in public policy, and have an important role in any discussion about internet public policy, but they should not be the only voice. There is a broad range of public policy issues pertaining to the internet, such as security, privacy, access, and the administration of the technical protocols, which are often complex and interdependent.  The multi-stakeholder model enables a full range of views to be expressed.  The Australian Government has been a strong supporter of this model, and actively participates in multi-stakeholder forums to encourage an open, secure and stable internet. Within the current multi-stakeholder framework, ICANN is a key decision-making forum for internet governance and domain name policy. ICANN’s multi-stakeholder model brings together representatives from diverse sectors who work together to set the technical and policy framework for the stable and effective operation of the global internet. The Australian Government has participated in ICANN’s Governmental Advisory Committee since its inception, and will continue to work to improve and strengthen the multi-stakeholder model as the internet evolves. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | We find it practical to develop international recommendations on regulatory practices in Internet coordination and management, regarding the possibility to apply them at national scale.  Republic of Belarus thinks that cooperation between governments is required to discuss questions of public policy on Internet management. This cooperation could be effectively done through ITU, as a specialized UN agency on international telecommunications. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | With the depletion of IPv4 addresses, Botswana is looking into migrating to IPv6. An IPv6 task force has been formed in that regard.  The Botswana Communications Regulatory Authority also recently acquired the management of the Botswana country code Top Level Domain (ccTLD), this being the Government initiative for Telecommunication networks to support the growth and use of Internet. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | As mentioned above, Bulgaria does not license nor register in anyway with the domain names and the Internet addresses, and that’s a decision that has been continuously supported by governments and parliaments on a constant base since 1999. The Bulgarian example shows that less regulation results in higher competition, better choices for the users, as well as affordable and very fast access to the Internet. We would encourage other governments to study and use this example. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses** As a consequence of ICANN’s decision of June 2011 to launch the new gTLD programme a new bill regarding domain names is being debated in the Parliament in order to facilitate letters of non-objection to applicants for gTLD’s with a geographic name that is related to Denmark. The Danish Government is presently hosting meetings with ISP's and business associations in order to cooperate with the parties regarding information to Danish enterprises about IPv6. The Danish Government is also hosting regular multi-stakeholder meetings regarding ongoing internet governance issues and input to ICANN meetings and is responsible for the annual Danish Internet Governance Forum. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | • Starting the project of internet gateway.  • Working on developing our networks in a way that ensures the capability of tracking and tracing in the network to ease the work of investigating the cybercrimes.  • Adopting a special policy for the registration of domain addresses and names and arbitration, see this link [www.cmc.iq/en/iq.html](http://www.cmc.iq/en/iq.html)  • A study is under process to organize the Iraqi digital content. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  GAC in ICANN has contributed to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses, from the perspective of universal connectivity, security/stability, robust development, transparency and non-discriminatory in multi-stakeholder model.  For example, GAC advised to ICANN Board on new gTLD applications, which potentially violate national law and improvement of Accountability and Transparency of ICANN.  **Actions to be undertaken by governments**  As before, governments should contribute to considerations on operation and management of Internet resources, from the perspective of universal connectivity, security/stability, robust development, transparency and non-discriminatory, through participation of ICANN/GAC, in the multi-stakeholder system, as a stakeholder of the Internet.  **Additional Comments**  Regarding domain names and IP addresses, we’ve already had existing mechanisms, such as ICANN and RIR, led by the private sector to consider those policies.  Since the beginning of the Internet, as it develops, those mechanisms have gradually been established and have been operated favorably.  These mechanisms should be continuously maintained to consider policies on organizations on identifers of the Internet which globally spreads.  As before, governments should respect the mechanisms led by the private sector to determine policies and should engage in the mechanisms as a member of the multi-stakeholders of the Internet. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | 1. **Management of Internet Resource**   Korea is allocated internet resource by APNIC, a regional Internet Registry that allocates IP and AS numbers in the Asia Pacific region. Korea Internet & Security Agency (KISA)’s role as to internet resource is to manage kr domain and development of kr domain policy, to allocate and assign the Internet Protocol (IP) addresses and Autonomous System (AS) numbers, and to the operate and DNS(Domain Name Server) etc. When domestic ISPs or organizations are assigned a certain amount of IPs and then ISPs later allocates IP address to end-user (customers).   1. **IPs and ASs**   Korea has been making efforts to stably secure IP (Internet Protocol) addresses and AS (Autonomous System) numbers. As of the end of April 2013, Korea has 112,261,632 IPv4 addresses, No. 6 in the world, and 5,231 IPv6 addresses (/32, 296), No. 8 in the world, while it has 1,016 AS numbers, making it No. 11 in the world.   1. **Domain**   As to the domain, there are two kinds of top national domains in Korea: ‘.kr’ and ‘.한국(*Hankook*)’. The ‘.kr’ domain was launched as a three-tier system such as ‘abc.co.kr’ when introduced in 1986. The two-level ‘Korean alphabet.kr’ system was introduced in 2003, and the two-level English system, e.g. ‘abc.kr’, was introduced in 2006. By the end of December 2012, a total of 1,094,431 addresses had been registered in the ‘.kr’ domain. Meanwhile, according to the demand of non-English speaking countries that want to use their own languages for a domain, ICANN (Internet Corporation for Assigned Names and Numbers), which establishes the global policy for the world’s internet addresses, finalized its plan in October 2009 to introduce multi-language top national domains. In response, the KCC decided to use the Korean characters of ‘.한국’ for the top national domain. In February 2011, ICANN delegated KISA as the authority responsible for managing the ‘.한국’ domain, and registration for ‘.한국’ domain names commenced on May 25, 2011. To smoothly introduce the ‘.한국’ domain and prevent any confusion or conflicts likely to occur in the early stages, KISA handled the assignment of domain names in three pre-launch stages. First instituted was a registration period during which government and public institutions were given the opportunity to register domain names first, then trademark holders were added, followed by a lottery registration period during which registrants were given one registration opportunity with those having identical requests being determined by lottery. After the domain was launched, as with the ‘.kr’ domain, domain names have been registered on a first come- first-serve basis. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | *Please refer to Section 1.* |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) A Multi-Stakeholder Forum on Internet Governance will be set up to formulate policies for the management of internet domain names.  (b) Migration from IPV4 to IPV6 facilitated by Government. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Domain names registration and management is performed in accordance with the "Regulation on domain names management under the country code top-level domain .md", approved on August 28, 2000, by the National Regulatory Agency for Electronic Communications and Information Technology.  The Ministry of Information Technology and Communications is the authority responsible for policies and strategies of domain names governance in the country code top-level domain .md. The Ministry issues the policy and management strategy of the top-level domain names .md.  National Regulatory Agency for Electronic Communications and Information Technology is the authority responsible for applying the regulation and management strategy assigning names for country code top level domain. md.  The Republic of Moldova resident enterprise in the information field "MoldData", appointed by the Ministry, is the empowered national assigner and administrator authority of names for the country code top level domain .md. The national registrar of names for country code top level domain .md is to be held liable for following the IANA/ICANN rules as well as the current law. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **Moroccan policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**   1. **Domain names/ “.ma” ccTLD**   Since August 2006, the National telecommunication Regulatory Agency of the kingdom of Morocco (ANRT) has been designated by ICANN as the “.ma” ccTLD manager.  Otherwise, the law No. 29-06 amending and supplementing law No. 24-96 on the Moroccan post and telecommunications, has expanded ANRT’s attributions in the management of Internet domain names under the ".ma". ANRT is notably responsible for:   * Assigning domain names ".ma" and defining the terms of their administrative, technical and commercial management in transparent and non-discriminatory condition, in line with international practices. (At the end of December 2013, the total number of « .ma » domain names has reached **50.945**). * Defining rules for the “.ma” domain management and follow-up of its implementation. * Authorizing the “.ma” registrars so as to guarantee sound and fair commercial practices. (At the end of December 2013, the total number of « .ma » registrars is **32**). * Protecting end-users with regards to abusive use of “.ma” domain names. * Introducing rules governing dispute management regarding the use of “.ma” domain names. (See: Domain Name Dispute Resolution Service for “.ma” domain names: <http://www.wipo.int/amc/fr/domains/rules/cctld/ma/index.html>). * Representing the ".ma" domain in international bodies. * Ensuring the continuity of ".ma" domain name registration services.   In this context, ANRT has prepared and published a naming policy for “.ma” domain names, which has been adopted through the ANRT decision N° ANRT/DG/11/ 08.  ANRT is currently working on the improvement of “.ma” management system, through the coming implementation of a new technical management platform, based on international standards and practices.   1. **IP addresses**   **Moroccan national strategy for the transition to IPv6**  In order to develop a national strategy for the transition to IPv6, ANRT and the Ministry of the Industry, trade, Investment and the Digital Economy have commissioned a study, which provided with three main components:   * The analysis of the IT ecosystem maturity regarding IPv6. * The technical and economic impacts of a transition to IPv6. * Developing an action plan for the transition to IPv6 at the national level.   The lessons from the maturity analysis of the ecosystem combined with a national benchmark of good practices for national transition in many countries around the world, helped to build a strategic plan for Morocco, which put the authorities in the lead of this transition. The plan focuses on four strategic priorities, detailed in more than thirty actions:   * Priority 1: To encourage ISPs to have commercial IPv6 connectivity offers; * Priority 2: Ensuring IPv6 compliance for all components present in the territory; * Priority 3: Raising awareness of the ecosystem and promote IPv6, particularly among businesses; * Priority 4: Ensuring, through the transition to IPv6 for all government agencies, the existence of a qualified demand for IPv6.   The implementation of these priorities is managed by a governance structure, included as part of national governance of information technology plan. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 1.* |
|  | Norway [(INF/35)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0035/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses.**  Norway has taken the opportunity to participate in the multistakeholder work within the entities responsible for the technical management and coordination of Internet resources, such as ICANN’s Governmental Advisory Committee (GAC) and the Regional Internet Registry (RIR) in our region, RIPE NCC.  Norway has taken an active part in the Governmental Advisory Committee and encourages all governments to take part in developing policies related to the DNS. Norway strongly supports active participation of governments in the GAC. To contribute to greater participation of governments we have together with the Government of Brazil and the Government of the Netherlands, taken the initiative and have put forward funds to establish and finance an independent GAC Secretariat. Norway believes that a good functioning GAC secretariat will help all governments, including governments in developing countries, to take a more active part in the work and policy processes in the Governmental Advisory Committee.  Norway also takes part in the RIPE NCC Roundtable meetings for governments where policy issues regarding management of Internet resources are addressed. We value this kind of cooperation and information exchange between the various stakeholders.  As encouraged by several entities, both the Internet technical community, and by several ITU resolutions on IPv6, Norway established in 2011 a national IPv6 working group with multistakeholder participation, to collectively address the challenges with the transition from IPv4 to IPv6. The Norwegian Government has taken this lead to highlight the importance for Internet Service Providers to start planning the transition from IPv4 to IPv6. This has proven very successful focusing on the IPv6 issues. RIPE NCC has also contributed in a very positive manner in this Norwegian national working group. |
|  | Oman (TRA) [(INF/10)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0010/en) | TRA published (domain name regulation) which regulate domain names under (.om ccTLD) & (عمان. IDN)  Active participation in international forums and meetings for example ICANN, RIPE, DNS forums and APTLD |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Currently, Paraguay plan to encourage investment in data centers of foreign companies in Paraguay. For example Facebook has embarked on his Paraguay Local Data Center via a mobile phone company. Also gradually other companies come in this regard, depending on the improvement in infrastructure and backbone operating in Paraguay. The local allocation domain is administered by the National Computing Centre dependent (CNC) of the National University of Asunción and Catholic University. Please see [www.nic.py/about.htm](http://www.nic.py/about.htm). |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**   * 1. **Gdansk Technical University[[7]](#footnote-7)**   Active contribution to the global standardization process through participation in the Internet Engineering Task Force (IETF) and the International Federation for Information Processing (IFIP).   * 1. **NASK**   Committed, long-standing and active participation in the Council of European national Top Level Registries (CENTR,  an association of Internet ccTLDs) and the ICANN. NASK is the sole funder, contributor and supporter of the Polish delegate to the GAC ICANN. It also delegated staff to the Management Board of ENISA. Since 2010 it has also been member of the Country Code Names Supporting Organization and is active in the RIPE Network Coordination Center.   * 1. **PCSS**   Launching of the K-root DNS server on the PIONIER network (2004) in Poznań. The server was the first one of this kind to have been set up in Poland and the Central and Eastern Europe. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Portugal has provided technical support to the responsible entities from Angola and Cape Verde for the ccTLDs from .AO and .CV management.  Portugal has signed two collaboration Protocols in 2012:  - A cooperation Protocol with Guinea Bissau for technical support in the operation of ccTLD.gw.  - A cooperation Protocol the Republic of Cape Verde that foresees technical support for the creation of internationally recognised Computer Security Incident Response Team (CSIRT) in Cape Verde. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Development of globally applicable principles on public policy issues as well as norms, rules and decision-making procedures associated with the coordination and management of critical Internet resources.  There is a need to establish a platform enabling governments, on an equal footing, to carry out their responsibilities, in international public policy issues pertaining to Internet, but not to get into day-to-day technical and operational matters that do not impact the international public policy issues.  The Russian Federation notes the importance of further internationalization of the oversight management of critical Internet resources in the direction of the environment, which ensures equality amongst citizens of all countries, represented by their governments’ participation on an equal footing.  The Russian Federation emphasizes the importance for ITU Member States to further clarify the role of each stakeholder, and especially governments, in multi-stakeholder implementation mechanisms with regard to international Internet-related public policy issues.  Notes the importance to consider the international character of decision-making processes regarding core functions of Internet, which is needed to develop international internet public policies, harmonize national laws, and facilitate international agreements, treaties and conventions.  The cooperation of governments with regard to international Internet-related public policy issues should be done in the framework of the International Telecommunication Union (ITU) as the UN specialised agency for information and communication technologies – ICTs. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Internet and the management of Internet resources, including domain names and addresses**  **ICANN , AFRINIC and AfIGF fora**  Rwanda actively participates in different meetings of ICANN and AFRINIC related to Internet resources management. Rwanda is represented in the Government Advisory Council (GAC) and Africa Government Working Group (AfGWG) responsible for handling the Internet governance and Internet resources management issues.  Rwanda as host of East African Communication Organization (EACO) is committed to integrated solutions related to international Internet issues and governance. It is in that framework that Rwanda hosted the fourth East African Internet Governance Forum (EA-IGF) that recommended developing harmonised guidelines on Internet policies for East African countries.  **National Internet Governance Forum (N-IGF)**  Rwanda has national Internet Governance forum (N-IGF) which meets once a year and composed of Internet community, Government representatives, ICT Regulator and ISPs. The forum is governed by non-profit organization (RICTA) in partnership with the Rwanda Private Sector Federation - ICT chamber (PSF-ICT).  The ISOC-Rwanda chapter also plays a vital role in organization of National Internet governance forum. The Rwanda IGF is an open forum where all Rwandans are to engage in active discussions about how ICT can improve their livelihood. The forum is facilitated by multiple media such as audio visual broadcasting, Telephones, Short massages (SMS), and social media. Rwanda National IGF provides a countrywide collaborative discussion about ICT.  The discussions are held mainly in national language (Kinyarwanda).  **Country code top level domain management**  The GoR has re-delegated the management of ccTLD to RICTA and is managed locally after its repatriation. This has facilitated the acceleration of development of e-applications in various socio- economic activities.  **Regional initiatives**  Based on dot africa registry policy on reserved names, Rwanda in partnership with other EACO countries will develop the reserve name list (RNL) for reserving Government names. The RNL provides for the following four categories:   * **Geographical Names**: *names recognizing geographic areas and features that are of substantial significance to governmental authorities, for examples regions/states, cities, provincial capitals, major towns among others.* * **Religious, Cultural and Linguistic Names**: *identifiers such as languages, tribes, peoples, religious groups and places of cultural or historic significances.* * **Economic and Public Interest Names**: *Names of substantial economic or public interest significance and uniquely linked to governmental authorities.* * **Offensive Names:** *Names that would inherently have the effect of advocating prejudice or hatred on the basis of race, ethnicity, ,political association, gender, sexuality, religion, conscience, or culture; or have the effect of inciting violence or causing of harm to any person or class of persons.* |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  A. Develop international public policies to ensure equitable and balanced distribution of Internet resources, including domain names and addresses, and to ensure that there is no unilateral control of those resources, including the administration of the root zone files and system.  **Actions which have been undertaken by Governments**  A. There has been no movement since 2005 on internationalizing the management of Internet resources. One entity still maintains unilateral control. Though some countries participate in providing advice regarding policies adopted by the entity, no mechanism exists to put in place meaningful, agreed and enforceable international public policies in this area. |
|  | Singapore [(INF/6)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0006/en) | “Net neutrality” is a term generally used to refer to Internet service or network providers treating all sources of Internet content equally, and the right of a consumer to access content and services on the Internet on a non-discriminatory basis.  Broadly, the net neutrality debate pitches parties who argue for encouragement of network investments (and hence oppose net neutrality rules), against parties who argue for the promotion of consumer choice and innovation.  On 16 June 2011, following a public consultation, IDA published a decision which set out Singapore’s policy approach towards net neutrality. This consists of the following:  1. No blocking of legitimate Internet content  • Internet Service Providers (“ISPs”) and telecom network operators are prohibited from blocking legitimate Internet content.  • ISPs and telecom network operators cannot impose discriminatory practices, restrictions, charges or other measures which, while not outright blocking, will render any legitimate Internet content effectively inaccessible or unusable.  2. Comply with competition & interconnection rules  • ISPs and telecom network operators must comply with IDA’s competition and interconnection rules.  3. Provide Information Transparency  • ISPs and telecom network operators must comply with IDA’s information transparency requirement and disclose to end-users their network management practices and typical Internet broadband download speeds.  4. Meet Minimum Quality of Service (“QoS”) standards  • ISPs must meet the minimum broadband QoS standards to ensure a reasonable broadband Internet experience for end-users.  • Reasonable network management practices are allowed, provided that the minimum Internet broadband QoS requirements are adhered to, and that such practices will not render any legitimate Internet content effectively inaccessible or unusable.  5. Niche or differentiated Internet services allowed  • ISPs and telecom network operators are allowed to offer niche or differentiated Internet service offerings that meet IDA‟s information transparency, minimum QoS and fair competition (including on interconnection) requirements.  This policy position is intended to facilitate consumers’ access to content and services on the Internet, while providing flexibility for ISPs, network operators, platform or device makers, and Internet companies and content providers to differentiate their services for economic efficiencies and innovation.  More information can be found here:  <http://www.ida.gov.sg/~/media/Files/PCDG/Consultations/20101111_Neteutrality/NetNeutralityExplanatoryMemo.pdf> |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | NTC, NIC, and local ISPs are collaborate with the regional register (AfriNIC) to develop regional policies to efficiently manage Internet critical recourse. However we have our reservations regarding the current management model. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Governments contribute to the work of ICANN through the GAC, along with other stakeholders. More countries should engage in the GAC, and the opportunity to engage in RIR, LIR and technical groups should also be considered. There is a need for better awareness and knowledge about the current internet governance regime especially for governments and agencies with little previous experience of multistakeholder policy environments. Comprehensive training programs at request for officials in low- and middle income countries could be useful to deepen political understanding of the internet governance system. The task of promoting a more active participation can, for instance, be addressed by regional organisations. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | Internet domain names represent a key infrastructure resource for the information society. The Federal Council supports the on-going development of the use and governance of the internet, including the domain name system at international level, in accordance with liberal, democratic and constitutional principles and through cooperation between public and private stakeholders.  On 27 February 2013, the Federal Council adopted the Strategy of the Confederation for the operation of internet domain names, cf. <http://www.bakom.admin.ch/dokumentation/medieninformationen/00471/index.html?lang=en&msg-id=47908> .  With this strategy, the Swiss Confederation wishes to ensure better protection of its own interests and those of Switzerland in the area of domain names.  The new strategy has also taken the international opening-up of the domain name market into account. For example, in 2012 the Confederation applied to ICANN, the global administration body for internet addresses, for assignment of the new extension .swiss. In this way the Confederation wishes to ensure that attractive internet domain names are available in sufficient quantities for businesses and society in Switzerland. It also wishes to promote the visibility of Switzerland in the virtual domain.  <http://www.bakom.admin.ch/themen/internet/00468/04153/index.html?lang=en> |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | The UK works through ICANN’s Governmental Advisory Committee (GAC) on these issues. All governments are invited to participate in the GAC, established specifically for governments to provide advice to the ICANN Board and community on the public policy aspects of issues related to the Domain Name System. Over 100 national governments now participate in GAC meetings, and ICANN bylaws provide that the ICANN Board must take due account of GAC advice when making policy decisions.  Governments have a role in managing Internet resources with regard to the management of their national country code domains. Referred to as ccTLDs, these are controlled directly by the ccTLD operator, while the government maintains important oversight functions, and is involved in any re-delegation process. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Governments have a number of opportunities to participate in the work of the multistakeholder entities responsible for coordinating the technical management of Internet resources, including domain names and addresses. All governments are invited to participate in ICANN’s Governmental Advisory Committee (GAC), established specifically for governments to provide advice to the ICANN Board and community on the public policy aspects of issues related to the Domain Name System (DNS). Over 130 national government members, and 32 representatives from Intergovernmental Organizations now participate in GAC deliberations , and ICANN Bylaws provide that the ICANN Board must take due account of GAC advice when making policy decisions, thus guaranteeing the involvement of national governments in the management of domain name matters. The GAC also provides funding for its developing country members to participate in GAC/ICANN meetings, interpretation in the 6 UN languages is provided for every meeting, and documents are routinely translated into other languages to facilitate broad participation in GAC deliberations.  Governments have a direct and vital role in managing Internet resources with regard to the management of their national country code domains, or ccTLDs.  Governments also can play a vital role by encouraging technological updates to infrastructure, specifically for the deployment of IPv6. As Internet use continues to grow across the globe, widespread adoption of IPv6 is critical to accommodate the millions of devices which will come online.  Governments can and should take an active role in working with Regional Internet Registries (RIRs) to encourage domestic IPv6 deployment. The United States strongly encourages governments to actively participate in ICANN and the RIRs, each of which manage policy development processes for their membership; there is no substitute for participation in these bodies that develop the policies related to the DNS. Governments interested in global network operations should also participate in Internet standards bodies, such as the Internet Engineering Task Force (IETF), and operational groups, such as Network Operator Groups. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - There are governmental and civil-society organizations participating in international Internet Public policy discussion and development.  - Domain registration process update: migration from third level “.com.uy” to second level “.uy”  - See also answer to issue 4. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **International public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses**  Zambia adheres to the IANA/ICANN guidelines for the management of Internet resources.  The regulator (Zambia Information &Communications Technology Authority), on behalf of the Government Republic of Zambia, successfully submitted for re-delegation of the .zm ccTLD from an ISP to the regulator after a consultative process amongst stakeholders.  Zambia is also looking at gradually transitioning from IPv4 to IPv6. The Authority is also looking at improving the operations of the Internet Exchange Point in Zambia- thereby reducing the international-capacity requirements for traffic meant to be “local”. |

# **The security, safety, continuity, sustainability, and robustness of the Internet**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  The Australian Government undertakes various programs to raise awareness amongst small-to-medium enterprises, along with the community more generally, of cyber security risks and the measures they can take to protect themselves and their business(es). The Stay Smart Online Program provides information targeted to individuals and small businesses to increase their online confidence and engagement by actively protecting their own, and others’, personal and financial information online. The Australian Government has also partnered with industry in the implementation of the Internet Service Providers (ISPs) voluntary code of practice for industry self-regulation in the area of cyber security – better known as the icode. At present, more than 30 ISPs are signatories to the icode. This includes a number of small and medium ISPs and most of Australia’s largest carriage service providers, representing up to 90 per cent of the home user market.  CERT Australia is the national computer emergency response team for Australia and the point of contact for international engagement with the global network of computer emergency response teams. It is the point of contact for operational cyber security issues affecting Australian businesses and is a trusted source of expert & actionable cyber security information. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | Republic of Belarus appreciates active cooperation at international level in the field of information security. At the same time we find it necessary to maintain an independent national policy on information security to protect national interests. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | Refer to item 5, 6 and 7 |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | Security is normally within the responsibilities of the Internet service providers, the telecom operators, and the users. The role of the Government is to provide the appropriate conditions to the above players. In order to achieve this the Bulgarian Government works in close coordination and cooperation with law-enforcement authorities, like ENISA, the IMPACT and other relevant bodies, including also through Bulgarian rapporteurs on Cybersecurity to the European Parliament.  Bulgaria has acceded to the initiative. Within this partnership Bulgaria hosted 2 successful Regional Conferences on Cybersecurity: in 2008 and 2012. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **The security, safety, continuity, sustainability, and robustness of the Internet** The Danish Government established a new Centre for Cyber Security in 2012 as stipulated in the Danish government coalition agreement from 2011. The aim of the centre is to strengthen the protection of the critical infrastructure, which supports vital functions in the Danish society. The centre is the national it-security authority and comprises the civilian and military Computer Emergency Response Teams in order to prevent, detect and mitigate cyber threats.  The Danish government will present a proposal for a new law on the Centre for Cyber Security in the spring of 2014. The aim of the new law is to strengthen the centre’s abilities to examine and prevent cyber attacks. Furthermore, the aim is to regulate the processing of personal data in thecentre in order to strengthen the protection hereof.  Currently, the Danish government is working on a national strategy for cyber security, which will be presented later this year. The strategy will include strategic priorities and tangible initiatives on the cyber security area, which will enable the continuously prevention, detection and mitigation of known as well as emerging cyber hreats. The strategy will also recommend a strengthening of the cooperation between the government agencies and the private sector. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **The security, safety, continuity, sustainability and robustness of the Internet**  The Indian government plays an important lead role in managing critical infrastructure such as energy, telecom, Internet etc. The Internet relies on a complex physical infrastructure of telecommunications and computer capacity and a set of common technical standards and protocols. The Indian government has a number of roles, along with other stakeholders, in helping to ensure that this infrastructure is robust and that it continues to develop on an open and pro-competitive basis to allow for new entrants, new services and new applications and for new users from around the world.  The **Section 70 of the Indian Information Technology Amendment Act (IT Act) 2008** provides guidelines for Critical Information Infrastructure and Protected System. The Indian Computer Emergency Response Team (CERT-In), a government body under the Ministry of Information and Technology, has been designated as the National Nodal Agency for incident response. By virtue of this, CERT-In will perform activities like collection, analysis and dissemination of information on cyber incidents, forecasts and alerts of cyber security incidents, emergency measures for handling cyber security incidents etc.  The role of CERT-In in e-publishing security vulnerabilities and security alerts is remarkable. CERT-In is very crucial and there are much expectations from CERT for not just sending out alerts but in combating cybercrime, monitoring the web-traffic, intercepting and blocking malicious sites, creating mechanisms for security threat early warning, vulnerability management and response to security threats whenever so required and with due process of law. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Connecting the Iraqi fiber optic cable to all Iraqi provinces and cities through a network of many rings. * Establishing a blog titled “The security in using the computer and internet”. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has undertaken various activities on security in the field of telecommunications such as establishment of a safe network environment, promotion of R&D, raising awareness of users and the promotion of international cooperation. under the initiative of headquarters for overall coordination on security policies.  **Actions to be undertaken by governments**  Governments will continue to undertake these activities on security in the field of telecommunications under the initiative of the headquarters.  **Additional Comments**  As the Internet rapidly grows and changes, demands on security and robustness of the Internet also grow. So, technologies and services should follow the movement of the Internet and should continuously evolve themselves.  Therefore, regarding security, sustainability and robustness of the Internet, technology community, which engages in technological development, standardization and operations, has consistently tackled those issues and has supported explosive expansion of the Internet.  Those efforts will also bring great achievements in the future too hence these issues should continuously be left to the technology community.  When the term "security" is used as a concept, the term includes many notions and tends to be multi-sense and ambiguous. Because of this ambiguity, constructive discussions have not been made.  Therefore, regarding discussions on the security and safety on the Internet-related public international policy, first of all, we should shed light on detailed items on security and analyse them, then carefully discuss them to determine proper policies. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | **IV. The security of the Internet(Information Security in General)**  2012 witnessed a variety of security threats, and intrusion incidents continuously occurred. Hacking of enterprises with the aim of stealing personal information, and DDoS (Distributed Denial of Service) attacks targeting game companies, portals and DNS servers continued throughout 2012, and sophisticated phishing attacks, which induce financial information leaks and payments, resulted in direct financial losses. Responding the internet incident requires the central government to provide situational awareness and establish a common operating picture for the entire relevant entities as appropriate, and to ensure that critical report reaches government decision makers in collaboration of relevant organization and the ISP/Vaccine firms.  To suppress such attacks, the MSIP (Ministry of Science, ICT and Future Planning) and the KISA (Korea Internet & Security Agency) operate the KrCERT/CC (Korea Computer Emergency Response Team Coordination Center) to detect, analyze and respond to signs of abnormal web traffic in advance, prevent intrusion incidents, analyze damaged systems and malicious codes, establish countermeasures, and quickly respond to intrusion incidents jointly with related agencies to prevent proliferation of damages. Most security incidents including zombie PC occur in private sector and KISA under the MISP is responsible for that incidents. If an incident occurred in public sector, National Cyber Security Center (NCSC) under the National Intelligence Service (NIS), military national defense sector in the under umbrella national defense has a strong drive to deal with the incident. All 3 sectors manager report to Senior Secretary to the President for National Crisis Management.  Korea also is operating Cyber Threat Warning System composed of 5 threat levels -Normal, Moderate, Substantial, Severe, and Critical- for the private sector. MSIP/KISA is in charge of issuing cyber security alarm and in each of level, the action ought to be taken is identified. Korea has issued substantial warning level but has not issued any level above severe or critical level yet.      **MSIP**  **MSIP**  **MSIP**  **MSIP**  Turning to the prevention aspect of the incident, Korea adopted a new system referring to “Information Security Management System (ISMS)” to evaluate if an organization has appropriate information security environment. Article 47 Certification of Information Security Management System in the “Act on Promotion of Information and Communications Network Utilization and Information Protection” (hereinafter ‘IT Network Act’) set out the legal basis of ISMS.  ISMS is a set of policies and procedures for systematically and continuously managing organization’s sensitive data since the risk gap grows over time without consistent management of information. As of February 18, 2013, compulsory ISMS has been operated along with voluntary ISMS. The following subjects must obtain the ISMS certificate in 2013, otherwise a certain amount of penalty (KRW 10 million) will be charged: Internet Service Providers (ISP), Internet Data Centers (IDC), and Internet Communications Services Providers with more than KRW 10 billion of total sales in previous fiscal year or more than one million users (on average) on a daily basis during last 3 months of the previous fiscal year. The certificate is valid for 3 years and required to renew it. It has been issued 151 certificates until 2012. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | **Activities of RRT in the area of ensuring network and information security, network sustainability and robustness** (issuses 4, 5, 6, 7 in Annex 1)   * **Activities of the national CERT-LT team in the area of network and information security**   With the rapid growth of ICT sector and development of e. business, e. health, e. learning and other ICT services, network and information security becomes increasingly relevant on both national and international level. In order to address the growing challenges to network and information security and to deal with network and information security incidents in public electronic networks in Lithuania on a coordinated basis, in 2006 a Lithuanian national Computer Emergency Response Team was established within RRT.  The mission of the CERT-LT team of RRT is to ensure the investigation of incidents of public electronic communications networks and information security, to coordinate the actions for the purpose of preventing incidents. CERT-LT coordinates activities of solving network and information security incidents on the national level, performs preventive activities by providing the information on new threats to computer users. The information is published on special websites, which also provide the users with recommendations and advice on how to avoid larger dangers and eliminate the consequences of the incidents.  CERT-LT receives the notifications of electronic communications service providers concerning network and information security incidents and threats, it registers and investigates incidents in public electronic communication networks and information systems in the Republic of Lithuania and conveys the material of the incident investigation to the institutions according to their competence, if CERT establishes the elements of possible criminal or administrative offences, regarding the security of electronic communications networks and information. Also, CERT monitors the state of security of electronic communications networks and information in the Republic of Lithuania. CERT-LT has developed a number of tools for its activities, such as the system of identification of malicious public websites, an early warning system, which analyses the available information and, if necessary, notifies the corresponding groups of the IT security threats, also, the laboratory, which investigates and analyses malicious code, creates measures and recommendations for the users.  When resolving international incidents, CERT-LT cooperates with the CERT units and incident investigation institutions operating in other states. CERT-LT has signed cooperation memorandums with the CERT units in other countries and other international partners that investigate international network security incidents. CERT-LT is a member of FIRST (a global Forum of Incident Response and Security Teams) and Trusted Introducer network.  In 2013, CERT-LT organised a national inter-institutional cyber training exercise. In 2011, CERT-LT also participated in pan-European exercises on Critical Information Infrastructure Protection CYBER EUROPE organised by EU Member States and facilitated by the European Network and Information Security Agency (ENISA). The objective of the exercise is to promote communication and collaboration between countries in Europe to try to respond to large-scale attacks.  To foster cooperation and best practice sharing, Lithuania participates in the activities of ENISA, the European Union Agency for Network and Information Security. Lithuania is also a member of ITU International Multilateral Partnership Against Cyber Threats (IMPACT), a multistakeholder alliance against cyber threats on a global scale.   * **Ensuring network sustainability and robustness: reliability study of the Internet network infrastructure**   Since 2008 RRT has been performing periodical assessments of reliability of Lithuania’s Internet infrastructure. The main aim of such assessments is to analyse the reliability of the national Internet network infrastructure of Lithuania and identify the potential risks. In 2012 RRT, together with academic community, as a part of a research, created new monitoring methods for defining, evaluating and establishing the reliability of critical objects of Lithuania’s Internet infrastructure, also, an instrumental model for monitoring implementation. According to these new methods, the critical objects of Lithuania’s Internet infrastructure were identified. |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | *Linked to No. 5* |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **The security, safety, continuity, sustainability, and robustness of the Internet (Morocco)**  With the development of the internet as a global infrastructure for business and as a new tool and resource for productivity and added value for economic sectors and for the public administration, the threat of cyberspace has become a central topic for national and international security.  Every day, news websites and social networks report attacks against personal accounts, businesses and government agencies.  In response to the increasing number of attacks in the cyberspace and to secure the ICT infrastructure and networks, protect the citizens and ensure the business continuity of critical Information Infrastructures, the Moroccan government has adopted the digital trust program as a support measure to implement the Moroccan National Strategy for Information Society and Digital Economy “Digital Morocco 2013”, launched in October 2009.  Ensuring business trust, enhancing security capabilities, securing critical information infrastructures and combating cybercrime are the ambitions of the Moroccan digital trust plan.  Through the digital trust plan the Moroccan government has identified the following initiatives and actions to develop the security, safety, continuity, sustainability, and robustness of the Internet:  **Initiative 1: Update and reinforce the legislative framework**   * Upgrade/update the legal and regulatory framework related to the Information Security System (ISS), digital trust, electronic exchange, protection of personal data, protection of online consumer   **Initiative 2: Put in place appropriate organisational structures**   * Set up a committee in charge of Information Systems Security, * Put in place a centre of coordination and response to incidents related to Information Systems Security (ma-CERT) at a national level, * Support the creation of PKI provider for ensuring electronic signature, * Encourage the development of backup sites and data center to ensure the Business Continuity of Critical Information Infrastructures of Morocco.   **Initiative 3: Promote and sensitise social operators to information systems security**  The improvement of the Information Systems Security and the response to cybercrime requires the development of a real culture of security. In addition to developing a good understanding of Information Systems Security, this awareness program should allow individual citizens to be aware of the measures taken to promote digital confidence.   * Raise awareness within the children, young people and parents of the Cybersecurity and cyberconfidence issues, * Implement a sensitisation and communication program about ISS in order to raise awareness within the children, young people, parents, administrations and enterprises of the Cybersecurity and cyberconfidence issues, * Integrate the Information Security Systems (ISS) in the Higher Scientific Education and training programs, * Set up and develop training programs in ISS for judges and magistrates, * Set up and develop training programs in ISS for administration employees/officials, * Encourage training in ISS for the private sector.   **Realizations**  As a result of actions undertaken within the framework of the digital trust program to develop the security, safety, continuity, sustainability, and robustness of the Internet, Moroccan government has succeeded to:  **Initiative 1:**   * Adopt the law no 07-03 related to the information Systems infractions, * Adopt the law no 53-05 related to electronic exchange of legal data to facilitate the use of encryption means and electronic certification, * Adopt the law no31-08 related to the protection of online consumers, * Adopt the law no 09-08 related to the protection of the personal data, * Elaborate a global study of the legal instruments related to the information technology, cybersecurity and cybercrime to strengthen the Moroccan legal act and fill existing gaps that may be an obstacle to ensure the digital trust and combat cybercrime,   **Initiative 2:**   * Create the Strategic Committee of Information Security Systems responsible for elaborating the policy related to the protection of critical information infrastructure, * Create the General Directorate of Information Security Systems, * Create the Morocco-Computer Emergency Response Team (maCERT) to respond to security incidents, coordinate responses at the national level and propose different services related to the handling of these incidents, the analysis of their vulnerability and the restoration of systems under attack, * Create the National certification authority and service provider of electronic certificates.     **Initiative 3:**   * Implement an awareness and communication program about cybersecurity and safe internet * Provide training programs on cyber security for engineering and IT students to enlarge the pool of ISS experts * Provide training programs on cyber security for legal professions (magistrates, judges), * Encourage innovation in cybersecurity, electronic signature, cryptography… and support private initiatives and activities in ISS. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | **NETWORK STABILITY: The security, safety, continuity, sustainability, and robustness of the Internet**  The New Zealand Government undertakes a number of activities to support the stability of its national ICT infrastructure. New Zealand’s Cyber Security Strategy was launched in 2011, with three priorities:  **1.** Increasing Awareness and Online Security  **2.** Protecting Government Systems and Information  **3.** Incident Response and Planning  This strategy recognises that as the use of the internet in New Zealand increases, so too does our vulnerability to cyber threats.  New Zealand established its National Cyber Security Centre in 2011. The Centre is a key element of [New Zealand's Cyber Security Strategy](http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf) released in June 2011, providing enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.  In 2012 the National Cyber Policy Office was established in the Department of Prime Minister and Cabinet to lead and coordinate cyber security policy for New Zealand. The NCPO provides policy advice to the government on cyber security issues, works on engagement with the private sector and the community, and leads New Zealand’s international cyber policy work.  In partnership with the .nz domain name registrar, we also actively participate in relevant multistakeholder organisations to support the stability of the Internet and the services that run over these networks.  We encourage the ITU to progress actions in support of PP. Resolution 120, particularly the actions that support the ITU to:  • take a significant role in existing international discussions and initiatives on the management of Internet domain names and other Internet resources within the mandate of ITU; and  • to play an active and constructive role in the process towards enhanced cooperation as expressed in § 71 of the Tunis Agenda.  Furthermore, the New Zealand Government also assesses the sustainability and robustness of the telecommunications infrastructure that facilities use of the Internet in New Zealand through its National Infrastructure Plan. The Plan is designed to reduce uncertainty for businesses by outlining the Government's intentions for infrastructure development over a 20-year timeframe. The Plan sets out a vision that, by 2030, New Zealand's infrastructure is resilient, co-ordinated and contributes to economic growth and increased quality of life. Inputs into this plan include an assessment of the current state of the infrastructure, scenario and trend analysis, national resilience assessments, and projections for future investment. |
|  | Norway [(INF/35)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0035/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  Ensuring security and robustness of Internet has been and continues to be high priority for Norway. Norway has developed in cooperation with relevant private stakeholders a Cyber Security Strategy for Norway which includes security for telecommunications networks and the Internet.  <http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf>  Governments have an important part to play in addressing these issues nationally and globally and ensure good cooperation amongst government stakeholders. In this regard many private stakeholders also have an import part to play working to ensure the security, safety, continuity, sustainability and the robustness of the Internet. Governments must ensure that all relevant stakeholders can take an active part. |
|  | Oman (TRA) [(INF/10)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0010/en) | TRA became an LIR and hosted RIPE NCC training on LIR’s, RIPE database and IPv6.  We also maintain .om DNS root server. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  Most banks, financial companies and cooperatives entities in Paraguay have their website. These web sites can performed transfer money between accounts of the same user, different users, remittances abroad, payment services , credit card payments, etc. All these services have received counseling from foreign companies for the implementation of systems of computer security, the Paraguayan professionals are continually being trained for improvement, updating and creating new options. Paraguay also exists in a Team of Cyber Incident Response [CERT -PY ] ([www.csirt.gov.py](http://www.csirt.gov.py)) coordinated by the Public Ministry (Attorney General office) ([www.ministeriopublico.gov.py](http://www.ministeriopublico.gov.py)) Moreover, the mobile phone companies also have robust systems security.  Paraguay count with the Law No. 4017/2010 "Legal validity of electronic signatures, digital signatures, data messages and electronic record" and its Regulatory Decree No: 7369/2011 and the Law No. 4868/2013, "Electronic Commerce".  Some websites of public institutions have been attacked by hackers, but exists in Paraguay a Team of Cyber Incident Response [CERT -PY ] ([www.csirt.gov.py/](http://www.csirt.gov.py/) ) coordinated by the Public Ministry (Attorney General office) ([www.ministeriopublico.gov.py/](http://www.ministeriopublico.gov.py/)) |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**   1. **Warsaw Technical University[[8]](#footnote-8)**   Developing of the **NEWMAN** project. It aims at rolling out of infrastructure, staff training at regional level, supporting R&D of Polish research teams through exchange of information with facilities around the world by means of the backbone network of the Polish Optical Internet PIONIER.  The university is also running the projects PL-GRID and PL-GRID plus under which national data shops[[9]](#footnote-9) are set up and developed.   1. **NASK**  * The main line around which NASK’s Internet safety activities are structured is expanding and maintaining capacities for enhanced response on emerging network threats, which since 1996 has been channeled through the **CERT Polska**.   CERT Poland was the first response team to have been established in Poland, tasked with taking measures to combat cyber-threats. Apart from that it also disseminates safety breach related information across end users and by constant cooperation with other CERTs it continuously develops in order to provide up-to-date and relevant service.   * Last year NASK took control over the governmentdomain **.gov.pl.** with a view to provide enhanced protection on valuable resources.  1. **ABW (Internal Security Agency)[[10]](#footnote-10)** (crosscutting activity covering section 5, 8 and 9)  * Development and adoption of cyberspace security policy * Development of the **SBC.POL project** (Cyberspace Security System) in Poland. * Cooperation at **pl. ID, CEPIK 2.0** projects on e-administration * Creation of enabling environment on security through working out of recommendations and reports on cyber security.  1. **MSW**[[11]](#footnote-11) **(Ministry of the Interior)**  * Establishment of **CERT.GOV.PL** - the Governmental Computer Security Incident Response Team (2008)withthe chief task in ensuring and developing the capability of public administration units to protect themselves against cyber-threats, in particular against attacks aimed at the infrastructure involving IT systems and networks. * The **ARAKIS-GOV** system. An early warning system reporting threats arising on the Internet. The system has been developed by the IT Security Department of the Polish Internal Security Agency in cooperation with the CERT Polska. It was established in order to support the existing security measures protecting IT resources of public administration.  1. **PCSS**  * Establishment of the **PIONIER CERT** team (2001) tasked with security provision over the PIONIER network. One of the recent extensions of its terms of reference was launching research on DDoS (Distributed Denial of Service) type of cyber-threats. * PCSS is also **active in cyber security R&D**. For example, in 2010-12 it developed the project “*High-security advanced architecture of the Integrated IT Platform*” meant for use by the Police. It produced a safe IT network and application environment allowing reliable, effective, calibration- and storage-friendly data processing, as well making available of applications. Other PCSS projects: “*Management of information and knowledge in services requiring higher level of protection*” with the outcome of a dispersed detection system targeting MetaIDS intruders or “*Sensory data correlation module for detecting unwarranted behavior and supporting decision-taking process (SECOR)*” * **Running wide-reaching trainings** is another example of PCSS activity (many different target groups, various levels, technology-oriented studies), part of which, when recorded, is made available to the public free of charge. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  Apart from the European initiatives on this matter, Portugal is evaluating the definition and implementation of the National Strategy on Cybersecurity. The development of a National Centre on Cybersecurity was proposed by a dedicated Commission. This proposal is currently being examined by the Government and such a Centre is expected to be set-up.  Moreover, the national Digital Agenda (“[Agenda Portugal Digital](http://portugaldigital.pt/index/)”) foresees measures to ensure high levels of telecommunication and information security, high levels of consumers trust and confidence and to promote cybersecurity and privacy in the use of Internet and ICT.  There is a Computer Security Incident Response Team (CSIRT) network in Portugal, created on the initiative of [CERT.PT](http://www.cert.pt/) operated by [FCT - Fundação para a Ciência e a Tecnologia](http://www.fct.pt/) with the objective of improving responsiveness to threats of network and information systems security, including critical infrastructures. Actually, the CSIRT network consists in 20 organisations from private and public sectors including military forces and financial institutions.  Across borders, Portugal is mainly working with the EU in civilian contexts, and in military contexts also with NATO. As member of the European Network and Security Agency (ENISA) Management Board, Portugal is actively involved in its activities. Portugal has also been involved in the European Forum for Member States (EFMS) set up for ICT security within EU and in the European Public Private Partnerships for Resilience (EP3R) created in 2009 by the European Commission Action Plan under the Communication on Critical Information Infrastructure Protection “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”.  A Portuguese IPv6 Task-Force was created in 2004. The Portuguese Research and Education Network has been an active promoter of IPv6 since the late 90s. It assured IPv6 capabilities of DNS at top level very early. Its other main activities are related to the promotion of the adoption of IPv6 in a timely manner in all higher education and R&D institutions. The backbone of the network operates in dual-stack mode (IPv4 and IPv6) since 2003. During 2008, significant investments have been made to enable dual-stack operation of the following services in these institutions: DNS servers, mail servers and Web servers. Portugal has been involved in successful European sponsored projects aiming at securing experience in IPv6 deployment and migration from existing IPv4 networks and promoting IPv6 technology including the involvement of Africa, Latin America, Asia and Eastern Europe countries. Training and workshops on IPv6 have been organized throughout the past 10 years. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | The Russian Federation considers public policy issues pertaining to the Internet governance in terms of ensuring the integrity, sustainability, robustness, security of Internet and enabling environment for innovation and economic growth.  Notes the importance that Internet should remain an open and un-fragmented global resource with fair and truly international governance, which should be able to engender trust, equal capabilities for economic development and confidence for everyone.  The Russian Federation considers the relevant task to create an International information security based on universally recognized principles and norms of international law, which would facilitate the implementation of effective measures to counter existing threats, and of equitable partnership in the global information space. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  **Internet security in Rwanda**  In 2010, Rwanda enacted the law governing electronic messages, electronic signatures and electronic transactions.  In a bid to implement the above stated law, Rwanda has implemented the National Public Key Infrastructure (PKI) project in two phases. The implementation of the root CA infrastructure was concluded in December 2013. The second phase on the implementation of the Rwanda certification system that will issue the digital certificates to the end users is on-going.  Rwanda is currently implementing a National Computer Security and Incident Response Team (CSIRT) project. The CSIRT is required to manage and respond to any cyber threats targeting Rwanda’s ICT infrastructure.  Rwanda is in the process of reviewing the legislation regarding ICT governance in general and cyber security in particular. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**   1. Develop international public policies to ensure the security, safety, continuity, sustainability and robustness of the Internet and to prosecute those that deliberately attack the security and safety of the Internet. 2. Propose and support R&D programs related to technical and administrative improvements in the Internet.   **Actions which have been undertaken by Governments**  B. Those countries where R&D is undertaken are generally supporting those programs. There are continuing issues, however, with the role of developing and less developed countries regarding input to R&D programs. |
|  | Singapore [(INF/6)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0006/en) | Singapore has ensured that our industry is prepared for IPv6 as the underlying Internet protocol. However, IDA identified the issue of “islanding” as a potential problem during the initial period of IPv4/IPv6 co-existence.  “Islanding” refers to a situation where there are groups of users on IPv4-only systems or IPv6-only systems who are unable to access content on systems using the other protocol and are therefore being limited to services and content within their respective protocols, creating separate IPv4 and IPv6 Internet “islands”.  To address this problem, the Info-communications Development Authority of Singapore (“IDA”) held consultations on an Internet Protocol “No Islanding” Principle (“Principle”) and published its decision on 30 April 2012. Under the Principle:   1. Each Internet Access Service Provider (IASP) will be required to ensure that systems, equipment and networks within its control and operation for the provision of Internet access services to residential or non-business end-users in Singapore are capable of allowing access to content on the public Internet, regardless of the address type of the end-user (IPv4 or IPv6); 2. Each Internet Exchange (IX) will be required to ensure that it will not be in a position to cause traffic (whether on IPv4 or IPv6) from IASPs peering at the IX to be disrupted, due to the IX.s inability to support IPv4 and IPv6; and 3. Each wholesale broadband service provider will also be required to ensure that it will not be in a position to cause traffic (whether on IPv4 or IPv6) from IASPs to be disrupted, due to the inability of the wholesale products and services to support IPv4 and IPv6.   The Principle came into effect on 1 June 2013 and is to be reviewed after three years.  More information can be found here:  <http://www.ida.gov.sg/~/media/Files/PCDG/Consultations/20110620_NoIslandingPrinciple/IntProNoIslPrinciple.pdf> |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | The Sudanese CERT (cert.sd) was established by NTC to undertaken these issues. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  There are many actors participating in developing and ensuring security, safety, sustainability and robustness. It involves several layers of the internet ecology and includes the engagement of the private sector as well as government.  Sweden has implemented EU rules (the “Telecoms Package”), covering security requirements, security breach notification and personal data breach notification, into Swedish law. Sweden has financed numerous studies, projects and PPP:s in order to strengthen the robustness of electronic communications, including the Internet, on a national level. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | Critical infrastructures are infrastructures whose disruption, failure or destruction would have a serious impact on the functioning of society, the economy or the state.  The goal of critical infrastructure protection is to reduce the likelihood of occurrence and the impact of a disruption, failure or destruction of critical infrastructure and to minimise downtime. More about the strategy to protect critical infrastructure can be found at:  <http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.html>  On 27 June 2012 the Federal Council approved the «National strategy for Switzerland's protection against cyber risks».  <http://www.isb.admin.ch/themen/strategien/01583/index.html?lang=en>  The Federal IT Steering Unit ensures implementation of the ICT strategy of the Federal Council. Their Plan focuses on the years 2013 and 2014 and defines 20 milestones and assigns responsibilities to organization units within the federal administration. More information can be found at:  <http://www.isb.admin.ch/themen/strategien/00070/index.html?lang=en> |
|  | Turkey [(INF/24)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0024/en) | ***Safer Internet Service in Turkey***  Internet penetration is increasing rapidly all over the world and this trend makes it easy for users to access information. In this environment, children can be exposed to harmful content on the Internet and this may have negative effects on their spiritual health. It is considered necessary to protect children from Internet abuse and to prevent sexual exploitation of children. “By-Law on the Principles and Procedures Concerning to the Safer Internet Service” has been implemented and entered into force on 22 August 2011 above considerations in mind so as to provide safer internet service.  Safer Internet Service is a discretional and free of charge internet access service offered by Internet Service Providers via their own networks through which families and children have the opportunity of protection against harmful contents such as gambling, leading to suicide, child sexual abuse, drugs, images of violence, bloody and violent martial arts, animal fights, fraud and malicious software and web sites or applications providing access to such content.  Principles to determine, allow and block lists are constituted by the “Child and Family Profiles Criteria Working Board” that meets regularly. This Board is made up total of 11 members; 2 members from Ministry of Family and Social Policies; 2 members from non-governmental organizations; 1 member from the Digital Games Federation of Turkey, 3 members from academia, experts on respectively pedagogy, sociology and psychology; and 3 members from the Information and communications Technologies Authority (ICTA), one of which is the Chairman of the Board.  Safer Internet Service of Turkey is in parallel with European Union and ITU efforts. Safer Internet Service of Turkey is a good example of better internet concept designated by Communication for a European Strategy for a Better Internet for Children initiated by the European Commission by Neelie Kroes. Moreover prominent Internet service providers have recently sent their intention letters to join the CEO Coalition for a Better Internet for Kids introduced by Mrs. Neelie Kroes.  Turkey is willing to roll out and develop better internet efforts in the basis of governance and participation principles. Turkey is always open to any other relevant stakeholders for experience sharing.  ICTA activities on protecting children can be summarized as:   * Web portals: Web portals designed to promote Safer Use of Internet, such as <http://www.guvenliweb.org.tr> and [http://www.guvenlicocuk.org.tr](http://www.guvenlicocuk.org.tr/), developed with a view to enable children to safely surf the cyber world. * Seminars & Booklets: For the conscious, safe and effective use of Internet, seminars are held to mainly families and children throughout the country. As in previous years, ICTA continue to publish and distribute different awareness guide booklets and continue to develop projects with related organizations. For instances, ICTA initiated a new project with Ministry of National Education, which is  training of trainers about safer use of Internet and related technologies at schools in Turkey. 400 ICT teachers around Turkey were being trained with this project. * Safer Internet Service provided by ISPs: Internet Service Providers offer safer internet service which enables children to browse safe on the internet when they are alone when they are accompanied by their parents. * Cooperation: Turkey’s Internet Hotline, [IhbarWeb](http://ihbarweb.org.tr/), a member of INHOPE (International Association of Internet Hotlines), for reporting abuse content of Internet has been established. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | For items 4 to 7 – the UK is a signatory to the Budapest Convention on Cybercrime.  The UK, as part of NATO and the EU, participates in cybersecurity exchanges within those alliances. GovCertUK and CSIRTUK are members of the European Government Cert Group – [www.egc-group.org](http://www.egc-group.org)  The UK participates fully in cybersecurity debates within the UN (including UNODC), Interpol, ITU, EU, NATO and OSCE. This work is spread amongst many UK government departments and is coordinated by the UK Cabinet Office and Foreign and Commonwealth Office. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  Governments have a responsibility for promoting the security and reliability of domestic networks in the face of an evolving threat environment. Recognizing that cybersecurity is a shared responsibility among a range of stakeholders, including government, the private sector, the technical community, civil society, and individual users, it is necessary for governments to facilitate a cooperative environment among these relevant stakeholders to manage security risk. To this end, it is necessary to establish a national cybersecurity strategy that seeks to enable such a cooperative environment to manage risk amongst the government, network operators, online commercial enterprises and users and build a culture of cybersecurity. Such a strategy should address government-private sector collaboration, incident management capabilities (such as creating a national Computer Security Incident Response Team), legal infrastructure, and education/awareness-raising.  Governments have a part to play in ensuring that domestic networks operate in a secure and stable environment. The first step towards this end is establishing a national cybersecurity strategy that encourages a cooperative environment amongst government stakeholders, network operators, online commercial enterprises, and users of the domestic network. Such a strategy should include: establishing a national Computer Security Incident Response Team (CSIRT), encouraging other domestic entities to form CSIRTs, criminalizing activities that target ICT networks, and raising user awareness through public education.  There are a number of venues that can assist governments in cybersecurity matters, including: the Forum for Incident Response and Security Teams (FIRST), the Meridian Process and Conference, the Asia-Pacific Economic Cooperation Telecommunication and Information Working Group (APEC-TEL), Asia Pacific Computer Emergency Response Team (APCERT), Organisation for American States Committee Against Terrorism (OAS CICTE). ITU-D Question 22-1/1 also provides an opportunity for member states to share national experiences and best practices related to enhancing cybersecurity.  Government representatives can work with the Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), the RIRs, and ICANN, among other industry standards groups and fora to improve security of the infrastructure through development of technical means, e.g., to improve security of the routing infrastructure, standards to secure domain names, and new methods to validate the certificate infrastructure used throughout the World Wide Web. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - Infrastructure with security and redundancy at national and international levels.  - Existence of one Tier 3 datacenter and currently building one Tier 4 datacenter, both by the state owned Telecommunications Company.  - Computer Emergency Response Team/ Coordination Center, in charge of preventive and proactive network security in electronic governmental platforms.  - Root servers copies in Uruguay: currently nic.uy hosts a copy of the root-l and there is an agreement between the state owned Telecommunications Company and the regional RIR’s “+Raices” project that enables the state owned Telecommunications Company to host a copy of the root-f.  - Working in the analysis of critical telecommunications infrastructure at the domestic level and at the border international connectivity. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **The security, safety, continuity, sustainability, and robustness of the Internet**  Government has enacted the ECT Act No. 21 of 2009 to provide for a safe, secure and effective environment for the consumer, business and the government alike to effectively use the internet.  Zambia is also in the process of implementing DNSSEC to increase the security of the registry infrastructure servicing the zm ccTLD.  The Regulator is also proactively encouraging managers of critical information infrastructure to obtain ISO27001 certification, while also providing necessary assistance to achieve this goal to the respective CII.  Zambia is looking at implementing Public Key Infrastructure, |

# **Combating Cybercrime**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Combating Cybercrime**  Australia considers that ensuring an effective response to cybercrime is a priority for governments.  Australia released its National Plan to Combat Cybercrime in July 2013.  This plan represents a commitment from the Commonwealth, State and Territory governments of Australia to work together to address the threat posed by increasingly sophisticated cybercrime.   The Plan provides an overarching strategic framework to better align the efforts of domestic agencies responsible for combating different types of online crime.  The Plan is available online here: [www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx](http://ims.dept.gov.au/tccache77/3945977/www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx)  While the Plan focuses on the actions that governments will take, it also acknowledges the key roles played by industry and individuals and the importance of forging strong partnerships to deal with cybercrime.  The Plan identifies six priority areas for action, shaped around the critical contributions governments can make in strengthening our national response to cybercrime—areas where we must focus our efforts for the short to medium term in building our response to cybercrime.  These include:   * educating the community to protect themselves * partnering with industry to tackle the shared problem of cybercrime * fostering an intelligence-led approach and better information sharing * improving the capacity and capability of our agencies to address cybercrime * strengthening international engagement on cybercrime * ensuring our criminal justice framework keeps pace with technological change.   A key initiative under the Plan is the development of a national online reporting facility for cybercrime, to be called the Australian Cybercrime Online Reporting Network (ACORN). The ACORN will make it easier for the public to report cybercrime, get the information they need to protect themselves and ensure agencies can respond more quickly. The ACORN will also give a clearer picture of the scope and nature of cybercrime affecting Australians and enable better operational and policy responses.  It is expected that the ACORN will be operational in the second half of 2014  The Australian Government considers the Budapest Convention on Cybercrime the most appropriate basis for international cooperation on cybercrime.  Australia became a Party to the Convention on 1 March 2013.  Acceding to the Convention has helped to make our domestic laws more robust, while access to reciprocal arrangements with other Convention countries has enhanced cooperation on law enforcement investigations. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | In order to effectively oppose cybercrime it's reasonable:  - to strengthen information exchange between law enforcement agencies during cybercrime investigation;  - collaboration between governments through UN in order to develop aligned approaches to combating cybercrime. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | Botswana Government through the Ministry of Transport and Communications and the Botswana Communication Regulatory Authority in conjunction with other stakeholders, is collaborating with the International Multilateral Partnership Against Cyber Threats (IMPACT), which is the cybersecurity executing arm for the International Telecommunication Union (ITU) in an effort to ensure our cyberspace is secure.  With assistance from ITU-IMPACT, Botswana has successfully completed a country readiness assessment for the establishment of Computer Incident Response Team (CIRT) for Botswana. Botswana is also in the process of aligning the Cybercrime and Computer Related Crimes Act of Botswana with the SADC Model law on Cybercrime.  A National Cyber-security Reference group has been set up to be responsible for spearheading cyber-security issues in Botswana. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | The Bulgarian Government has ratified the Budapest Convention on Cybercrime. This issue is also provided for in the Penal Code. It has also joint activities with the International Cybercrime Academy, based in Sofia, and other entities, in order to secure the Internet to a maximum degree possible, with the limited resources available from the Government budget. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **Providing a consistent domestic legal framework for :**  **Combating Cybercrime, use and misuse of the Internet**  Indian government has to play a major role in combating cybercrime particularly new challenges posed by child protection, copyright infringement and consumer protection. Indian government has to place broader set of roles and responsibilities of various stakeholders to fight cybercrime.  In this respect the Indian government has passed the **IT Act 2000 and IT Amendment Act 2008** to tackle the menace of cyber crimes those dealing with cognizable offences and criminal acts as mentioned under Section 65, Section 66, and Section 67 etc.Transborder cyber crime is bound to increase as more people get connected to the internet. This would create a demand for not just domestic law enforcement involvement / efforts but also those at a regional and international level. To achieve these there needs to be in place Multilateral and Bilateral agreements between countries which would be negotiated by the respective governments. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Legislation of required laws, (1) The law of Information and Communication Technology; (2) The law of Cybercrimes; (3) The law of Freedom of Expression and Peaceful Protest; (4) The law of Electronic Signature and Electronic Transaction. * Joining the Arab Countries Treaty on Combating Cybercrimes. * Establishing a national work group consisting of 12 Ministries collaborating with CLDP to prepare a draft Iraqi strategy toward cybercrimes, and already having a national policy in this regard. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan concluded the convention on cybercrime (Budapest convention) in July 2012. Based on this convention, the government is to correspond with cybercrimes.  Besides, the government of Japan has established basic frameworks for this issue. Also the government has promoted voluntary actions taken by multi-stakeholders.  For example, to prevent illegal accesses, the government of Japan takes the following actions:   * Establishment of domestic law (Act on the Prohibition of Unauthorized Computer Access)   **Actions to be undertaken by governments**  The government of Japan will continuously observe the convention to correspond with cybercrimes. The government of Japan will also continuously establish basic frameworks for this issue and promote voluntary actions by multi-stakeholders. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | **V. Combating Cybercrime**  Recently cyber-crimes are not limited in hindering service provided in web-site but more likely to disturb the privacy and relate to the financial purpose through cyber-bullying, fraud like phishing scam. The police has been responding and investigating by establishing 'Cyber Terror Response Center' since 2000, but it is situated in environment where a responsive action is hard to work effectively due to the various relevant organizations in dealing with cyber-crime. The domestic organizations pertaining to the cyber-crime are varied from the investigation authorities to public agency referring to Korea Internet Security Center (KISC). |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | *Please refer to Section 4.* |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) A Committee on Cybersecurity has been set up to address all issues relating to cybersecurity.  (b) A National Cyber Security Strategy and Action Plan for 2014-2019 is being developed. The implementation of the strategy will help Mauritius to better respond to cyber threats. The strategy defines four main goals. The action plan is spread over a period of 5 years for the completion of all projects.  The four defined goals of the strategy are as follows:  (i) to secure our Cyberspace and establish a front line of defense against Cybercrime.  (ii) to enhance our resilience to Cyber Attacks and be able to defend against the full spectrum of Threats.  (iii) to develop an efficient collaborative model between the authorities and the business community for the purpose of advancing National Cyber Security and Cyber Defense.  (iv) to improve the Cyber Expertise and the comprehensive Cyber Security Awareness of all societal actors.  The Strategy also includes the development and implementation of Critical Information Infrastructure Protection (CIIP) framework for Mauritius. This policy will help critical sectors to defend against range of cyber threats.  (c) Mauritius acceded to the Budapest Convention on Cybercrime on 22 November 2013. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **Combating Cybercrime**  The Republic of Moldova approved, by the Law nr. 6-XVI from 02.02.2009, the Council of Europe Convention on Cybercrime adopted in Budapest on November 23, 2001.  The Republic of Moldova Law Nr. 20-XVI on Preventing and fighting cybercrime was adopted on February 03, 2009.  National Strategy for Information Society Development "Digital Moldova 2020" approved by the Government Decision Nr. 857 dated 31.10.2013 states as one of its main task setting the conditions for increased security and confidence in the digital environment. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **Policy to combat cybercrime In Morocco**  Moroccan governments recognize that the challenges presented by cybercrime require a coordinated national response.  The Moroccan National Strategy for Information Society and Digital Economy “Digital Morocco 2013”, launched in October 2009 has adopted the "digital trust "as one of the two support measures of this strategy to create the necessary conditions to develop the confidence of citizens and businesses in the digital economy.  Ensuring business trust, enhancing security capabilities, securing critical information infrastructures and combating cybercrime are the ambitions of the Moroccan digital trust plan.  Through the digital trust plan the Moroccan government has identified the following initiatives and actions to strengthen his response to cybercrime:  **Initiative 1: Update and reinforce the legislative framework**   * Upgrade/update the legal and regulatory framework in order to face the Cybersecurity challenges and harmonize it with the partners countries.   **Initiative 2: Put in place appropriate organisational structures**   * Set up a committee in charge of Information Systems Security, * Establish a centre of coordination and response to incidents related to Information Systems Security (ma-CERT) at a national level, * Support the creation of PKI provider for ensuring electronic signature, * Encourage the development of backup sites to ensure the Business Continuity of Critical Information Infrastructures of Morocco.   **Initiative 3: Promote and sensitise social operators to information systems security**  The improvement of the Information Systems Security and the response to cybercrime requires the development of a real culture of security. In addition to developing a good understanding of Information Systems Security, this awareness program should allow individual citizens to be aware of the measures taken to promote digital confidence.   * Raise awareness within the children, young people and parents of the Cybersecurity and cyberconfidence issues, * Implement a sensitization and communication program about ISS in order to raise awareness within the children, young people, parents, administrations and enterprises of the Cybersecurity and cyberconfidence issues, * Integrate the Information Security Systems (ISS) in the Higher Scientific Education and training programs, * Set up and develop training programs in ISS for judges and magistrates, * Set up and develop training programs in ISS for administration employees/officials, * Encourage training in ISS for the private sector.   **Realizations:**  As a result of actions undertaken within the framework of the digital trust program to develop the cybersecurity culture and response to cybercrime, Moroccan government has succeeded to:  **Initiative 1:**   * Adopt the law no 07-03 related to the information Systems infractions, * Adopt the law no 53-05 related to electronic exchange of legal data to facilitate the use of encryption means and electronic certification, * Adopt the law no31-08 related to the protection of on line consumers, * Adopt the law no 09-08 related to the protection of the personal data, * Elaborate a global study of the legal instruments related to the information technology and cybercrime to strengthen the Moroccan legal act and fill existing gaps that may be an obstacle to ensure the digital trust and combat cybercrime.   In addition, and in order to strengthen its legislation governing ICT / digital confidence and ensure its harmonization with international / regional conventions, Morocco has adopted the following laws:   * Law No. 136-12 approving the Convention No. 185 of the European Union on Cybercrime and its Additional Protocol, * Law n°75-12 approving the Arab Convention against information technology crimes.   **Initiative 2:**   * Create the Strategic Committee of Information Security Systems responsible for elaborating the policy related to the protection of critical information infrastructure, * Create the General Directorate of Information Security Systems, * Create the Morocco-Computer Emergency Response Team (maCERT) to respond to security incidents, coordinate responses at the national level and offer (or suggest) different services related to the handling of these incidents, the analysis of their vulnerability and the restoration of systems under attack, * Create the National certification authority and a service provider of electronic certificates.   **Initiative 3:**   * Implement an awareness and communication program about cybersecurity, * Provide training programs on cyber security for engineering and IT students, * Provide training programs on cyber security for legal professions (magistrates, judges). |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | **CRIME: Combating cybercrime, dealing with spam, issues pertaining to the use and misuse of the Internet and protecting children and young people from abuse and exploitation.**  *Cybercrime and child protection*  New Zealand is working with international organisations such as Interpol and the Virtual Global Taskforce to ensure cooperation on child protection, spam, and other criminal matters, in support of existing international justice agreements. The New Zealand Government has also entered into a partnership with ECPAT New Zealand, part of a global organisation the purpose of which is the elimination of child prostitution and pornography and trafficking of children for sexual purposes.  In 2006 the New Zealand Government passed the Crimes (Intimate Covert Filming) Amendment Act 2006. This Act makes it an offence to film people in intimate situations without their knowledge or consent, protecting privacy and potential misuse of the images obtained. This Act is similar to legislation in other jurisdictions such as the United States and Britain.  The New Zealand Government supports the non-profit organisations that promotes confident, safe, and responsible use of online technologies in New Zealand.  In addition, the New Zealand Government is also exploring opportunities to support capacity-building activities in the Pacific relating to combating cybercrime.  The New Zealand Government recognises the gap between supply and demand for cyber security capacity building internationally. New Zealand has delivered a number of capacity building initiatives in the ASEAN region over the last four years. We are committed to continuing to support our regional partners to boost their cyber capacity.  *Spam*  In 2007, the New Zealand Government passed the Unsolicited Electronic Messages Act, which came into effect on 5 September 2007.  The Act prohibit unsolicited commercial electronic messages (‘spam’) with a New Zealand link (i.e. messages sent to, from or within New Zealand), or address-harvesting software being used to create address lists for sending unsolicited commercial electronic messages.  The Act is also intended to encourage good direct marketing practice by:   * Requiring electronic messages to contain a functioning unsubscribe facility * Ensuring electronic messages are sent only to customers who have consented to receiving it * Restricting the use of address-harvesting software.   The Electronic Messaging Compliance Unit was established in September 2007 to enforce the Unsolicited Electronic Messages Act 2007 by investigating complaints about spam. In the first four years of operation, the anti-spam enforcement unit has issued three statements of claim, 18 infringement notices and 218 formal warnings under the Act.  *Harm minimisation*  In 2009, the New Zealand Government introduced the Digital Child Exploitation Filtering System, a filtering system operated by the Department of Internal Affairs in partnership with Internet Service Providers which blocks websites that host child sexual abuse images. This system is available for Internet Service Providers on an opt-in basis.  The New Zealand Government is currently considering the Harmful Digital Communications Bill, which introduces a range of measures to address damaging online communications and ensure perpetrators are held to account for their actions. This Bill puts in place a range of measures to both reduce harm from threatening behaviour online. In particular, this Bill seeks to provide protection for young people, who are bullied more easily, instantly, and anonymously online, by providing a civil enforcement regime to resolve issues in the most effective way possible. |
|  | Oman (ITA) [(INF/2)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0002/en) | The Oman National Computer Emergency Readiness Team (OCERT) was established in May 2009 to serve a wide group of ICT users, particularly the national infrastructure institutions and major industries, in addition to nationals and residents. It provides a diverse set of information security related services. The Centre also aims to The OCERT aims to build local and national cyber security capabilities in the sultanate of Oman and to analyze and handle cyber and information security incidents on the internet and Oman’s cyber space, as well as to enhance information security awareness and culture among different social strata, whether individuals or institutions.  In addition, the Sultanate Issued Cybercrimes Law through Royal Decree No. (12 / 2011 ) |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Combating Cybercrime**  In this aspect, Paraguay implemented laws and regulations concerning electronic and digital signature to protect Internet users against online identity theft. In addition, Paraguay has worked with multinational companies (eg, Microsoft, the American intelligence agency and others) to investigate electronic data exchanged to commit kidnapping and sexual abuse. Paraguay has a CSIRT ([www.csirt.gov.py](http://www.csirt.gov.py)) |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Combating Cybercrime**  **a. NASK**   * **Training.** In 2013 NASK trained ca. 500 enforcement agencies and justice affairs officers in combating cybercrime, with a focus on fighting sexual child abuse and child pornography. * **CERT Polska.** Apart from standard assignment relating to incidents handling, coordination, collecting and sharing information on threats, CERT Polska specializes in analysis of malware and neutralization of botnets. Through CERT, NASK reaches out to cooperate with enforcement and government agencies in Poland and abroad. * **Dyżurnet.pl.** NASK’sresponse team tasked with receiving and reacting to notifications on illegal contents (especially child sexual abuse) on the Internet. All verified notifications are sent over to the Police or contact points at the International Association of Internet Hotlines (INHOPE). * Full **implementation of the Domain Name Security Extension** (DNSSEC) on the .pl domain (2012).  1. **MSW**  * **“Razem bezpieczniej** (*Safer together*)**”** funding scheme. The programme mobilizes resources to co-finance regional level’s and NGOs’ projects aiming at limiting risks of threats including on the Internet. * **Hotline 116111** (2008). The facility has enabled minors to report all threats on the Internet. Verified notifications are sent over to the Police or the dyżurnet.pl. * Creation of **a cyber-security department** at the National Police Headquarters (2010) * **Amended law –** adding new types of crime to the penal code (2009) enabling penalization of criminally approaching minors under 15 through means of telecommunications.  1. **PCSS**  * Active participation in the works of the PPBW (Polish Platform for Homeland Security). For one of the joint projects called “*Management of information and knowledge in services requiring higher level of protection*” the two agencies took up the issue of exchange of retention data between telecommunications operators and authorized information handlers (e.g. Police). The outcome was in working out a **standard format for exchange of information**, based on the XML and the ETSI technical specification TS 102 657. * Based on that format, PCSS managed to develop a tentative prototype of the **SOPEL** system (Electronic crime exchange of information system). Plans for further development are in place. * Further research is planned on combating cyber-crime, e.g.: development of systems detecting abnormalities of networks as well as sensory security systems. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Combating Cybercrime**  Portugal has ratified the 2011 Budapest Convention on Cybercrime from the Council of Europe and adopted a Law on Cybercrime (Law nº. 109/2009, 15 of September).  In 2011, a Cybercrime Office under the *Procuradoria-Geral da República*, *Ministério Público* was established to ensure operational coordination, the training of judges and the interaction between private entities and law enforcement entities. |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | **Combating Cybercrime:**  MICT has established Qatar Computer Emergency Response Team (Q-CERT) in December 2005, in cooperation with the Carnegie Mellon's Software Engineering Institute (CERT Coordination Center).QCERT is a national, government-sponsored, organization setup under the auspices of Supreme Council of Information and Communication Technology (ictQATAR). |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | In order to improve efficiency of combating crime in the field of information and communication technology there is a need in further enhancement of international cooperation at various levels such as:  - Improvement of mechanisms associated with exchange of information between national law enforcement agencies in cybercrime investigations, sharing experiences on investigating methodologies and court practice in case hearing on the crimes in this field;  - Interaction of governments under the aegis of the United Nations on a harmonized approach to cooperation in the field of combating computer crime. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Combating Cybercrime**  In 2012,Rwanda enacted an organic law instituting the penal code, in which specific provisions deal with computer related crimes.  Rwanda Development Board (RDB) regularly carries out the national cyber security awareness. The campaign aims at educating citizens on basic cyber security requirements to raise knowledge regarding confidentiality, integrity, availability of systems, data, and related threats.  The GoR supports regular trainings to equip different institutions with skills to detect and investigate cyber-crimes, understand cyber terrorism, principles of evidence collection for cyber-crime, electronic money transfer technology, and basic IT tools in analyzing cyber crime evidence. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  A. Develop international public policies to combat cybercrime and to prosecute cyber criminals. Actively seek out cyber criminals operating within their territories and cooperate with other nations who are victims of cybercrime.  **Actions which have been undertaken by Governments**  A. A number of countries are actively involved in discussions of cybercrime and/or have national policies and laws related to cybercrime. However, no mechanism exists yet to put in place meaningful, agreed and enforceable international public policies in this area. Though some amount of bilateral or multilateral cooperation is being developed based on the evolution of existing discussions and forums, bilateral agreements are not the answer. |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | The Sudanese CERT (cert.sd) was established by NTC to undertaken these issues. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Combating Cybercrime**  Cybercrime is dealt with through the Budapest Convention. Sweden would like to build further on this convention and has proposed to tie the ITU to the Budapest convention on Cybercrime through a MoU – thereby ensuring that the ITU recognizes that this global convention is the one ITU Member States should adhere to when developing national cybercrime legislation.  There is a legislative proposal for full accession and ratification to the Budapest Convention on Cybercrime currently being considered by the Swedish government. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | The Cybercrime Coordination Unit Switzerland (CYCO) is Switzerland’s central office for reporting illegal subject matter on the Internet. After conducting an initial analysis of the incoming report and securing the relevant data, CYCO forwards the case to the appropriate law enforcement agencies in Switzerland and/or abroad. The Cybercrime Unit also actively searches the Internet for illegal subject matter and carries out in-depth analyses of Internet crime. The Cybercrime Unit is available to the public, the authorities and Internet service providers to answer questions on legal, criminal and technical aspects of Internet crime. It is also contact point for its foreign counterparts. Website: <http://www.fedpol.admin.ch/content/fedpol/en/home/themen/kriminalitaet/cybercrime.html> |
|  | Turkey [(INF/24)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0024/en) | ***Combating Cybercrime***  There are two main legislations regarding cyber activities. First is the Turkish Criminal Law that involves some articles regarding cybercrime. Second is the Law on Regulation of the publications on the Internet and Combating against committed crimes by these publications.  Moreover, Cyber Security Board chaired by the Minister of Transport, Maritime Affairs and Communications, was established, in order to determine the measures regarding cyber security, to approve the prepared plans, programs, reports, procedures, principles and standards  and ensure the application and coordination of them. The first action of the Board was to prepare National Cyber Security Strategy and Action Plan 2013-2014 which is approved by Cabinet Decision Nr.2013/4890. This Strategy Document includes provisions about the implementation of internationally recognized cyber security standards within the public sector. The strategy is based on the principal of securing the information systems used in critical infrastructures and taking necessary measures to provide national cyber security. For his purpose, it encourages the efficient use and sharing of resources between public and private sector in cyber security related activities.  The main outcome of the Strategy and Action Plan was to establish national cyber incident response team, shortly TR-CERT which is responsible for national and international coordination about cyber security issues. The relations between other national and sector specific CERTs, law enforcement agencies, research centers, internet service providers, hosting firms, other governmental agencies and other private sector institutions are arranged by TR-CERT with the help of “Communiqué on the Establishment, Responsibilities And Activities of CERTS”. Besides, TR-CERT works in close collaboration with international networks such as FIRST and Trusted Introducer. As a result, TR-CERT has also been collecting cyber security incident reports from over 30 countries. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | *Please refer to Section 4.* |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Combating Cybercrime**  Combating cybercrime is an inherently governmental responsibility. Governments must therefore pass appropriate domestic laws on cybercrime, and strengthen operational domestic capacity to effectively investigate and prosecute cybercrime violations. Because much cybercrime activity is transnational in nature, each country must have domestic legislation, and continuous training for investigators and prosecutors charged with fighting cybercrime. A country’s ability to assist international partners depends on the state of its domestic law which permits cooperation with foreign partners as well as a fully trained and experienced police and prosecutor corps. Countries that may need assistance in developing robust domestic capacity on anti-cybercrime efforts should participate in regional trainings offered under the auspices of OAS, Association of South East Asian Nations (ASEAN), APEC, the African Union, the Council of Europe, and others. The United States also offers a comprehensive training program to regional organizations and foreign law enforcement partners upon request to improve anti-cybercrime capacity. In turn, the U.S. provides cooperation for data requests and joint investigations as authorized under domestic law.  The UN Office on Drugs and Crime (UNODC) is the appropriate venue for governments seeking assistance on cybercrime matters. As established by the UN General Assembly, UNODC is the sole venue within the UN system for member states to address the policy, investigation and prosecution of cybercrime, including technical assistance and capacity building to strengthen international cooperation. UNODC has established the Global Program on Cybercrime which offers both regional and bi-lateral training and technical assistance to member states to improve anti-cybercrime investigation, prosecution, and adjudication. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - Several laws on cybercrime and privacy, and creation of specialized groups within the State.  - Computer Emergency Response Team/Coordination Center (CERT), responsible for protecting critical information assets and promoting awareness on information security.  - Computer Incident Response Team (CIRTs) in public and private organizations working in coordination.  - Cyber security capacity building through conferences on various topics and training of specialists, with the support of international partners.  - Knowledge transfer: orientation, advisory and accompanying to several countries at regional level.  - Technical assistance to public agencies to strengthen information security management systems and monitoring of government web sites.  - Uruguay is Chair of eLAC working group on Cyber security. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Combating Cybercrime**  The Electronic Communications & Transactions Act No. 21 of 2009 in Part XV makes provision for combating crime by criminalizing such activities as unauthorized access to, interference of or interference with data (Section 99), computer related extortion, fraud and forgery (Section 100), prohibition of pornography (Section 102), hacking, cracking and viruses (section 103) etc.  However, the recent country assessment report conducted by the ITU through the HIPSSA Project reveals that there is still need to strengthen the Act.  The completion of the recommendations from the HIPSSA project will strengthen the legislation of the Country on combating Cybercrime.  The regulator assigned a toll free short code 116 being hosted by Child line Zambia for reporting and protecting children from cyber crime.  Zambia, through a partnership with ITU and IMPACT, set up a Computer Incident Response Team (CIRT) to act as the focal point and response centre for cybersecurity related matters. Zambia is now looking at the establishment of sector-specific CIRTs.  The regulator has also focused on building capacity for Law Enforcement Agencies and other Security wings, primarily through training.  The government through the regulator is also building computer forensic labs for Law enforcement agencies, and undertaking to train the beneficiaries in the usage of the associated tools. |

# **Dealing effectively with spam**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Dealing effectively with spam**  Spam is a global problem that requires a global solution. Governments can play a key role in the effective regulation of spam and the Australian Government takes a multi-layered approach in this regard. There is also a very important role for the private sector to play in the provision of anti-spam tools for consumers and businesses.  To respond to the economic and social impacts created by the spam, Australia introduced the Spam Act in 2003 prohibiting the sending of unsolicited commercial electronic messages. Australia’s spam legislation was one of the first of its kind against spam in the world. It takes an ‘opt-in’ approach to commercial electronic messaging which requires recipient consent before commercial electronic messages can be sent. This method is consistent with Australian Privacy Principles and considered best practice - given the large volumes of unsolicited electronic messages consumers would otherwise be required to respond to in order to opt-out. This approach has similarly been taken in other countries, such as Japan, Canada and Taiwan, China.  In administering Australia’s spam legislation, the ACMA’s goal is to promote confidence in electronic messaging as a form of commercial communication. To do this the ACMA uses:   * Traditional compliance and enforcement strategies, together with * International engagement and cooperation * Industry and citizen education programs * Partnerships with industry * Market intelligence.   Cooperation with international agencies and regulators ranges from providing information and assistance on specific matters to an ongoing involvement with international anti-spam bodies such as the London Action Plan, which encourage cross-border collaborations between regulators, law enforcement and industry. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | Governments should take any possible measures to prevent spam distribution. For making these efforts more effective it's necessary to stimulate exchange of best practices between Member-States. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | The country has slow progress in this area and minimal participation in meetings such as ITU Study Group 17 and World Telecommunication Standardization Assembly (WTSA) that cover issues of cybersecurity and combating spam.  Continuous participation in such meetings is important for a country to assist in development of policies in the particular area and Botswana endeavors to seriously start participating in these meetings. |
|  | Brazil [(INF/38)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0038/en) | **Dealing effectively with spam**  In 2011, as a result of a joint effort by the National Telecommunications Agency (Anatel) and the Internet Steering Committee (CGI.br), Brazil adopted regulatory measures to combat spam. Since then, all relevant e-mail service providers in the country take part in a cooperation agreement that establishes a formal commitment to implement the management of TCP ports 25 and 587. The following website is the reference for anti-spam activities in Brazil: <http://www.antispam.br>.  Here as well, Brazil actively participated in ITU efforts to raise awareness of this issue at the World Conference on International Telecommunications (WCIT-12). |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | The Government deals with incoming spam, at the front routers/gateways, and makes sure that spam does not reach the mailbox of users. Historically, commercial operators have proven quite good in dealing effectively with spam. In the course of the recent couple of years the volume of spam in Bulgaria has decreased by more than 20%. The Bulgarian share in the global spam stream is 0.76%. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Starting some technical projects, like the project of internet gateways. * Taking the necessary measures on the level of institutions. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has established basic frameworks for this issue. Then the government has promoted voluntary actions taken by multi-stakeholders.  For example, the government of Japan has undertaken several activities:   * The Act on Regulation of the Transmission of Specified Electronic Mail (the Anti-Spam Law) has been enforced in 2002. * The opt-out regulation was amended to the opt-in regulation in 2008. * Sharing information on spam with other country’s governments. * Recommendation of introduction of technical measures to prevent transmission and reception of spam.   **Actions to be undertaken by governments**  Governments should steadily implement the national legal frameworks and to share information, knowledge and best practices with other countries.  More than 90% of spam in Japan comes from overseas, and it’s difficult to solve this issue in only one country. So international cooperation on anti-spam measures should be promoted. It is important that governments and public sectors from all countries have a meeting in a multi-lateral framework(ex. London Action Plan). |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Dealing Effectively with Spam**   Recent Spam is not only sending unsolicited advertising, but also affecting the leakage of personal information, as well as spreading malicious code. Hacking in conjunction with other malicious activities, thus, make users anxious and distress about spams is being intensified.  In Korea, Korea Communications Commission (KCC) and Korea Internet & Security Agency (KISA) have dealt with spam related grievance management since 2003 to relieve the inconvenience and discomfort of spam. A received report is under process to confirm whether the case violates the existing law. If is, administrative penalties will be imposed or further investigation will be undertaken. In addition, phone numbers for illegally sending spam, domain, IP in cooperation with internet service provider (ISP) take restrictive measures.  Corresponding to mitigate spam activities in Korea, KCC and KISA prevent the creation of a fake phone as well as the awareness toward users was promoted to restrain from using a fake phone since 2009. In addition, the amount of text message is also limited in 500 times at a time and the amount of phones to own personally is limited per capita. As a result, “phone to phone” method greatly reduces the amount of spam sent, on the other hand, companies such as through bulk SMS sending “web to phone” way to increase the amount of spam being sent through the pattern seems consistently increasing.  In line with “Comprehensive Anti-spam Measures” in 2009, an “intelligent anti-spam service” was initiated. Intelligent anti-spam services are providing a comprehensive analysis of the content, the reply code, sending patterns in the process of the transfer of text messages. It is a carrier's spam free value-added service to users and the effect to block the spams is appreciable.  Another step the Korean government took is to establish M-RBL (Mobile Real-time Blocking List) system to prevent the spread of malicious spam, through the mobile phone. A carrier with KCC and KISA interact to share and block the spam by extracting spammers number. Since 2005, in order to prevent the spread of spam email from a variety of sources collected domestic and foreign information, IP-based real-time anti-spam list, RBL(Real-time Blocking List) periodically generated through a comprehensive analysis. The list is provided to Korea's major portal, which is easily targeted at spam, as well as small mail server operating agencies. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | *Please refer to Section 4.* |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) To combat the problem of Spam in Mauritius, the National Computer Board, a statutory body under the Ministry of ICT implemented Anti-Spam Action Plan in 2006 and number of initiatives has been taken till date.  (b) The draft Unsolicited Electronic Commercial Message Bill will be reviewed by a consultant from the Council of Europe to align same with international laws. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 5.* |
|  | Oman (TRA) [(INF/10)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0010/en) | SPAM Awareness Campaign carried on 2010 |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Dealing effectively with spam**  In Paraguay there are private companies in the field of programming and technology that offer the implementation of anti-spam firewall in professional level. The Ministry of Industry and Commerce – MIC [www.mic.gov.py](http://www.mic.gov.py) has implemented a website for citizen of Paraguay could claim against spam received on mobile phones. Paraguay is entering into e-commerce with the Law 4017/2010 "From legal validity of electronic signatures, digital signatures, data messages and electronic record" and its Regulatory Decree No: 7369/2011 and the Law No. 4868/2013, "Electronic Commerce". |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Dealing effectively with spam**   1. **NASK**   CERT Polska is active in fighting spam affecting Polish networks. The measures applied include deactivation of botnets and removing malware from computers used for spamming. That removal is basically carried by ISPs who are approached and notified through a special CERT Polska’s IT platform - **n6[[12]](#footnote-12)**. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Governments should take measures to prevent the propagation of unsolicited bulk electronic communications and minimize its impact on international telecommunication services.  In addition, there is a need in strengthening dialogue and dissemination of best practices in countering spam between involved organizations/companies. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  A. Develop international public policies to deal effectively with spam and to prosecute spammers. Actively seek out spammers operating within their territories and cooperate with other nations who are victims of spam.  **Actions which have been undertaken by Governments**  A. A number of countries are actively involved in discussions of spam and/or have national policies and laws related to spam. However, no mechanism exists yet to put in place meaningful, agreed and enforceable international public policies in this area. Though some amount of bilateral or multilateral cooperation is being developed based on the evolution of existing discussions and forums, bilateral agreements are not the answer. |
|  | Singapore [(INF/6)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0006/en) | Spam can be defined as unsolicited commercial messages sent in bulk. Spam could be sent via mobile telephony systems or electronic mail (e-mail). Spam typically advertises or promotes goods or services, which may also include business opportunity or investment opportunities.  Spam is a growing concern for Internet users and it now accounts for a large percentage of e-mails worldwide.  Although spam transcends national boundaries, Singapore, as an Infocomm Technology hub, has in place measures to keep it in check. Public education and technical countermeasures act as our first line of defence.  This is supplemented by the Spam Control Act which was enacted on 15 June 2007, and serves as the overarching framework for spam control. Among other conditions, the Spam Control Act sets out requirements for senders of spam to comply with as well as provides for civil action to be taken by persons who suffer loss or damages.  More information on the Spam Control Act can be found here:  <http://www.parliament.gov.sg/sites/default/files/070006.pdf> |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | The Sudanese CERT (cert.sd) was established by NTC to undertaken these issues. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Dealing effectively with spam**  There are several global initiatives dealing with spam, such as The Messaging, Malware and Mobile Anti-Abuse Working Group (MAAWG) and the (LAP) London Action Plan. Sweden sees no need to start new fora, but to support the on-going initiatives.  Dealing with spam is not an international public policy issue. It is an issue for commercial spam-filters and their use on local levels. It may also be a national legal matter (legislation on commercial communications) and should be dealt with under the national legal framework. Also, it should be noted that both technological developments and fast changing user behaviour, with many users moving from e-mail to social networks or other online services, is quickly making the issue of spam less relevant . |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | Switzerland has implemented a functioning legal framework for combating spam. In consideration of the recent developments of spam it seems appropriate to adopt a holistic view of cybercrime in general of which spam has, together with malware, botnets, direct attacks, ransomware and other tools, become an integral part. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | *Please refer to Section 4.* |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Dealing effectively with spam**  The solution to unwanted spam includes the adoption of appropriate and existing technologies, the pursuit of appropriate enforcement actions against senders of spam, and the adoption of domestic laws that allow consumers to restrict their receipt of unsolicited commercial email. Filters, authentication programs, and other technologies have vastly reduced the receipt of unwanted commercial emails in regions where email providers have adopted these fundamental tools. Further, some countries have adopted laws that impose penalties on senders of spam who disregard restrictions on such mail, be they opt-in or opt-out programs.  When spam is a vector for malicious code, such as botnets, the appropriate criminal authorities, as noted above, should take action. As such, the US supports an approach that relies on the widely available and successful technologies, supported by appropriate law or enforcement regulatory action against entities that violate local anti-spam laws, finding this a proven and successful model. A number of multistakeholder organizations assist governments and other entities to control spam, including:   * The London Action Plan (LAP), a multinational forum of anti-spam enforcers, regulators and technologists. The group develops training for investigators, supports the development of anti-spam technology advances, and promotes joint law enforcement actions. Members of the LAP have brought coordinated civil cases involving global spammers and other consumer frauds. Further, the LAP, in partnership with the Messaging Malware and Mobile Anti-Abuse Working Group (M³AAWG), has developed for the OECD best practices for dealing with botnets, which often are the source of massive spam attacks. * Internet Society (ISOC) conducts capacity building programs in developing economies on how to manage spam. In addition, ISOC has compiled relevant guidelines for technical and policy approaches to spam, and toolkits of best practices established by experts in the technology field. ISOC has bureaus in Africa, Asia-Pacific, Europe, Latin America and Caribbean, the Middle-East, and North America. * Anti-Phishing Working Group (APWG), a multistakeholder coalition whose mission now far exceeds phishing attacks. In addition to serving as a networking resource, the APWG provides technical whitepapers and briefings from leading technology enterprises on well-established fixes for common spam-related threats. * Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) provides technical assistance and training for the implementation of anti-spam technologies in India. It has sponsored a new training foundation to replicate this program in other regions that need assistance addressing spam and malware abuses. In addition, M³AAWG provides free on-line training, and offers printed best practices information in seven languages, in addition to English. M³AAWG’s regular meetings offer unparalleled access to leading anti-spam technologists. * Additionally, ITU-D Question 22-1/1 provides a venue for member states to share national experiences and promote best practices related to combating spam.   M³AAWG reportsthat despite the high volumes of spam today, its members prevent all but a relatively small percentage of this abusive email from reaching users’ inboxes. According to this group, the most powerful anti-spam approaches identified to date are: 1) the widespread adoption of proven best practices based on shared industry expertise; and 2) industry collaboration in an environment of mutual trust and open dialogue.  The organizations identified above encourage all relevant entities – both public and private sector – to participation in their multistakeholder bodies, with the goal of developing a national experience unburdened by spam. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - The national telecommunication network includes various anti spam tools.  - The national awareness campaign “safe-connected” includes recommendations related to spam.  - Training for public servants about major security problems, including spam and recommendations to mitigate it.  - Public guides with recommendations and best practices available.  - Local Computer Emergency Response Team address complains and coordinates actions regarding local spam. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Dealing effectively with spam**  Section 105 of the Electronic Communication & Transaction Act of 2009 does not criminalize spamming per se; it only becomes an offence if the unsolicited information is for purposes of “illegal trade or commerce or other activity”.  Nonetheless, the regulator is encouraging the usage of SPAM filters at Internet Service Providers, Government Ministries, and Critical Information Infrastructure.  The regulator also sets out to increase awareness within the country regarding the unproductiveness of SPAM, while acknowledging the increasing complexity of SPAM detection. |

# **Issues pertaining to the use and misuse of the Internet**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Issues pertaining to the use and misuse of the Internet**  The Internet and cyberspace are not without rules. Australia considers that existing international law applies to the Internet and cyberspace. In relation to the use of the Internet by states, we note the June 2013 consensus report of the UN Group of Government Experts on developments in the field of information and telecommunications in the context of international security (UN General Assembly document A/68/98) which concluded that international law, and in particular the Charter of the United Nations, is applicable to the use of ICTs by states. We also note Human Rights Council Resolution 20/8 of 5 July 2012, adopted by consensus, which affirms that the same rights that people have offline must also be protected online, in particular freedom of expression.  As the Internet is integral to the conduct of economic transactions and social interactions, it has inevitably attracted criminal activity seeking to manipulate and take advantage of these communications. One pervasive criminal industry that has emerged in the past decade is that of cybercrime perpetrated through malicious software (or malware). While the Australian government is combating this crime through a number of approaches, it is also focusing on reducing the impact of this crime on Internet users through a voluntary government sponsored program - the Australian Internet Security Initiative (AISI). The AISI provides daily alerts to Australian Internet providers of malware infections on their networks, and expects these providers to use this information to identify and alert their customers that their computing device(s) is compromised. The Australian experience to date is that a collaborative approach between the Internet industry, government and consumers is the most effective mechanism to combat malware infections, as it enables flexible and rapid responses to these infections in a constantly changing threat environment. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | The most important issue for the Republic of Belarus is a need to effectively combat and mitigate the results of DDoS attacks. It’s necessary to effectively collaborate between Member-States on this issue. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | In order to promote the use of the internet, Botswana recently finalized the National Broadband Strategy which will ensure roll out of broadband infrastructure and services. The regulator is also continuously keeping track of internet products in the market as well as their pricing and quality to ensure affordability and best experience for the consumer.  Issues of misuse of the internet would be handled by the national Computer Incident Response Team to ensure the internet is used appropriately. The Botswana Communications Regulatory Authority (BOCRA) requires Internet Service Providers to ensure that their networks are secure and monitored to guard against misuse of the internet. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | This issue is provided for in the Penal Code and falls within the competence of the Ministry of Interior |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | *Please refer to Section 5.* |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Legislation of the required laws, as in item (5) above. * Joining the Arab Countries Treaty on Combating Cybercrimes. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has established basic frameworks for this issue and the government has promoted voluntary actions taken by multi-stakeholders.  For example, Inviting Internet users’ attention on these issues:  Regarding illegal access on net banking, the government of Japan requested cooperation for telecom-operators associations to announce to their users to take basic anti-virus measures.  For example:   * The government of Japan participates in private-led voluntary meetings on measures against goods violating intellectual properties, as an observer.   **Actions to be undertaken by governments**  Regarding judging the legality of specific Internet usages, governments should well organize technological aspects of the legality and judge whether those usages are legal or not according to existing laws.  Therefore, regarding the legality, governments should develop national frameworks that can properly judge their legality through multi-stakeholder consultations. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Issues pertaining to the use and misuse of the internet (including protecting children)**   Without doubt internet is an important source of information, education and communication for children and young people. But it also bring threats and risks to children's safety, security and privacy by exposing children not only to harmful, violence and inappropriate content, but also to strangers and pedophiles, who sexually exploit children and expose them to online abuse such as child pornography and child prostitution. The Internet also provides avenue for harassing, stalking and bullying online that threaten the physical and emotional security as well as privacy of the children.   1. **Enhancing Internet Ethics**   Everyone must be aware of and practice Internet ethics so that social problems caused by the Internet can be resolved. Accordingly, the KCC and the KISA operate a youth organization to promote a sound Internet culture, prevent cyber bullying, and enhance Internet ethics. Their ‘Korea Internet Dream Star’ and ‘Beautiful Internet World’ campaigns are conducted every year.  In particular, the “Korea Internet Dream Star”, which celebrated its 3rd anniversary in 2013, selects different topics and targets every year, whereby it helps teenagers to learn Internet ethics for themselves, and use it properly. The Beautiful Internet World campaign is an Internet cultural movement for all citizens intending to create a sound Internet culture. The “Korea Internet Dream Star”, which targets elementary and middle school students who are the future leaders of the Internet society, is a youth organization that was established to develop young leaders who have a sound understanding and appreciation of high ethical values in the Internet society by operating programs that teach proper use and understanding of the Internet. Through the ‘Korea Internet Dream Star’ program, youth can develop their ability to creatively express their thoughts and properly accept others’ opinions, as well as participate in various activities (education, campaigns, experience/exploration, social contributions, etc.) to improve their ability to take the leadership in fulfilling their social responsibilities in the evolving Internet society.  On September 12, 2012, the government hosted its first ‘International Internet Ethics Symposium’ in Seoul jointly with the Korea Society of Internet Ethics to share information on the Internet ethics issues and responses of different countries. At this symposium, not only great scholars of Korea, but also famous foreign scholars in internet were invited. They all gave presentations on the emergence of internet ethics, their necessity, the internet ethics problems of different countries and their responses, and participated in panel discussions featuring open Q&A sessions.   1. **Online Protection of Children**   The diffusion of the Internet enriches the lives of children and youth by providing them with opportunities to access limitless information as well as enjoy a rich cultural life including online education, games, videos and music, but also exposes them to a variety of social dysfunctions and detrimental content. In the online world, children are exposed to an increasing variety of risks that are getting more serious day after day, such as distribution of illegal contents, cyber violence, pornography, online game addiction and online frauds.  To protect children and youth from illegal and harmful contents in the ever changing broadcasting and communication environment, the Korea Communications Standards Commission built its Green I-Net (www.greeninet.or.kr) in 2008, and has since been providing programs to respond to harmful information on the Internet, such as supporting the filtering of information harmful to teenagers, grading information harmful to youth, preventing infringement of cyber rights, and managing Internet information usage time.  The government also formed an emergency response hotline council consisting of 30 Internet service providers like portals, P2P and web-based storage/services to prevent the distribution of illegal and harmful information on the Internet in a bid to monitor obscenities like child pornography. As a result, Internet providers like portals reinforced their monitoring to prevent youth from uploading obscene materials, and conducted strict self-inspection to check whether affiliated contents are legal or not. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | *Please refer to Section 4.* |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) There is a National IPR Committee consisting of BSA members and the US embassy on the promotion of use of genuine software.  • Among the various programs identified is conducting ongoing awareness campaign on the risks of using counterfeit software obtained from various sources like counterfeit software downloaded from illegal sites on the Internet.  • Software piracy rate is about 57% in Mauritius.  (b) Internet Usage Policy formulated in 2009 to ensure that Internet Access provided by Government is used for official/business purposes. Misuse or abuse thereof may slow down the Internet Access meant for rightful business oriented usage. Users are also informed of the security risks of accessing inappropriate Internet contents and the penalties/disciplinary measures that might be envisaged in case of misuse. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **Issues pertaining to the use and misuse of the Internet**  In order to assure safe financial transactions on the Internet, the Law on prevention and fight with money laundering and financial terrorism was enacted on 26.06.2007. Also the National Strategy on prevention and fight against money laundering and terrorism financing for 2013-2017 timeframe and as well as the Action Plan to this strategy was adopted by the Law Nr. 130 from 06.06.2013. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 5.* |
|  | Oman (ITA) [(INF/2)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0002/en) | The Electronic Transactions Law of the Sultanate of Oman has been issued by His Majesty’s Royal Decree 69/2008. The formulation of this law begins a new era for Oman, where a truly e-enabled society evolves in the realisation of the digital society of Sultanate. It is a major milestone in the implementation of the national IT strategy by the Information Technology Authority of Oman. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Issues pertaining to the use and misuse of the Internet**  Internet access is provided by different lenders nationwide. People prefer the use of mobile phone with 3G technology to access the Internet from anywhere. There are also mobile devices with 4G and point to multipoint Wimax technology.  Also there are internet accesses over fiber to the home and HFC systems are available in several cities.  Some good practices and correct use of Internet recommendations can be seen in <http://www.cert.gov.py> |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Issues pertaining to the use and misuse of the Internet**  **a. UKE**[[13]](#footnote-13) **(Office of Electronic Communications)**   * On 11 September 2013, the President of UKE published a **Manual on illegal practices of using telecommunications services and possible measures to protect safety, privacy and personal data when using publicly available telecommunications services[[14]](#footnote-14).** * In 2009, a certification programme of telecommunications services was launched by the Office of Electronic Communications. Between 2009 and 2013 telecommunications undertakings were awarded certificates, including in the "**Fair transfer" category**. The telecommunications undertakings who were awarded certificates in the "Fair transfer" category were obliged to provide transparent and reliable commercial information addressed to their customers as well as transparent procedures for the removal of failures and line verification, accompanied by information to the customer. * In addition, the President of UKE takes numerous information and education measures - during direct meetings with consumers and by means of a Consumer Information Centre[[15]](#footnote-15).   **b. DSI MAC (Department of the information Society, Ministry of Administration and Digitization)**   * Polish government supports all activities which aim to promote better understanding of a digital world among children, their parents and teachers. We encourage the safe use of the Internet and other digital media. In this context NGOs receive support from the government for their activities in the field of child protection on the Internet. Through open public competitions, announced by the Ministry of Administration and Digitalization in the second half of 2013, several projects, which aim at increasing of knowledge and skills in the use of the Internet, received substantial financial support. Various state-founded NGOs and public bodies are also tasked with combating child abuse and removing illegal online material, including child pornography. We are not, however, planning on introducing any sort of general filtering system, as these are expensive to set up and operate, have been proven to be ineffective and easy to circumvent, while often blocking legitimate content in the process. We encourage however the use of end-user solutions to protect minors from exposure to harmful content. * The Polish government supports the development of Internet tools to increase capacity of the public authorities to improve transparency of the decision making process and dialogue with the citizens. We also support easy access to public sector information and we are planning to create user friendly tool for re-use of information that are stored by public authorities. We should work for the Internet to remain a free and unfettered media serving the free exchange of opinions in accordance with the initial assumption of its creators.   **c. PCSS**   * Cooperation was established with a number of secondary and post-secondary schools in the region. Its framework includes lectures for students, their parents, teaching staff, including on the occasions of the Safer Internet Day or school conferences grouping delegations from enforcement agencies, psychologists or those held at the request of teachers.Topics covered include: safe use of the Internet technologies, the issues of the use or yielding to cyberbullying, copyright infringement. Ways to get help are also being indicated. * PCSS elaborated also on the use of modern IT technologies, in particular solutions available via the Internet, especially web pages and e-mail (training publication available free of charge). |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Issues pertaining to the use and misuse of the Internet**  The national Digital Agenda includes actions to reinforce the use of ICTs for social inclusion in order to ensure a broad penetration of technologies and of the Internet economy within the population and to enhance digital citizenship, namely of citizens in remote areas, with low educational levels, elderly or with special needs.  The [Portuguese Safer Internet Centre](http://www.internetsegura.pt/) supported by the EU since 2007 aims at fighting illegal content; minimising the effects of illegal and harmful content; promoting safe use of the Internet; to raise society’s awareness of the risks associated with Internet use. The Centre assures the operation of the hotline ([*Linha Alerta*](http://linhaalerta.internetsegura.pt/)) that receives complaints from any person reporting potentially illegal content on the Internet which, after review by a technical team, are sent to criminal investigation authorities in Portugal or to the INHOPE hotline network for content housed abroad, triggering requests of content removal issued to most of the main Portuguese ISPs with whom there exist protocols. As of 2011, the Portuguese Safer Internet Center also combines a helpline (*Linha Ajuda*).  The Portuguese Safer Internet Centre has regular activities in the form of online safety awareness sessions, seminars, webcasts, media campaigns, lectures and open *fora* and also promotes and supports specific campaigns (yearly national campaigns in schools and other dissemination networks) at certain times namely during the Safer Internet Day, the World Telecommunication and Information Society Day. The component of the project SeguraNet promotes awareness raising activities in schools and the educational community. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | One of the very important topics in misuse of Internet is DDoS attacks and other attacks on Internet resources.  It is needed to elaborate regulation and practice at national level as well as interaction at international level in order to effectively counter attack, identify attribution of the source of the attack, and define responsibility for damages, including cooperation authorized national CERT/CSIRT  Based upon broad public consensus, the Russian Federation adopted laws and decisions about blocking sites containing child pornography, drug and suicide propaganda. Nowadays, our experience shows that foreign companies are taking the necessary steps and measures. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Issues pertaining to the use of the Internet**  Rwanda has clear policy and strategies for the development and usage of Internet services. As of September 2013, the number of Internet subscriptions is 1,674,053 which represent the Internet penetration rate of 15.8%. This shows an increase of 26.4% as compared to the second quarter of year 2013. This increase is mainly due to the widespread of use and adoption of Internet services, availability of content and applications accessible and affordable by low income population. There is an increasing use of online services and popular social media networks especially by young generation.    **Source**: RURA Report Q3,2013  **Figure 2**: Rwanda Internet penetration as of September 2013 |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  A. Develop international public policies to deal with misuse of the Internet and to prosecute those that deliberately misuse the Internet.  **Actions which have been undertaken by Governments**  A. A number of countries have national policies and laws related to use and misuse of the Internet, but they are not coordinated with international public policy since there is no mechanism to develop such policy. |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | The Sudanese CERT (cert.sd) was established by NTC to undertaken these issues. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Issues pertaining to the use and misuse of the Internet**  There is no international public policy issue under this heading that is not dealt with under the two preceding headlines. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | On 27 June 2012 the Federal Council approved the «National strategy for Switzerland's protection against cyber risks».  <http://www.isb.admin.ch/themen/strategien/01583/index.html?lang=en>  The Federal IT Steering Unit ensures implementation of the ICT strategy of the Federal Council. Their Plan focuses on the years 2013 and 2014 and defines 20 milestones and assigns responsibilities to organization units within the federal administration. More information can be found at:  <http://www.isb.admin.ch/themen/strategien/00070/index.html?lang=en> |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | *Please refer to Section 4.* |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Issues pertaining to the use and misuse of the Internet**  Please see our response the sections above on “The security, safety, continuity, sustainability, and robustness of the Internet” and “Cybercrime.” |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - Local multi-stakeholder working group on e-commerce issues.  - Several laws and regulation on Internet use and misuse.  - Consumer Protection Act applies to online local transactions as well. Uruguay is Vice-Chair of eLAC working group on consumer protection  - Distribution of information in public web sites according to the Free Software and Open Format for the Government Act.  - Public software portal.  - Also see answer to issues 4, 5,11 and 12 |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Issues pertaining to the use and misuse of the Internet**  The government through the regulator has embarked on establishing ICT clubs schools. So far 100 ICT school clubs have been established across the country. The objective of the ICT Clubs is it to educate pupils on online risks and vulnerabilities.  The regulator has been conducting Child Online Protection (COP) quizzes on the National Television and social media platforms. The quiz questions are based on Child Online Protection and cyber security issues.  The regulator has produced COP materials in form of brochures, booklets, radio and TV adverts. The COP material has focused on the following: sexting, identity theft, digital reputation, identity theft and parental advice. The objective is to protect children from illicit and harmful content. The adverts are running on National Television and Radio stations.  The regulator has partnered with the National Television Broadcaster in the production and airing of national debate. The debate focuses on ICT related topics as well as Child Online Protection, use and misuse of the Internet. In this year’s programme, secondary schools from neighbouring countries like; Zimbabwe, Botswana, Namibia and South Africa have been invited to participate.  The regulator conducted a research on illicit and harmful content. The results of the research are yet to be finalized. The regulator will develop a comprehensive national COP strategy based on evidence from research carried out.  The Regulator will soon embark on a nation-wide awareness campaign focused on training the teachers; so that they can effectively be ambassadors of “Safe Internet Usage”. |

# **Availability, affordability, reliability, and quality of service, especially in the developing world**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**  Reliability and quality of service continue to be very important aspects of consumers’ use of communications services.  Quality of service (QoS) has historically focused on the technical attributes of end-to-end service provision – especially for voice services. However, consumers increasingly have an expectation of a broader ‘quality of experience’, which includes not only the technical quality of the service, but also minimum (and consistent) download speeds and access to ‘value added’ broadband applications and services.  There is currently a wide array of VoIP services currently on the market, and end-users can choose different VoIP services on the basis of price, technical quality and other functional aspects.  There is ongoing work in the ITU-T to develop end-to-end technical performance requirements for VoIP and other services (including data services).  It should be noted that the technical parameters for ‘carrier grade’ VoIP derive from the quality of service parameters for circuit-switched voice services developed originally by the ITU, and which are contained in ITU-T recommendations. There is also working being undertaken in other standards development organisations (SDOs), including the Internet Engineering Task Force (IETF) and the European Telecommunications Standards Institute (ETSI) on IP quality of service and associated technical activities.  To assist end-users in making informed purchasing decisions, Australia supports the development of objective technical criteria that can be used by suppliers of communications services to describe the technical capabilities (and limitations) of those service. To that end, Australia supports the continuation of the ITU-T’s QoS technical studies for both voice and data services, working in close collaboration with other SDOs including IETF and ETSI.  However, such technical studies should not unnecessarily limit the scope for innovation in the market, especially in the development of communications products and services.  Australia has funded a range of projects in the Asia-Pacific region with the aim of improving availability, affordability, reliability and quality of service, including for example, an ICT infrastructure project in Solomon Islands, where in conjunction with the World Bank, Australia supported the establishment of a Telecommunications Commission and the issuing of a second mobile telecommunication license. This financial assistance resulted in an increase in mobile phone coverage, a reduction in mobile calls costs and an increase in the number of mobile phone subscribers in Solomon Islands. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | We find it reasonable to perform active regulation aimed on improving quality of services by introducing technical parameters, their norms and methods of control. Moreover, it’s necessary to update legislation with focus on consumer right protection.  In order to make BB more available for all kinds of population it’s reasonable to develop and follow national BB plans. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | In order to ensure universal access, provision of affordable, reliable and quality ICT services, Botswana is in the process of establishing a Universal Service Fund in order to deploy services for all including unserved and underserved areas.  In ensuring internet access for all, Botswana is in the process of implementing the national Broadband Strategy, which aims at among others; upgrading the networks, capacity building, development of local content and providing connectivity in rural and underserved areas.  The regulator also keeps track of pricing of market products to ensure they are affordable. The Authority has completed the Quality of Service guidelines that service providers have to adhere to and also in the process of obtaining monitoring equipment for both voice and data. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | Nowadays in Bulgaria there are more than 600 enterprises on the broadband services market, which is the necessary prerequisite for availability, affordability, reliability, and quality of service.  As already mentioned above, this is an area where Bulgaria has positive achievements and its experience should be widely shared, including with the help of the ITU. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world** Access to Information and Communications Technologies has a considerable potential in securing access to information and basic services for the world’s poor populations. The Strategy for Denmark’s development cooperation “The Right to a better Life” identifies access to ICT as an important element in ensuring the population in Danish partner countries, including poor and marginalized population groups, access to information and influence on matters affecting their life and thus the ability to participate in democratic processes. Furthermore access to ICT can contribute to innovative ways of ensuring access to basic services.  Example: In Kenya Danida is supporting, in cooperation with Grundfos and IFU, establishment of so called LifeLink systems ensuring access to clean drinking water. The system is made up of solar powered water pumps, a remote monitoring system ensuring maintenance, and a mobile phone based pre-payment system. The project delivers clean drinking water to at least 27.500 citizens and at the same time collects valuable information on patterns of consumption use for the further development of the system. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | • Lowering the price of capacities provided to ISPs to minimum possible price (the price of the cost).  • Providing the service to all Iraqi provinces and cities.  • Increasing competition in providing the service by granting licenses to the maximum suitable number of ISPs.  • Building FTTH networks in all Iraqi cities. Some of provinces completed their work in this regard.  • Lowering the price of domain names under the Iraqi domain name (.iq). |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has undertaken to conduct ODA projects in the field of ICT, such as technical cooperation and establishment of ICT infrastructure and to implement international cooperation, such as capacity building, best practice sharing, and cooperation towards literacy improvement and awareness-raising activities, in cooperation with other stakeholders, to developing countries.  **Actions to be undertaken by governments**  For the affordability of the Internet, governments are encouraged to support the reduction of prices for ICT networks, and services should be evolved by the further liberalization of the telecommunications market, enhancement of competition, and promotion of investment.  Taking account of the recent increase in penetration of mobile communications in developing countries, it is effective to implement policies that realize broadband communications with mobile communications and expand mobile services corresponding to broadband mobile communications. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Availability, Affordability, and QoS in the Developing Countries**   This section is not applicable to this summary report. |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) The ICT Authority is the Controller of Certification Authorities and has set up the Public Key Infrastructure. To encourage the take up of PKI for the benefit of e-commerce, the ICT Authority has published an Information Guide. The Authority is now embarking on the setting up of an e-Commerce Framework, whereby a Seal of Trust will be issued to e-traders and businesses to safeguard the consumer interest and encourage e-Commerce in a safe and secure environment.  (b) In line with the National Broadband Policy 2012, the ICT Authority is proposing a Quality of Service Framework tailored for broadband Internet service provided using wired, fixed wireless access and mobile access. The framework will cover service coverage, availability, service quality and reliability, adequate and equitable bandwidth access to consumers in Mauritius. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **AFFORDABILITY AND ACCESSIBILITY OF TELECOMMUNICATION SERVICES in Kingdom of Morocco**  Since it has been liberalized in 1998 by the law 24-96, the Moroccan telecommunications sector has known a radical change, ending the monopole of "Itissalat Al Maghrib" and establishing the principle of competition in telecommunication services to citizens.  This change, embodied by an unprecedented development, since the size of the market and services have been greatly improved, has been made in accordance with legislative and regulatory rules predefined, ensuring both fair competition between all operators of public telecommunications networks and providing a minimum service of specified quality at affordable prices and, on the whole national territory and all layers of the population.  In order to make available and accessible telecommunication services to the entire population, regardless of its geographic location, the Moroccan legislator has ensured, through law 24-96 and its implementing texts as amended and completed, the principle of universal service is to impose to the all operators of public telecommunications networks to provide or fund the missions and the resulting costs.  **Content of the universal service**    The furniture of universal service of telecommunication is now based on the following elements:   * Enlargement of the scope of the universal service, initially limited to a basic telephone service, to enclose a telecommunications service including a telephone service either fixed or mobile, missions of space planning and value-added services, including Internet access; * Establishment of an interministerial committee called the "steering Committee of the Universal Telecommunication Service (CGSUT)" primarily responsible of definition and validation of programs to implement universal service to cover all localities with no telecommunications services, called "white areas" or those poorly served; * Creation by the Finance Act 2005, of a fund in the form of special account called the "Universal Telecommunication Service Fund" (FSUT) for receiving financial contributions by the telecommunication operators and for financing universal service programs approved by the CGSUT, by awarding financial grants to operators responsible for carrying out such programs; * Definition and clarification of the specific rules for implementing the universal service obligations by operators of public telecommunications networks, particularly in establishing the principle of "pay or play" , "fund or carry out", which gives the choice to the operator, either to achieve universal service projects, or pay the contribution they are due to the FSUT for each year.   The expansion of the scope of the universal service was made necessary by the increase of use of certain mobile and Internet services, and the willingness to put our country in the global information society and knowledge. The scope has been extended to following aspects:   * A telecommunication service, including telephone service based on a specified quality at affordable prices; * Mandatory services, including the routing of emergency calls, providing an information service and a telephone directory in printed or electronic form; * Services related to space planning, which are now an integral part of the missions of universal service. These services are no longer limited to a fixed conception of traditional goals of serving the national territory with "telephone boxes", as they now include the service coverage for the peripheral urban areas, industrial areas and rural areas by means of telecommunications ; * The value-added services, including services for Internet access.   **Universal service Steering Committee in charge of the Universal telecommunication Service (CGSUT)**  In order to efficiently manage the universal service and make it part of a coherent and integrated government strategy, an interministerial committee responsible for the management of the universal service for telecommunications (CGSUT) was established.  This Committee, chaired by the Head of Government is composed of the following members:   * The government authority responsible for the interior; * The government authority responsible for the planning; * The government authority responsible for finance; * The Government Telecommunications Authority; * The government authority responsible for national defense * Chairman of the Management Committee of the ANRT; * The Director General of the ANRT.   ANRT is the permanent secretariat of this committee.  This Committee is responsible for:   * Defining the main objectives and priorities for the development of universal service. These priorities are expressed, especially in terms of services and facilities to be provided and / or area to be served; * Identifying the annual and / or multi-year programs for the implementation of universal service in the country and in accordance with the priorities he has learned; * Suggesting, for each call up the contents of the universal service in accordance with the provisions of Law 55-01 amending and supplementing Law 24-96 as above; * Approving the draft specifications for competitive bidding for the achievement of universal service programs adopted by the Committee.   ***Funding of universal service obligations***  The universal service funding is provided by the FSUT fund established for this purpose by the Finance Act 2005. This Fund is endowed by contributions from telecommunication operators up to 2% of their turnover excluding tax, net of interconnection fees, sales of terminals and of the payouts for value-added services suppliers.  The fund may also receive any contribution in the form of donations and bequests allocated by international organizations or in the development programs of universal telecommunications service.  The revenues of FSUT funds are intended to finance programs and projects approved by the universal service CGSUT.  ***Mechanisms for carrying out the missions of the universal service.***  The mechanism of "pay or play" chosen by the Moroccan legislator, offers to the existing operators two possibilities: to participate in carrying out the tasks of universal service. The operator can contribute to the missions and costs of universal service either by making financial contributions to the universal service fund, or by implementing the universal service programs approved by CGSUT .  The operator who chose to achieve by themselves the tasks of universal service, may submit to the appreciation of CGSUT, their proposals for universal service programs. In the case where these programs are approved by the CGSUT, the operator will carry out these programs under the conditions set by the committee and according to particular scope statement.  Regarding the programs defined by the CGSUT, a call for competition is organized. This call for competition, to which both existing operators and new entrants may participate, is intended to choose the operator which will be in charge of carrying out those programs, based on the best technical and pricing offer and in consideration of the lower financial contribution requested.  **Universal Service projects for the deployment of the covering network**  Since its creation in July 2005, CGSUT has approved several universal telecommunication service projects conducted by existing telecommunication operators. These projects aim to cover digital divided rural localities/rural villages with required telecommunications infrastructure and services.  The table below describes the universal service projects whose realization was entrusted to the operators for the period 2005-2007:   |  |  | | --- | --- | | **Project** | **Objectives** | | Renovation of the rural service in Fixed line, ADSL and CDMA | * 159 rural localities connected to ADSL * 826 rural localities connected to internet via CDMA-450 | | Mobile coverage in rural area | Coverage of 243 rural localities with GSM technology | | Strengthening the GSM network | Strengthening the coverage of 40 rural localities | | Initiative of rural public telephony | Deployment of 42 Computer Access Centres (CAC)  For phone services in the major souks of Morocco | | Internet coverage in rural area | Furnishing the fixed network of 207 rural localities with the necessary equipments to provide Internet service via ADSL technology | | Extension of the GSM coverage to remote areas :  Installation of Computer Access Centres (CAC) | Coverage of 184 rural localities with GSM technology and VSAT |   In 2007, and in order to have the global information about not covered rural localities, the CGSUT required the census of all rural localities/rural villages that were not covered by telecommunication services (voice and data) , called "white areas", and decided to launch a consultation with all existing operators, in order to ensure coverage of these locations.  Therefore, the census identified 9263 rural localities/rural village not covered by telecommunication services. A program has been defined to cover these areas and was named "PACTE " program.  PACT program was running with the participation of operators acting in fixed, mobile and Vsat telephony markets.  The state of progress of « PACTE » program at 31st December 2013 is as follows:   |  |  | | --- | --- | | **Items** | **%** | | Covered localities (rural villages) | 90,5 | | Localities in the process of covering | 7,4 | | Localities with electrification issues | 0,9 | | Localities with land acquisition issues | 1,0 | | Localities with operational difficulties for its coverage | 0,2 | | **Offered services are using GSM (2G) EDGE, 3G, and Vsat (for Community access Centers)** | |   The implementation of the PACTE program, expected during 2014, will allow all populated rural areas of the Kingdom, to be provided by a basic telecommunications service. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | **DEVELOPMENT: Availability, affordability, reliability, and quality of service; developmental aspects of the Internet, and contributing to capacity building for Internet governance in developing countries**  Transport and Communications Infrastructure, specifically improving connections for the Pacific to modern communications services, has been identified as a sector priority for the New Zealand Aid Programme (NZAid). NZAid is working in conjunction with the World Bank and other partners to provide support for connecting the Pacific to modern communications.  Capacity building activities relating to cybercrime and network stability are addressed above. |
|  | Oman (TRA) [(INF/10)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0010/en) | TRA launched an operational scalable registry system for the .om ccTLD and (.oman) Arabic IDN. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**  The parameters of quality of service, availability, reliability and accessibility were partially implemented. Ways to improve the process of measuring these parameters are explored, so that the regulatory agency (CONATEL) in Paraguay performs an upgrade in its parameter list.  In Paraguay a Universal Service Fund is used to access internet in squares and public spaces; Fiber Optic Infrastructure to rural communities and access to Mobile Phones. |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**   * 1. **UKE** * The President of UKE published its **Final Report on the outcome of work on identification of quality of service indicators** which was developed as part of the **Memorandum for improving the quality of telecommunications services** as a document drawn jointly and agreed between the Memorandum Leader (the President of UKE) and 44 Signatories to the Memorandum on Quality (telecommunications undertakings, service providers, measurement companies, scientific bodies and consumer organizations). All Signatories committed themselves to jointly strive for ensuring reliable and comparable information about quality of service (QoS) indicators for consumers[[16]](#footnote-16). * In order to launch measurement campaigns and further operations a **Steering Committee for Mobile Network Measurements** will be established in early 2014. It will be composed of telecommunications undertakings affected by the measurements (operators providing services in mobile networks) and the Office of Electronic Communications on equal footing. The first measurement campaign is planned for 1st half of 2014. Such measurement sessions are planned twice per year. UKE will have supervisory functions over these measurements. The measurements will be conducted by an independent entity (a measurement company). The choice of a measurement route should take account of population distribution patterns, traffic patterns and the area of service provision. The minimum duration of the measurement campaign is 800 hours. At least 80% of the measurements will be conducted in motion. * UKE conducts **permanent quality tests for telephone calls** in PSTN, calls from PSTN to GSM networks and fax over PSTN, using the AWP-IŁ system (some 1000 probes). * UKE has 4 ROMES (Rode&Schwarz) measurement sets for the assessment of quality of service indicators for voice and Internet access services over mobile networks. UKE conducts periodic measurements in large cities, on domestic highways and railway routes. * UKE has an nGenius system for the measurement of availability and quality indicators in IP networks (measurement probes are installed at border routers of service providers). * In 2014, UKE plans to implement a project aimed at developing a reliable IT tool for end-to-end measurement of broadband network parameters. UKE will make the System for Internet Quality Measurement (SMJI) available to Internet end users (clients) and the results of these measurements will be sent and stored in the SMJI in order to prepare reports and visualise measurement outcomes on a digital map of Poland. * To ensure maximum benefits for users in terms of choice, price and quality of telecommunications services as well as effective and transparent enforcement of the obligation to publish information on the quality of publicly available telecommunications services (QoS), the **President of UKE published reports on the quality of service indicators for publicly available telecommunications services**. The purpose of quarterly publication of indicators for the networks of the tested undertakings is to compare the quality of services provided by individual operators for different types of such services (telephony, fax, data transmission) in fixed-line (PSTN) and mobile (GSM) networks. This information may be useful both for consumers when choosing their provider of telecommunications services and for telecommunications undertakings in order to improve the quality of their network operation[[17]](#footnote-17). * As regards affordability of telecommunications services, the President of UKE published the **Position of the President of UKE of 19 July 2010 regarding the control of compliance with certain regulatory obligations, including assessment of price lists and rules and regulations of service provision, by the operator with significant market power in the retail market**. The purpose of this Position is to present the basic rules applied by the President of UKE in enforcement of regulatory obligations imposed on the undertaking with significant market power in retail markets, including price obligations[[18]](#footnote-18). * As regards availability and affordability, the President of UKE presented on 16 October 2012 a **Report on ensuring individual services comprising universal service by the market after expiration of the relevant obligation imposed on the designated operator** (i.e. after 8 May 2011). The document presented makes an assessment of the availability and affordability of services comprising universal service[[19]](#footnote-19). * As regards affordability of telecommunications services, the President of UKE in 2009 launched a certification programme of telecommunications services aimed at supporting equal and effective competition in the provision of telecommunications services - for the category "Offer comparison website." The certification programme of the President of UKE in the "Offer comparison website" category is addressed to entities operating in the telecommunications sector which provide price benchmarks for a wide range of telecommunications services.   1. **PCSS** * There is a number of cutting-edge services to the PIONIER network that make it go beyond a standards level of commercial networks. These include applications allowing for advanced DVC sessions, dispersed calculations, universal hard drive, huge-scale calculations, etc. Those tools provide the academia with more access to and reliability of better quality networks. * PCSS is closely cooperating with leading manufacturers of IT and measuring equipment. The joint efforts and solutions may have the potential for being implemented in final products making their way to the market.   1. **NASK**   Introduction of the Registry-Registrar system of partnership with entities representing domain subscribers, which allows them to be approached with the NASK’s wholesale offer. That in turn works for the end user who enjoys more choice on the market both in terms of pricing and quality. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**  Please refer to section 2. |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world:**  Amongst the various missions of ictQATAR Regulatory Authority,  it has to ensure that telecommunications services, including the internet, are available, affordable and offered with a high quality of service in all the state of Qatar.  MICT has also developed a program offering internet connectivity to the public, free of charge, in several parks throughout the country. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Adoption of national programmes on broadband access development aimed at both transport network and access network infrastructure development and ensuring quality of service and affordability, especially in remote and sparsely populated areas, and furthering the work jointly with private sector to improve computer literacy. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Availability, affordability, reliability, and quality of service**  The following actions were initiated in the line of ensuring the provision of quality service:   * Development of appropriate standards and guidelines for the setup of networks, operations and provision of Internet services to end users. * Acquisition of Quality of Service (QoS) Monitoring Toolsto measure the Quality of Service (QoS) of Broadband Internet provided by ISPs. * Spectrum Monitoring System: A system was put in place to monitor and inspect the use of radio-communication frequencies for efficient use of scarce resources. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**   1. Enact national and regional regulation promoting competition.   B. Promote network rollouts and participate in funding as appropriate.  **Actions which have been undertaken by Governments**   1. Most nations have established policies and/or independent regulators charged with the responsibility for promoting competition. 2. Though there are some efforts to provide funding support for network rollouts in developing and less developed countries, there is no clear public policy or consistent mechanism for making this happen. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**  International organisations such as OECD, ITU-D have a role into facilitating effective markets and deployment of broadband of increasing capacity in the developing world. Likewise, development agencies, such as the UNDP and the World Bank have a role in contributing to the establishment of infrastructure and policies conducive to growth and innovation in low- and middle-income countries. Several new important initiatives, such as the Alliance for Affordable Internet, are also tackling the underlying issue of anti-competitive and restrictive policies. This is an issue dealt with under WSIS Action Line 2 and 3 and could become an important part of the governance discussions of the post-2015 Development Agenda.  IPv6 is one important issue for availability where Sweden has been active on the international level within RIPE as well as within the ITU IPv6 group. We have translated our guidelines to be able to spread them through ITU and other fora to support the uptake of IPv6. Sweden has promoted the usage and uptake of DNSSEC on a local, regional, national and international level to increase the reliability of DNS. Private Swedish internet companies is working actively with setting up IXP:s in developing countries and exchanging best practice.  See also the reply on international internet connectivity. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | The UK, through its Department for International Development (DfID), has sponsored a number of activities in looking to make ICT services in developing countries more affordable and reliable. For instance, DfID has been a partner in the following schemes:  [Alliance for Affordable Internet](http://a4ai.org/)  [Private Infrastructure Development Group](http://www.pidg.org/) [Public Private Infrastructure Advisory facility](http://www.ppiaf.org/)  [Web Index](http://www.webfoundation.org/projects/the-web-index/)  However, the UK recognises that there is still a long way to go to ensure that all citizens in developing countries are able to access affordable and reliable ICT services in the future |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**  To promote widespread affordable access to the Internet, governments must enable policy and regulatory environments that are fair, transparent, stable, and predictable. Policies should promote competition, support innovation in technologies and services, incorporate education and training programs, incentivize private sector investment, and address market failure when necessary. These are the conditions that led to the Internet we have today, and these conditions must be maintained to ensure that we see continued technological innovation, diversification of services, and connectivity and access for all. A high priority is fostering an increasingly educated and skilled workforce around the world so that the developing and least developed countries can find ways to become creators and suppliers of Internet services, applications, content, and code.  In addition, the policy recommendations for encouraging broadband infrastructure development contained in the ITU/UNESCO Broadband Commission for Digital DevelopmentReport can also contribute to more affordable Internet connectivity in developing countries. The recommendations are for governments to:   1. Provide policy leadership for investment, including open consultations on necessary policy and legal frameworks; 2. Open telecommunications markets to competition through transparent licensing regimes, opening up international gateways, and taxation reforms; 3. Enable government services that will stimulate demand for and investment in telecommunications, especially in developing countries; 4. Establish a universal service program to support broadband infrastructure investment and to eliminate the access gap; 5. Develop National Broadband Plans; and 6. Encourage efficient and innovative mobile broadband practices for new market entrants and consumers.   These recommendations warrant additional observations. Internet Exchange Points (IXPs) enable local ISPs to connect directly together and exchange domestic traffic, typically with settlement-free peering, thereby reducing or eliminating tromboning[[20]](#footnote-20) and saving cost on international transit while reducing latency by avoiding local traffic to be carried internationally. Additionally; the increase in traffic at the IXP creates incentives for content providers to place their content closer to end-users by installing content caches or creating more direct routes to server hosts. Establishing IXPs would help change the business environment for local connectivity allowing services to be located closer to the users, potentially at lower cost. In some countries, domestic policies may contribute to the high cost of international Internet connectivity, for example, in markets in which high international leased circuit prices are caused by lack of competition and liberalization.  An additional key issue is the adoption of effective Universal Service and Access Funds (USAFs) by government, and the adoption of newer technologies by commercial carriers. Combined, these provide an incentive to expand to reach rural populations through less costly solutions. Often over 50% of the population in many countries is rural; these rural populations are both expensive to serve and often have limited financial resources to afford access. A number of international entities are available to assist governments in addressing affordability issues. For instance, the Internet Society (ISOC) provides training and assistance on developing and maintaining IXPs, which can improve service quality and reduce interconnection costs.  The Alliance for Affordable Internet is a coalition of private sector, public sector, and not-for-profit organisations who have come together to advance the shared aim of affordable access to both mobile and fixed-line Internet in developing countries. Its primary goal is to realize the UN Broadband Commission’s Broadband Target of entry-level broadband services priced at less than 5% of average monthly income realised. In working towards this vision, the Alliance seeks to assist many more users to come online with a particular focus on low-income countries. In particular, the Alliance has facilitated South-South dialogue to share expertise, best practices, and success stories. Also on a practical level, the Alliance has produced an outline of policy and regulatory best practices aimed at driving down the cost of internet access that is readily accessible online (<http://a4ai.org/policy-and-regulatory-best-practices/>).  TheAfrican Peering and Interconnection Forum addresses the key interconnection, peering, and traffic exchange opportunities and challenges on the continent and provides participants with global and regional insights for maximizing opportunities that will help grow Internet infrastructure and services in Africa. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - Universal Access Plan that includes 1GB of traffic per month without cost by the state owned Telecommunications Company.  - FTTH project that is bringing fiber connections to every home, though the state owned Telecommunications Company.  - Deployment of Internet in Rural areas though the state owned Telecommunications Company.  - OLPC Plan (“Plan Ceibal”) for school and high school students, including Internet connectivity to public education centers provided by the state owned Telecommunications Company.  - Several connection plans for business, education and home, with the lowest MB price in Latin America.  - Traffic to educational and government local websites free of charge for the state owned Telecommunications Company’s customers.  - Quality of service- At the domestic level: Rules of Quality of Service-Experience (QoE-QoS) in process. At the regional level: standardization of method and parameters. At the international level: trend analysis.  - Spectrum planning for future deployment of new wideband mobile networks. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Availability, affordability, reliability, and quality of service, especially in the developing world**  The Government through the Regulator (ZICTA) has put in place Quality of Service Guidelines which provide for minimum standards of quality of service as well as the set parameters/targets that service providers must meet. The Guidelines were revised in June 2013 to streamline enforcement procedures.  The pervasive nature of mobile internet has drastically reduced the cost of Internet in Zambia, while improving the availability, reliability, and quality of service. However, much improvement is expected from the service providers of both traditional Internet Services and the Value added service providers. |

# **Contributing to capacity building for Internet governance in developing countries**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Contributing to capacity building for Internet governance in developing countries**  The way the internet is governed will be important in shaping future economic and social developments. However, for many developing countries participating in internet-related policy processes presents a significant challenge. The Australian Government is supportive of measures aimed at enabling the effective participation of developing countries in internet governance, such as ICANN’s Fellowship Program and its ongoing development of regional engagement strategies. The Australian Government looks forward to working with ICANN and regional partners in the development of ICANN’s Oceania engagement strategy during 2014. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | Constant study courses update in academia is required along with staff training taking into account business needs. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | The country is working into creating a national Internet Governance Forum where all issues regarding the internet will be discussed.  There is limited activity regarding Internet Governance in Botswana as a developing country as there is limited participation by the country on Internet Governance Forums. This could be attributed to lack of a National Internet Governance Forum. However, Botswana through the Botswana Information Technology Society (BITS) has been doing some works in relation to internet governance and capacity building through conducting workshops every year. |
|  | Brazil [(INF/38)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0038/en) | **Contributing to capacity building for Internet governance in developing countries**  During the World Telecommunication/ICT Policy Forum (WTPF-2013) Brazil presented a draft opinion entitled "Operationalizing the role of government in the multi-stakeholder framework for Internet Governance", that points to the fact that we must together address two key issues: operationalizing the role of government in the multi-stakeholder framework for Internet Governance, and the need for capacity building on these issues in developing countries, particularly in the least developed countries, with the support of the ITU. The draft opinion presented by Brazil received significant support during the plenary sessions of Working Group 3 of the WTPF. Although not adopted, there was agreement that the issues should be further pursued within the ITU, as reflected in the WTPF Chairman’s Report.  Following on this recommendation, at the recent **Regional Preparatory Meeting for the Americas Region for WTDC-2014** Brazil submitted a contribution proposing that the ITU take a leading role in establishing a capacity building program for developing countries, and particularly for the least developed countries, in the area of international Internet Governance. This initiative is consistent with the role assigned to ITU, as one of the co-facilitator agencies for Action Line C4 - Capacity Building**,** of theGeneva Plan of Action of the World Summit on the Information Society (WSIS).  This contribution from Brazil is available at <http://www.itu.int/md/D10-RPMAMS-C-0008/en> |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | We are not sure what this means – Internet governance would not need capacity building and contributions, it is more into the line of a Government to provide the appropriate conditions for competition. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | Holding many training courses and workshops about internet networks in the Iraqi Academies and in the Sate Company for Internet Services, which is a governmental body. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has implemented ODA projects regarding human resource development in the field of ICT. The government also has implemented international cooperation, such as capacity building, best practice sharing, and cooperation towards literacy improvement and awareness-raising activities, in cooperation with other stakeholders, to developing countries.  **Actions to be undertaken by governments**  The government will continuously implement international cooperation, such as capacity building, best practice sharing, and cooperation towards literacy improvement and awareness-raising activities, in cooperation with other stakeholders, to developing countries.  Recently, ways to learn without charges are increasing on the Internet. For example websites like the “MOOC (Massive Open Online Courses)” are expected to bring a new opportunity to learn for developing countries. It would be effective for governments to offer information and support implementation on these helpful mechanisms through multi stakeholder model. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Contributing to Capacity Building in Developing Countries**   As Korea has been undergoing successful industrial development and informatization, Korean government is concentrating on spreading the power of ICT industries and sharing the knowledge with a global community. The main activities are focusing on digital switchover, information security, and spectrum management system  Korea has been implementing the ICT Development Consultation Program with the aim of promoting and ensuring digital opportunity in many countries. As a leading ICT think tank for the Korean government, KISDI has taken part in Korea’s ICT Cooperation Projects since 2002 with the support from the Ministry of Science, ICT, and Future Planning (MSIP). The ICT Development Consultation Program includes ICT Policy Consultation Project and ICT Advisory Mission Project where 31 ICT Policy Consultation Projects and 15 Advisory Missions have been successfully completed in 22 countries since 2002. In providing prompt and immediate solutions to the partner country’s needs, assigned experts with practical expertise deliver the knowledge to other countries.  The National Information Society Agency (NIA), a subsidiary organization under the Ministry of Science, ICT and Future Planning (MSIP), has tried its best in its mission to develop Korea into an information-oriented society and to reduce information gaps between individuals both domestically and internationally. Since 2002, NIA has carried out Information Access Center (IAC) project providing better access and opportunity to use ICTs for the general public in developing countries, thus contributing to improving the IT environment as well as cooperation in the ICT field. Its major task is to exchange human resource and digital contents and to establish a regional networking community share ideas and experience for sustainability and development of IAC.  A different pillar of capacity development activities for the developing countries is supporting improvement in the broadcasting environment. The International Telecommunication Union (ITU) has recommended the world to complete digital television transition by 2015. With success in completion of transition from analogue to digital TV at the end of 2012, Korea aims to share its know-how and first hand experiences on cost and time saving strategies with other countries by establishing a cooperative network with international broadcasting organizations such as Asia-Pacific Broadcasting Union (ABU), Asia-Pacific Institute for Broadcasting Development (AIBD) and ITU. Besides, South Korea plans to help these countries to reduce their burdens in completely replacing the existing analogue broadcasting equipment with digital ones.  The last one is to provide an IT specialized training. K-LINK(Korea Leader’s Information Network) is an ICT expert training program presented by KISA(Korea Internet & Security Agency). The ultimate goal of K-LINK is to assist broadcasting & telecommunications experts to get insight on policy making for growth and to implement advanced policies. We believe this program will be useful to all participants and their countries ICT development. The program for K-LINK is comprised of Broadcasting, Communication, Radio Frequency, Convergence and Information Security Technology and Policy.  Aside from the K-LINK, Korea ICT Learning (KoIL) program also invites policy makers, public officials, and experts in the ICT field to share the newest technologies and issues to be reflected on national policies and plans in order to address their social and economic challenges of using ICT tools. Participants at KoIL courses learn ICT development strategies, discuss current issues and trends, and seek means of cooperation to advance their nations' strategies on e-governance and new technology adoption. On-site courses are also available to better reflect each nation’s demands and circumstances. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | *Please refer to Section 2.* |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 8.* |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Contributing to capacity building for Internet governance in developing countries**  The e-government begins to be implemented in Paraguay, so tax returns, requests for documentation, etc. can be performed at the government sites. International agencies helps to implement short-term plans within the e-government mode to other institutions of Paraguay so that people can sign up, doing paperwork, applications in various areas of negotiations with the possibility the state to concentrate on a single Data Center.  The Paraguay through CONATEL ([www.conatel.gov.py](http://www.conatel.gov.py)) follows with great interest the issue of Internet Governance at different international forums. |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Contributing to capacity building for Internet governance in developing countries**  No contributions received |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Contributing to capacity building for Internet governance in developing countries**  Portugal supports regular yearly sessions and workshops under the Internet Governance Forum (IGF) on capacity building and individual empowerment. In particular, Portugal foresees to develop specific actions with Portuguese speaking African countries and other African countries in collaboration with the African Union Commission on this area. |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | **Contributing to capacity building for Internet governance in developing countries :**  MICT is supporting the Arab Internet Governance Forum “AIGF” and actively participating to the Global Internet Government Forum “IGF”.  Recently, an Internet Society chapter has been established also. It will represent the voice of the Qatari internet users community in the multi-stakeholder development of Qatar future Internet Policy. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Notes the importance to eliminate all formal and informal barriers to the participation of governments in particular those of developing countries - in international public policy issues pertaining to internet, to ensure equal possibility for economic development and capacity building of international telecommunication networks including international Internet infrastructure in developing countries.  Aspects ensuring capacity building could cover:  - government actions to support capacity building measures and stimulate industry development;  - professional development, attracting leading universities, together with other organizations of the Internet community establishing new courses and learning programs;  - transfer to electronic document for state bodies and public authorities associated with corresponding actions towards increasing open data and greater openness of public authorities and more accessible government. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Contributing to capacity building for Internet governance**  The capacity building is the cornerstone in the building of the information knowledge based society and the GoR recognised that in its vision 2020. It is in that framework that in every phase of NICI plan the capacity building is an important component and ICT has been introduced as a tool and discipline in all programs from primary to higher education.  The current NICI III plan (2011 - 2015) focus on content and application development and it is in that framework that new institutions such as Knowledge Laboratory (K-Lab) and Africa Digital Multimedia Academy (ADMA) have been created to target specific applications to meet the market needs. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  A. Propose and support related initiatives, including with expertise and funding.  **Actions which have been undertaken by Governments**  A. Existing efforts could be enhanced by developing supporting international public policies, but there is a need to develop such policies on an international level. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Contributing to capacity building for Internet governance in developing countries**  All international organisations and forums for discussions or practice of internet governance have a responsibility to ensure broad and competent representation from all countries, especially from low- and middle-income developing countries. There is a need for better awareness and knowledge about the current internet governance regime, especially for countries and ministries with little previous experience of the multistakeholder decision-making environment. There is also a need to support nascent civil society actors in this field in order to generate deeper national debates on internet related issues. Financial support mechanisms for supporting the participation of representatives of governments, civil society and the technical community in ICANN, GAC, IGF, IETF and other relevant forums should be improved. Regional organisations have a role in promoting active participation. Capacity building for Internet governance should be included in existing international development programmes for programmes that seek to strengthen civil society, industry and the institutional capacity of governments. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | Switzerland is launching a project entitled «Geneva Internet initiative» that aims at assisting in capacity and confidence building among stakeholders dealing with Internet-related policies, in particular developing countries. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | For items 9 and 10 – the UK believes that there should be greater collaboration between stakeholders to ensure that appropriate assistance is provided to developing countries to build capacity in the provision of ICTs going forward.  The UK believes that ICTs offer important opportunities to developing countries. ICTs have an important role to play in the attainment of the Millennium Development Goals (eradicate extreme poverty and hunger, achieve universal primary education, promote gender equality and empower women, reduce child mortality, improve maternal health, combat HIV/AIDS, Malaria and other diseases, ensure environmental sustainability, and develop a global partnership for development.  To achieve these aims, all stakeholders should focus on the promotion of broadband through abolition of regulatory and legal obstacles to infrastructure development, capacity and institution building, promotion of market access, competition and consumer protection. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Contributing to capacity building for Internet governance in developing countries**  As strong supporters of the multistakeholder system of Internet policymaking and governance, the United States believes that greater participation from governments in developing countries would further enrich and ensure the vitality of the various Internet institutions. A variety of capacity building opportunities and options are available to governments through: the GAC, where developing country members can receive funding to participate in ICANN meetings; ICANN; the Internet Governance Forum (IGF); ISOC; IETF; regional and national Network Operators' Groups; and the RIRs. Information and best practices information is also provided by regional country code top level domain organizations. The Internet Governance Forum (IGF) is another source of support. Since 2005, the IGF has catalyzed partnerships between governments and other stakeholders and opened new doors for cooperation and coordination on a broad range of Internet-related public policy issues. Through workshops, sessions, and open forums – and invaluable informal networking opportunities – the IGF, in particular, has enabled governments with emerging ICT sectors to better understand how to address technical aspects of establishing IXPs, offered technical, non-regulatory solutions to spam, and considered approaches to ensuring privacy and managing risk, among other very concrete take-away benefits. Specific examples of IGF initiatives that have yielded benefits for governments include:   * Through a series of IGF workshops beginning in 2006, the cooperative work of UNESCO and ICANN on multilingualism has evolved, eventually resulting in the conclusion in December 2009 of an MOU aimed at supporting the introduction of IDNs, particularly in the developing world; * During the 2010 IGF, UNESCO and ICANN signed a letter of intent to promote Internet access by users in Member States whose official languages are based on the Cyrillic script; and * A workshop at the 2013 Bali IGF featured a discussion of a project in Porto, Portugal, which uses cloud computing and the Internet of things to integrate bus, train, and Metro in a city where there is a multi-modal transportation system and fiber-optical Internet backbone. Government officials actively participated in the question-and-answer period.   Understanding the cost burden of participating in numerous Internet governance activities, the United States provides grants through its Commercial Law Development Program to assist governments in attending the IGF. Similarly, ICANN offers scholarships to developing countries to attend its meetings as does the Internet Society for those interested in attending the IETF meetings as well as annual IGF. Finally, the United States Telecommunication Training Institute (USTTI), a non-profit organization offering tuition-free training to IT professionals and regulators in the developing world offers courses focused on the Internet governance ecosystem.  One of the largest challenges in ICT is training the next generation to operate and manage the infrastructure. Through programs such as Cisco Network Academy, leaders in private sector provide many times in partnership with governments have established educational programs throughout the world, and especially in developing countries, that have trained over 4 million students so that they might establish successful ICT careers.[[21]](#footnote-21)  Deepening developing world participation in the various forums dealing with different aspects of Internet governance is a high priority for the U.S. Government. We strongly supports efforts of the numerous, successful multistakeholder institutions to better meet the needs of developing countries, and we welcome efforts to make the multistakeholder approach to Internet governance, standards development, and policymaking more inclusive. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - Participation on International Forums and training spaces related to Internet governance.  - Internet governance related topics are part of the academic activities of the Institute of Computer Law at the public University. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Contributing to capacity building for Internet governance in developing countries**  Zambia fully participates in regional, continental, and international meetings that focus on capacity building for Internet governance.  Zambia is a member of the African Top Level Domain (AfTLD), which looks at both technical and administrative issues surrounding Internet governance.  The Regulator is considering the establishment of a Zambian Internet governance forum with a view of developing a well-structured platform that looks at Internet Governance. |

# **Developmental aspects of the Internet**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | The following aspects of Internet can have strong impact on development from the regulatory perspective:  - implementation of e-gov services, involvement of citizens and business in government activities through consultations, infrastructure development for e-gov services;  - development of fixed and mobile broadband. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | The country, through the Ministry of Transport and Communications promotes development and innovation of online applications by youth. The Authority also promotes projects relating to the development of the internet; and they will be supported through Universal Service Fund once operational. |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | Likewise, we are not sure what it means |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **Developmental aspects of the Internet** The overall aim of Danish support to civil society is to support the development of a vibrant, independent and diverse civil society in developing countries while also contributing to the popular foundation and engagement in Denmark in development work. Approximately DKK 1 billion is allocated for this purpose in the Danish fiscal act.  In 2013, an innovation pool was established in an effort to encourage Danish civil society organisations to rethink their way of working with partners in developing countries and to promote innovative partnerships and methodologies by providing the funds for testing new ideas. Twelve Danish civil society organisations received a total of DKK 29 million from the pool. Many of the projects proposed the use of innovative methods, particularly in relation to new information and communication technology (ICT), social media etc., with the aim of producing evidence based documentation for activism, broad mobilisation, and national and international advocacy. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **Providing a consistent domestic legal framework for :**  **Developmental aspect of the Internet**  The Indian government plays an important role in empowering individuals, to develop an enabling environment for encouraging growth, interoperability and development of the Internetcommunities and businesses so as to be able to access and use the internet. Government of India is committed to ensuring the protection of networks and preservation of the democratic nature of the Internet and keeping interference to the minimum necessary to keep it socially responsible and legal.  **Digital Divide**  The Indian government has a major role in providing an enabling environment to its vast growing population for easy access to multi lingual (Indian languages) information, knowledge and skills which are in conformance with content and culture of the country to reap the benefits of its **demographic dividends.** It is the ultimate prerogative of the government to provide to its citizens access to affordable and fast broadband internet services necessary for their socio-economic development. The Internet also provides an enabling environment which brings e-governance close to the doorsteps of the citizens. As a highway or a bridge provides connectivity between people and places and its regular upkeep and maintenance is necessary role of the Indian government, similarly the deployment of optical fibres across the length and breadth of the country or providing extra terrestrial solutions for internet accessibility and penetration is pertinent to achieving wide encompassing development via the internet which could be achieved only through Indian government intervention to reach the nook and corner of the country.  Digital divide is a multi faceted challenge (affordability, usage, access, relevance, funding, etc) with no one-size-fits-all. Hence the governments in the developing and least developed countries need to ensure that they promote a coherent national level strategy including technological innovation and innovation clusters based on progressive and forward looking policies that addresses their respective concerns regarding digital divide in terms of the desired impact that they seek. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | • Encouraging establishing Iraqi websites by reducing the prices and easing the procedures, so these websites are in a rapid continuous increase.  • Increase the website hosting companies in Iraq.  • Staring the project of internet gateway.  • Starting a project of Iraqi national plan for migration to IP v6. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The Internet has been developing smoothly under private initiative in Japan.  The Internet community in the private sector has been conducted continuously support activities to the community in developing countries since early days of the Internet, and governmental assistance to developing countries have also brought many good results.  **Actions to be undertaken by governments**  It is indispensable to maintain the multi-stakeholder approach for the Internet to continue contributing to economic growth and innovation in the future.  In order to promote further free flow of information on the global Internet and to promote economic development that will be brought by free flow of information, governments and the private sector should promote their support activities and they should implement more effective supports through their mutual collaboration.  **Additional Comments**  We suppose that various problems related to the Internet may occur in the future. Under this assumption, governments should discuss the role of both private sectors and governments, taking into consideration of the fact that many issues had been solved mainly by private sectors. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Developmental Aspects of Internet**   This section is not applicable to this summary report. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | *Please refer to Section 2.* |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **INTERNET AND UNIVERSAL SERVICE**  To providing the universal telecommunication service the Moroccan Government has created in 2005 a special fund called universal telecommunication service fund (FSUT). This Fund is endowed by contributions from telecommunication operators up to 2% of their turnover excluding tax, net of interconnection fees, sales of terminals and of the payouts for value-added services suppliers. The fund may also receive any contribution in the form of donations and bequests allocated by international organizations or in the development programs of universal telecommunications service.  The revenues of FSUT funds are intended to finance programs and projects approved by the Moroccan government to allow access to the ICT for citizens in the rural areas, students, teachers and others professional bodies acting in social sectors.  Her below, are some programs conducted or are conducting by Moroccan government to ensure providing some categories of professionals bodies possibilities to access to the ICT benefits:   **" GENIE " program**  The GENIE program was launched by the Government in 2006. It aims to integrate information and communication technology and tools to the national education system by equipping all schools (9260 primary and secondary schools) with the multimedia environments connected to the Internet.  The GENIE program contains four axes aiming to improve quality of national education and learning skills in the public schools. Axes and objectives covered by this program are as follows:    **Infrastructure : MultiMedia environnement + internet Access**  **Digital Pedagogic content: provision of digital content + portal for content broadcasting**  **Training : Teachers training**   * **duration : 8 years** * Nb. of students **: 6 Millions** * Nb. of teachers **: 230 000** * Nb. schools **: 9260** * Budget supported by FSUT **: 1038 M MDH**   **Developing usage : supporting staffs from national education and learning to be familiar with ICT use**  GENIE Program  Currently, more than 3,000 schools are already equipped with multimedia environment and connected to the internet and 6500 other schools are equipped by multimedia devices (computer + projector ). Recently, the ministry of national education has launched two public tenders. The first is launched to equipped about 7800 schools with multimedia environment (PCs + digital board+ switch/router + scanner + video projector….) or multimedia bags (computer+ video projector) and the other tender aims to provide internet service to these schools.  In term of training, 70% of 230.000 teacher, included administrative staff, are benefit from training course that allow to increase qualification of use ICT tools in school. Also, 90% of the necessary digital content are acquired and broadcasted to targeted population through dedicated internet portal.  About developing ICT usage, the 20.000 workshop sessions conducted for the targeted population closely to their locations and its aims is supporting them to use ICT tools. Also 200.000 multimedia bags (Lap-Top+ video projector) were provided to the teachers in order to be used in learning courses.  **" INJAZ " program**  INJAZ program aims to allow to the university students to benefit from ICT access package consisting of contribution from the FSUT up to 85% of package cost capped at 3600 MDH. The ICT access package includes: - Lap-top or Tablet PC ; - Mobile Broadband Internet Service ; - Online Resources .  The implementation of INJAZ program is ventilated over four Academic years from 2009-2010 to 2013-2014. The number of targeted population and global provisioned budget to subsidize this program are presented in the following table:   |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | | **Academic year** | **2009-2010** | **2010-2011** | **2011-2012** | **2012-2013** | **2013-2014** | **total** | | **Targeted population** | **17 000** | **13 500** | **43 400** | **28 200** | **24 400** | **126 500** | | **Budget**  **(M MDH)** | **49** | **40** | **156** | **101** | **88** | **434** |   After four (04) previous editions, more than 86,000 students have benefited from this program. The 5th edition, which corresponds to the 2013-2014 academic year, will be launched in the first quarter of 2014. With a budget of more than 88 Million MDh , this edition will allow to the 24,400 students spread over 110 university institutes located in 20 cities in Morocco to benefit from Injaz Package.  **" Nafid @" program**  As part of the accompanying program for GENIE program, Nafida program aims to allow all primary and secondary school teachers to get access to the ICT by subsidizing for them internet service. The budget of this program is 216 million DHS. Actually, more than150.000 teachers are beneficiaries from subsidizing internet service subscription using 3G, ADSL or CDMA technology access.     **Community Access Center (CAC) program**   This program aims to create, in over 4 years and through national territory, 400 CAC that allow citizens in rural areas to access to the Information and Communication Technology, with a budget of 80 million MDh . Each CAC will be equipped at a minimum with the following equipment:  - A telephone device allowing access to telephony service . - Five computers for Internet access service. - Internet connection with a minimum rated capacity of 512 Kb / s.  Until 31 December 2013, 74 CAC are already operational at the Youth Homes attached to the ministry of youth and sport.  **" E -SUP " program**  This program aims to meet the requirements of the National Charter for Education and Training , including ICT is a strategic imperative to improve the quality of education. The implementation of this program will be spread over the next two years with a budget of 120 million MDh supported by the FSUT .  The realization of this program is structured around the following axes:  The first axis is to develop technology platforms university or campus allowing networking between the different stakeholders in higher education and access for teachers , students and administrative staff to the digital services and shared resources.  The second axe is to provide digital content and applications to access, pooling and sharing of appropriate higher education digital resources and scientific research.  The third axe aims to equip the centers of doctoral studies and research laboratories with multimedia environment and internet access service to promote networking research and development inside and outside of the university.   **" U - Net " program**  The Net-U program (wireless University network) aims to promote and expand access to ICTs, particularly the Internet , in high academic institutions and university cities to integrate the use of ICT in modes of learning.  The Net-U program, whose implementation is spread over three years, was designed to allow the wireless internet access to 108 university sites and 25 university campuses for their connection to the Internet , and ensuring adequate coverage of sites and universities cities.  This WIFI network will be connected to the Internet by transmission capacity sufficiently dimensioned by operators (internet suppliers) to provide users from university with quality access to the Internet. The budget of this program is estimated at 125 million MDh supported by the FSUT. |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 8.* |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Developmental aspects of the Internet**  Paraguay throw CONATEL has a National Telecommunications Plan: (<http://www.conatel.gov.py/index.php?option=com_content&view=article&id=30&Itemid=115>) and the initiatives of SENATICs in eGovernment ([www.senatics.gov.py](http://www.senatics.gov.py)).  Paraguay aims to deploy 1,000 miles of intercity optical fiber per year. This is currently being carried out in part through the Universal Service Fund of CONATEL and private companies that are committed to the country extending its lines and pipelines. At present, virtually all cities of the country have access to fiber optics. The sites which have not yet implemented are covered by wireless technologies. |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Developmental aspects of the Internet**   * 1. **NASK** * On 10th December 2013, all blocked regional names were finally made available for registration which soon had almost the whole pool registered or booked for registration. * NASK is planning on the .PL Registry Lock to become a standard security measure along the Register still in 2014. * There are plans also to implement modern, technologically advanced Registrar System allowing independent, self-reliant domain names management at end user level.  1. **Warsaw Technological University**   The Future Internet Engineering project in 2010-13. A joint effort of leading Polish technical universities. The project looked at ways to develop and evaluate next generation Internet infrastructure, including aspects of IPv6. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Developmental aspects of the Internet**  In the context of Governmental Advisory Committee (GAC), Commission on Science and Technology for Development (CSTD) and IGF, Portugal has been defending public policies towards better access and affordability of the Internet.  At a national level, it is worth mentioning the promotion of broadband in rural areas, which can contribute to ensure a level playing field for all citizens, promote info-inclusion and the development of human capital and contributing to the creation of externalities in rural development policy at the level of employment, growth, competitiveness and sustainability of the industries located in these areas.  The Portuguese government launched five Public Tenders for the deployment of "High-Speed Networks in Rural Areas", involving 139 municipalities, an investment of 156 millions of euros, covering more than 1 million of people. |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | **Development aspects of the Internet :**  MICT closely follows the impact of the Internet and its governance on the progress of society through its “Internet and Society” department. This department is serving as a research hub for studying Internet technology, policy and economics. The overarching objective of the researches is to determine the most effective ways for individuals and businesses to benefit from ICT/Internet innovations. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Developmental aspects of the Internet could include:   * enhancing openness of government body activity, inter alia, by providing electronic public services, development of access infrastructure to e-government services; * enforcement of intellectual property rights; * concern for the national interests; * improve access to national knowledge; * making the environment more attractive for investment into national broadband infrastructure; * supporting the development of local content and services in national languages; * promoting development of telecom infrastructure (fostering Internet broadband access, providing quality of service, affordability, including for remote and sparsely populated areas). |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Developmental aspects of the Internet**  Since 2000 GoR has established institutions and mechanisms to create an enabling environment for ICT development, deployed critical world-class infrastructure and is continuously developing a skilled human resource base in its quest to become a knowledge-based society.  The existence of a conducing legal and regulatory framework, availability of good infrastructure and a growing and innovative human resource base are the enablers of ICT development in Rwanda. The established liberalized environment catalyses and secures private sector initiative in the service development and delivery.  Rwanda adopted consultative approach in addressing Internet governance issues to ensure that all stakeholders’ opinions are taken into consideration. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  A. Propose and support R&D programs related to technical and administrative improvements in the Internet  **Actions which have been undertaken by Governments**  A. Those countries where R&D is undertaken are generally supporting those programs. There are continuing issues, however, with the role of developing and less developed countries regarding input to R&D programs. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Developmental aspects of the Internet**  To achieve fair and sustainable global development, everyone must have access to the technologies that define present-day realities. Internet access is key to increasing the opportunities for poor people to exercise their freedom of expression and information. Sweden generally emphasises the significance that ICT can have for development and for promoting the enjoyment of human rights, and is using ICT actively as a tool for sustainable development.  Sweden is working for increased access to, and use of, information and communication technology with the aim of increasing knowledge, dissemination of information and participation regardless of physical boundaries, and with particular focus on increasing the use of ICT by women and other groups that do not currently participate fully in the information society. Building local capacity for innovation, development and entrepreneurship in the IT sector in low and middle-income countries is an important area.  Within development cooperation, priority is given to ICT and the internet’s positive effects on poverty reduction, combating corruption, democratic development and participation. Access to an open and free internet plays a significant role in creating economic growth and contributing to the creation of open, innovative and resilient social structures in low and middle income countries. There are many examples of people raising themselves out of poverty where access to and use of ICT have been a contributing factor. Sweden supports a number of initiatives in these areas at bilateral, regional and global level. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | *Please refer to Section 9.* |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Delopmental aspects of the Internet**  The Internet has proven to be a tremendous engine of economic development. One recent study estimates that when Internet penetration rises by 10 percent in emerging economies, it correlates with an incremental GDP increase of one to two percent[[22]](#footnote-22). To best seize on the developmental opportunity afforded by the Internet, governments must establish an enabling regulatory environment where competition flourishes and innovators and entrepreneurs are encouraged to participate in the digital marketplace.[[23]](#footnote-23)  Governments can also use the Internet and other ICTs to help catalyze progress in traditional development projects in education, health, agriculture, and transportation. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - The Digital Agenda for Uruguay is a countrywide commitment, a multi-stakeholder agreement between government, academia, the private sector and organized civil society. It is focused on social inclusion and on the strengthening of national capacities through the use of ICTs. The Digital Agenda for Uruguay 2011-2015 has 59 concrete and measurable goals.  - IPv6: One of the goals of the Digital Agenda for Uruguay is: “Internet Protocol version 6 (IPv6) installed on all central government IT equipment directly connected to the Internet, by 2015”.  - Intensive promotion of the use of ICT applications (e-government, e-Business, e-employment, e-environment, e-health, etc.) to contribute to sustainable development.  - Initiatives to promote the development of national software and Apps. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Developmental aspects of the Internet**  Zambia also focuses on the development of capacity in aspects of the Internet, such as the implementation of automated Registry infrastructure, WHOIS services, and DNSSEC.  The Regulator also hosted the first African Internet Summit in 2013; which brought together acclaimed industry experts through the technical training conducted by the Africa Network Operating Group (AfNOG) – which has consistently focused on the capacity building for Network Operators in Africa.  The Regulator is also looking at strengthening the operations of the Internet Exchange Point in Zambia, through infrastructure development and training. This may include the establishment of IXPs in selected towns of Zambia. In this vein, the government plans to foster interconnection of IXPs with neighbouring countries to ensure that “regional traffic remains in the region”. |

# **Respect for privacy and the protection of personal information and data**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Respect for privacy and the protection of personal information and data**  Australia considers that the Internet and other digital communication technologies provide an unparalleled opportunity for exercise of the fundamental freedoms of expression, peaceful assembly and association.  Technological developments have also fostered opportunities for enhanced communication and connectivity, as well as improved access to health and education services for isolated communities.  Australia acknowledges that with these benefits also comes the risk that digital technologies can be used to undermine the protection of human rights.  Accordingly, it is essential that it is ensured that the same rights and freedoms people should enjoy in their everyday lives are protected and promoted in the online environment.  Australia considers that support for and implementation of the International Covenant on Civil and Political Rights (ICCPR) remains as relevant and vital today, in the digital age, as it ever was.  Within Australia, the *Privacy Act 1988* (the Privacy Act) is the principal piece of legislation that regulates the collection, use, storage and disclosure of personal information.  The Privacy Act is technology neutral. From 12 March 2014, reforms to the Privacy Act will introduce the Australian Privacy Principles, which will apply to both government agencies and certain organisations.  These Australian Privacy Principles will replace the existing Information Privacy Principles and National Privacy Principles and set out the obligations for the handling of personal information.  Australian law provides additional protections for the privacy of the content of communications and for non-content telecommunications data on the Australian telecommunications network. The privacy protections created by Australian law comply with international law, including Articles 17 and 19 of the International Covenant on Civil and Political Rights, Article 12 of the Universal Declaration of Human Rights and Article 15 of the Budapest Convention on Cybercrime. In particular, warrants and authorisations permitting Australia’s law enforcement and national security agencies to access the content of communications and non-content telecommunications data, which include consideration of proportionality, ensure that access to content and non-content data is not arbitrary or unlawful.  In May 2013, the Australian Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended that the laws protecting the privacy of Australian telecommunications and permitting lawful access by law enforcement and national security agencies be ‘comprehensively revised’ and that the revision be undertaken in consultation with privacy advocates and practitioners.  In December 2013, the Australian Senate Legal and Constitutional Affairs References Committee (Senate Committee) agreed to a further inquiry into the comprehensive revision of these laws. The Senate Committee is due to report by 10 June 2014. The Australian Government is considering the recommendations of the PJCIS and will consider any further recommendations made by the Senate Committee. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | Governments should develop and adopt legislation aimed on privacy and the protection of personal information and data. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | Botswana is in the process of adopting the SADC Model Law on Data Protection. The national Broadband Strategy also recommends for the Data Protection Act to be in place as the country is looking into rolling out broadband.  Lack of a national IGF hinders progress in some of these matters. |
|  | Brazil [(INF/38)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0038/en) | **Respect for privacy and the protection of personal information and data**  Brazil actively participates in efforts to promote universal principles based on common understanding, the indivisible and interdependent character of human rights and the right to privacy as fundamental aspects of the Information Society, forming the basis for the responsible use of ICTs, in a framework of cultural sensitivity, tolerance, and dialogue.  Brazil supports national, regional and international efforts towards the establishment of guidelines, frameworks and/or law, where appropriate, to which governments, companies and users may refer, particularly in regard to ethical standards, rights and responsibilities on the general use of ICTs, both online and offline.  In this regard, on 18 December 2013 the United Nations General Assembly adopted a resolution, tabled by Brazil and Germany, on the right to privacy in the digital age, reaffirming the basic principle that human rights apply just as much online as they do offline.  This UNGA Resolution is available at: <http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1> |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | In Bulgaria the respect for privacy and the protection of personal information and data are regulated by the [Law on Protection of Personal Data](https://www.cpdp.bg/en/?p=element&aid=373), adopted in 2002, the [Law on Electronic Communications](https://www.cpdp.bg/en/?p=element&aid=433) and the [Law for Civil Registration](https://www.cpdp.bg/en/?p=element&aid=435).  The Commission for Personal Data Protection was established under the [Law on Protection of Personal Data](https://www.cpdp.bg/en/?p=element&aid=373). It is an independent public authority whose main task is the protection of individuals when processing their personal data and providing access to these data. It also exercises control over observance of the Law on Protection of Personal Data and the other relevant laws and legislation acts. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **Respect for privacy and the protection of personal information and data** The Danish parliament has adopted Act number 429 of 31 May 2000 on the processing of personal data as amended. The Act is drafted in accordance with Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It follows from Section 55 of the Danish Act on Protection of Personal Data that Datatilsynet – a supervisory authority – supervises the processing of data covered by the Act.  In light of the present focus on data protection, in relation to the ongoing negotiations of the European Personal Data Regulation, , the Danish government has initiated a national debate among stakeholders with a broad view on "digital trust", focusing especially on the economic perspectives of data protection for both consumers and business. The Danish Government works on bringing this perspective of the data protection debate to the European level, in order to create a strong link between actions for both the protection of privacy and growth initiatives in regards to i.e. Big Data. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **Providing a consistent domestic legal framework for :**  **Respect for privacy and the protection of personal information and data**  Internet privacy involves the right or mandate of personal privacy concerning the storing, repurposing, provision to third-parties, and displaying of information pertaining to oneself via the Internet. **Section 66E** of Information Technology Amendment Act 2008 discusses privacy violation. Section 69 empowers the Controller; if he is satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, security of the State, friendly relation with foreign states or public order, to intercept any information transmitted through any computer system or computer network. Penalty for breach of confidentiality and privacy is also discussed in **Section 72**. Moreover with increasing proliferation of social networking sites the issue of privacy and data protection accrues a serious role in internet policy making where Indian government has to play a pivotal role. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Legislation of Cybercrimes law. * Studying the preparation of establishing special procedures in this regard. |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has established basic frameworks for this issue and the government has promoted voluntary actions taken by multi-stakeholders.  For example, as smartphones diffuse, applications to extract user information illegally increase. The government of Japan established a study group to consider ensuring appropriate handling of user information through smartphones.  The study group established a report ‘Smart Phone Initiative (SPI)’ which recommended to　establish privacy policies for each application.  Then the group established another recommendation, ‘Smart Phone Initiative II (SPI II)’ in which mechanisms to validate applications by third parties should be promoted by private sector’s initiative.  **Actions to be undertaken by governments**  The government of Japan is expected to follow-up actions on SPI and SPI II.  For example, private and public sectors will work together to establish and announce privacy policies for each application and periodically examine the situations of those establishment and announcement. In addition, the government of Japan will conduct demonstration experiments to find out what technological challenges exist for establishing private-sector-driven mechanisms to validate applications by third parties. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Respect for Privacy and the Protection of Personal Information and Data**   As the amendment to the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., which reinforces personal information protection in information and communication, went into effect in August 2012, various programs regarding personal information use and protection came into being. Accordingly, information and communication service providers are prohibited, in principle, from collecting and using the resident registration number of the user unless the personal identification authority or law permits, and various new systems, such as the personal information expiration system, the personal information usage notification system, and the notification and reporting of personal information leak to minimize the damage, were introduced. The biggest change to the personal information protection policies due to the amendment of the Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc. is the prohibition of the information and communication service providers from collecting and using resident registration numbers (RRN) on the Internet. The collection and use of RRNs was prohibited from August 2012, and the RRNs already in possession were to be destroyed within two years after the date of enforcement. Accordingly, the Korea Communications Commission (KCC) and the Korea Information Security Agency (KISA) opened the ‘Internet RRN Clean Center’ in May 2012 to support the RRN restriction policy. They also support laws on restriction of collection and use of RRN, technology counseling, RRN conversion support for small businesses, and provision of alternative RRN.  Korea enacted “Personal Information Protection Act” in order to increase the people’s rights and to ensure the protection of personal information in September 2011. The Personal Information Protection Act (PIPA) 2011 is comprehensive legislation, covering all sectors. Prior to September 2011 privacy protection was covered in part by the Act on the Protection of Personal Information Maintained by Public Agencies 1999 for Government, and Act on Promotion of Information and Communication Network Utilization and Information Protection 2001 for the private sector. This second Act only applies to the information and telecommunications industries that are providers of information and communications services such as common carriers, Internet service providers and other intermediaries, such as content providers. The Act also covers specific offline service providers such as travel agencies, airlines, hotels, and educational institutes.  PIPA identifies information pertaining to a living individual, which contains information identifying a specific person with a name, a national identification number, images, or other similar information (including information that does not, by itself, make it possible to identify a specific person but that which enables the recipient of the information to easily identify such person if combined with another information).  The relevant Korean authorities' understanding is that the construction of Personal Data under PIPA and that under IT Network Act are same in spite of subtle difference in definition wordings. The Minister of Public Administration and Security (MOPAS) is in charge of the execution of PIPA. The KCC is in charge of the execution of the IT Network Act.  Under PIPA, Sensitive Personal Data is defined as Personal Data consisting of information relating to a living individual's: (i) thoughts or creed; (ii) history regarding membership in a political party or labor union; (iii) political views; (iv) health care and sexual life; and (v) other Personal Data stipulated under the Enforcement Decree (the Presidential Decree) which is anticipated to otherwise intrude seriously upon the privacy of the person. The Enforcement Decree of PIPA includes genetic information and criminal record as Sensitive Personal Data. IT Network Act also has a similar definition  The KISA is an executing organization of personal information protection, although complaints handling is complemented by the work of the Personal Information Dispute Mediation Committee (PICO). Aside from the PICO, KISA has been operating 24/7 call center to consult personal information breach.  Aimed at increasing the awareness that appropriate management of personal information, Korean government has introduced “Privacy Impact Assessment (PIA)” to constrain from infringing of privacy and ensuring a secure process of personal information. According to the PIPA, the impact assessment in public organization is obligatory while the assessment for relevant stakeholders in a private sector is optional. |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | **Respect for privacy and the protection of personal information and data** (issues 11 in Annex 1)  The State Data Protection Inspectorate of the Republic of Lithuania (hereinafter – SDPI) participates in the project supported from the Civil Justice Programme of the European Union“Cross-border realization of the right of access of the data subject (Lithuania-Estonia and Estonia-Lithuania) JUST/2012/JCIV/AG/3383“. The aim of the project is to analyse the possibility of creating a unified information technology environment where citizens could perform various data queries concerning themselves. The result of this project will be an analysis about the legal and technical solutions to enable citizens to enquire personal data about themselves via the public user interface (AET) of integrated information system E-file from all the databases already interfaced with it. Those information systems (IS) are for example the Court IS, Procedural IS of the Police, the Criminal Procedure's Register, the Portal of Misdemeanour Proceedings, Criminal Record, Land Register and Business Register. Citizens would also be able to enquire data regarding third parties to whom their personal data has been forwarded or who has accessed it.  The SDPI and the Ministry of Transport and Communications of the Republic of Lithuania are members of the working group created by the Order of the Minister of Interior No. 1V-235 (20/03/2013) in aim to prepare Project of the Law on Cyber Security and in this way, participates in the policy making of internet security. The Project shall be prepared till 31/03/2014.  Also representatives of the SDPI and the Ministry of Transport and Communications of the Republic of Lithuania takes active part in the work of the Cyber Security Coordination Commission, which deals with various cyber security questions.  The SDPI prepared following recommendations on internet security and related topics:   * [Recommendation on the use of cookies and similar measures (2011)](https://www.ada.lt/images/cms/File/naujienu/slapuk_DV.pdf); * Recommendation on the use of cookies: tips for users of the electronic communication services [(2011)](https://www.ada.lt/images/cms/File/naujienu/slapuk_DS.pdf); * Secure data transmission using [https protocol (2009)](https://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/SSL20091228.doc); * Privacy protection using wireless networks [(2008)](https://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/Belaidziu%20tinklu%20rekomendacija_20081203.pdf); * Secure data transmission by email [(2008)](http://portalas.ada.lt/index.php?action=page&lng=lt&id=594).” |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | 1. Data Protection Act enacted in 2004 to provide for the protection of the privacy rights of individuals in view of the developments in the techniques used to capture, transmit, manipulate, record or store data relating to individuals |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **Respect for privacy and the protection of personal information and data**  For preventing unauthorised access to sensitive data and other information which is of private use only, Law on securing personal data Nr. 133 dated 08.07.2011 was adopted. Also the National Strategy on Personal Data Protection and the respective Action Plan was adopted by Law Nr. 229 from 10.10.2013. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **Respect of Confidentiality and Protection of Personal Data and Information**  **Realizations:**   * Adoption of the law n° 09-08 related to the protection of personal data and its implementing decree n° 2-09-165; * Adoption of the law n° 53-05 related to electronic exchange of legal databases and its implementing legislation, namely:   + the decree n° 2-08-518 taken to implement the articles 13,14,15, 21 and 23 of the law n°53-05;   + the order of the minister of industry, commerce, investment and digital economy n° 151-10 which fixes the form of the prior declaration of import, export, provision, exploitation or use of cryptography means or services and the companion file content;   + the order of the minister of industry, trade, investment and digital economy n° 152-10 which fixes the form of the request of prior authorization of importing, exporting, provision, exploitation or use of cryptography means or services and the companion file content;   + the order of the minister of industry, commerce, investment and digital economy n° 153-10 related to the approval of persons who do not have the approval of electronic certification service providers and who intend to provide cryptography services subject to authorization;   + the order of the minister of industry, commerce, investment and digital economy n°154-10 which fixes the form of the request for electronic certification service providers approval and approves the companion model of technical specification. * Adoption of the law n° 31-08 which enact measures for consumer protection (including the provisions related to online selling) and its implementing legislation:   + the decree n°2-12-462 which fixes the standard statute of consumer protection associations of public benefit;   + the decree n°2-12-503 taken for the implementation of law n° 31-08. * Elaboration of a global study of the legal instruments related to the information technology, protection personal data, cybersecurity and cybercrime to strengthen the Moroccan legal act and fill existing gaps that may be an obstacle to ensure the digital trust and combat cybercrime; * Accession to the Convention 108 of the European Union related to the protection of personal data and its additional Protocol; * Establishment of the National Commission of Personal Data Protection (CNPD).   **Objectives of Law 09-08:**   * Provide the Moroccan judicial arsenal with specific legal means to ensure effective protection of personal data; * Protect citizens and anyone living on the Moroccan territory against the misuse of personal data; * Develop the judicial arsenal (EU Directive 95/46/CE and Convention 108 of the Council of Europe as references) to promote the development of the Offshoring.   **National Commission of Personal Data Protection (CNDP):**  The National Commission of Personal Data Protection is a supervisory authority (or a regulator) placed under the authority of the Head of Government and established on the basis of the article 34 of the law 09-08.  The primary aim of this authority is to ensure the effective implementation and the respect of the provisions of law n° 09-08 which governs personal data protection.  **CNDP’s missions:**   * Inform people of their rights and obligations; * Advising the government, parliament and other administrations on aspects relating to the protection of personal data * Legal and technological intelligence * Control and investigation; * Regulation . * Technological and legal watch |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | **PRIVACY: Respect for privacy and the protection of personal information and data**  Privacy and the protection of personal data is legislated in New Zealand through the Privacy Act 1994. This Act demonstrates a flexible, modern approach to managing privacy in the face of ongoing technological developments. Privacy obligations and processes for handling personal information are detailed through twelve privacy principles. The privacy principles , covering [collection](http://www.privacy.org.nz/purpose-for-collection-of-personal-information-principle-one/) of personal information, [storage and security](http://www.privacy.org.nz/storage-and-security-of-personal-information-principle-five/) of personal information, requests for [access](http://www.privacy.org.nz/access-to-personal-information-principle-six/) to and [correction](http://www.privacy.org.nz/correction-of-personal-information-principle-seven/) of personal information, [accuracy](http://www.privacy.org.nz/accuracy-etc-of-personal-information-to-be-checked-before-use-principle-eight/) of personal information, [retention](http://www.privacy.org.nz/agency-not-to-keep-personal-information-for-longer-than-necessary-principle-nine/) of personal information, [use and disclosure](http://www.privacy.org.nz/limits-on-use-of-personal-information-principle-ten/) of personal information, and using [unique identifiers](http://www.privacy.org.nz/unique-identifiers-principle-twelve/). These principles reflect internationally accepted standards for good personal information handling.  The Officer of the Privacy Commissioner has responsibility for monitoring proposed legislation to see if it affects the privacy of individuals, and commenting on any privacy problems. It also provides [education](http://www.privacy.org.nz/workshops/) about privacy, monitors technological developments that can affect privacy, issues [codes of practice](http://www.privacy.org.nz/codes-of-practice/), which modify the privacy principles and which apply to a particular industry or topic, and investigating [complaints](http://www.privacy.org.nz/how-to-comply-with-the-privacy-act/) about interferences with privacy.  The Officer of the Privacy Commissioner is actively engaged in discussions regarding technology and privacy, and regularly engages with Internet stakeholders both on an ad-hoc basis, and through participation at Nethui, the annual New Zealand multistakeholder conference on internet public policy issues.  Private industry in New Zealand has also led the introduction of the New Zealand Cloud Code, a voluntary code for cloud service providers which requires signatories to declare what they offer so customers can make an informed decision.  The Code requires providers to make clear exactly what security precautions and back-up systems they have in place, where data is stored and a range of other disclosures, so customers can make an informed decision about which cloud service to use. |
|  | Oman (ITA) [(INF/2)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0002/en) | The Information Security Management Framework is part of the overall Information Technology Authority (ITA) standards framework aims to ensure the protection of information assets from unauthorized access to or modification information, whether in storage, processing, or transit. It also aims to protect against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document and counter such threats.  This project creates a secure and organized working environment and protects information and information assets. In addition, prevents an information security incident from occurring. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Respect for privacy and protection of personal information and data**  Banks, finance companies, cooperatives entities, private and mobile phone companies, the Ministry of Finance, has robust systems against information theft. Also, several companies are using in Paraguay the digital certificate provided within the country. Paraguay has approved law No. 4868 Electronic Commerce and the law of Electronic Signature No. 4017 (<http://www.acraiz.gov.py>) |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Respect for privacy and the protection of personal information and data**   * 1. **NASK**   Information on domain names administered by NASK can be accessed using the WHOIS application which is a generally available database holding information on Internet domain subscribers. Information on subscribers and on domains subscribed is publicly available which respects rights of Internet users, trademarks owners, copy rights, etc.   * 1. **PCSS** * Plans in place to launch the “TOR-box” research project, allowing end users, when in untrusted environment to request that a safe and anonymous communication channel be set-up (through e.g. a cell phone). PCSS is also looking forward to starting wide-reaching research on on-line privacy of end users using mobile devices, e.g. smartphones, palmtops, wearable electronics as well as the Internet of Things-related computer systems. * Development and making operational of all-in-one systems of data storage, e.g. PLATON - Science Services Platform or the National Data Storage (both available at a national level, offering remote archiving and backup as added value to the PIONIER network).   1. **DSI MAC**   + In Poland the right to privacy and protection of personal data is a constitutional fundamental right – Poles, having experienced a totalitarian regime are especially sensitive on this subject. The Polish government is very much involved in the work on the new EU general data protection regulation, as we believe it is one of the most important pieces of legislation currently under discussion in Brussels. It will shape the area of personal data protection law in Europe for the next 20 years. The Polish government’s objective during the work on the regulation is to develop the provisions that will ensure a high level of personal data protection without hindering the business activity of European enterprises.   + We are also involved in the process of modernization of the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, a legal instrument of wider application that has recently transcended the borders of Europe. Poland believes it is time to begin work on a global scale convention on the protection of personal data. The ease with which data may be transferred across borders renders national legislation ineffective.   + The threats to personal privacy do not only originate in the commercial sector. The recent revelations concerning the scale of government suspicion less bulk data collection programs which should also be addressed.   + Poland plans to enact a law governing the use of CCTV monitoring systems in order to better protect the privacy, as well as modernize its privacy protection regulations before the new EU regulation is passed. |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | **Respect for privacy and protection of personal information and data :**  Data privacy and protection of personal information are paramount for Qatar. Qatar is currently developing a comprehensive legal framework to provide the highest protection standards to its citizens and residents. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | The CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data came into force in the Russian Federation on 1 September 2013.  Governments should develop and adopt legal and regulatory frameworks protecting personal data and information privacy. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**   1. Develop international public policies to deal with privacy and the protection of personal information and data.   **Actions which have been undertaken by Governments**   1. A number of countries have national policies and laws related to privacy and the protection of data, but they are not coordinated with international public policy since there is no mechanism to develop such policy. At present, global personal data is handled according to the laws and policies of the country where that data is kept. There is a real need for international public policy on how this should be handled. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Respect for privacy and the protection of personal information and data**  The constitution of Rwanda has provisions that are relevant to the privacy of persons. The current legislation has provisions that protect and ensure the privacy of personal information and data. |
|  | Singapore [(INF/6)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0006/en) | Singapore enacted a data protection law in 2012 to govern the collection, use and disclosure of personal data. This is intended to address individuals’ concerns about the proliferation of personal data as well as to maintain individuals’ trust in organisations that manage personal data, even while enabling organisations to collect, use or disclose such data for reasonable purposes.  By regulating the flow of personal data among organisations, the Personal Data Protection Act (“PDPA”) also aims to strengthen and entrench Singapore’s competitiveness and position as a trusted, world-class hub for businesses.  The PDPA establishes a data protection law that sets out rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. The provisions relating to these data protection rules will come into force on 2 July 2014.  The PDPA also provides for the establishment of a national Do Not Call (“DNC”) Registry. The DNC Registry will allow individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organisations. The provisions relating to the DNC Registry came into force on 2 January 2014.  In the development of this law, references were made to the data protection regimes of key jurisdictions that have established comprehensive data protection laws, including the Australia, Canada, EU, Hong Kong, New Zealand and the UK, , , as well as the OECD Guidelines on the Protection of Privacy and Transborder Flow of Personal Data, and the APEC Privacy Framework. These references were helpful in the formulation of a regime for Singapore that is relevant to the needs of individuals and organisations, and also takes into account international best practices on data protection. The law was also shaped through three extensive public consultations conducted between 2011 and 2012.  The PDPA is administered by the Personal Data Protection Commission, a statutory body set up for this purpose.  More information is available at:  <http://www.pdpc.gov.sg/personal-data-protection-act/overview#sthash.K9v6Q35n.dpuf> |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Respect for privacy and the protection of personal information and data**  Privacy and the protection of personal information and data is an important aspect for trade-relations and -agreements, as most of all trade—including goods and services, entails cross-border transfer of data.  Sweden has implemented the EU rules on privacy and personal data protection. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | Switzerland has implemented a legal framework for privacy protection. The actual framework gives the person concerned possibilities to take actions relating to protection of privacy. The plaintiff may in particular request that data processing be stopped, that no data be disclosed to third parties, or that the personal data be corrected or destroyed. The Federal Data Protection and Information Commissioner can investigate cases when methods of processing are capable of breaching the privacy of persons and if there the data processing is related to Switzerland and/or the personal data pertaining is processed by natural or legal persons situated in Switzerland. In the context of the internet the legal framework has its limitation in territoriality principle. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | The UK participates fully in privacy/ data protection debates within the EU; UN and other international fora where appropriate. This work is spread amongst a number of UK government departments and is coordinated by the Ministry of Justice and the Office of the Information Commissioner in the UK.  Related links - <http://ico.org.uk/> and <http://www.justice.gov.uk/information-access-rights/data-protection> |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Respect for privacy and the protection of personal information and data**  Privacy protections are critical to maintaining consumer trust in networked technologies. When consumers provide information about themselves—whether it is in the context of an online social network that is open to public view or a transaction involving sensitive personal data—they reasonably expect companies to use this information in ways that are consistent with the surrounding context.  It is the responsibility of governments to establish a system that facilitates consumer data protection while allowing businesses that provide online services to thrive.  Uses of personal data, and consumer expectations of privacy, tend to be both context- and culture-specific. The strength of the U.S. framework for consumer privacy is that it rests on widely recognized, fundamental privacy values but is flexible and adaptable to these different contexts. There are numerous privacy laws in the U.S. that protect privacy with regard to specific types of data (e.g., health data, financial data, children’s data) and many different privacy enforcement authorities. The Federal Trade Commission (FTC) is the enforcement authority for several of these privacy laws and also has a general authority to protect against consumer fraud and unfair trade practices. The U.S. Commerce Department is working closely with a wide array of stakeholders to develop industry-specific codes of conduct enforceable by the FTC.  Because today’s global digital economy relies on the free flow of data across national boundaries, it is important that governments work together to enhance the consistency of consumer privacy protections while still enabling consumers to enjoy the benefits of globally available goods and services.  Given the contextual nature of privacy, trans-border privacy protections are best enhanced, not by attempting to harmonize national laws or trying to force nations to adhere to a single regulation, but through mutual recognition of different approaches to privacy that rest on the same fundamental privacy values, as well as enhanced cooperation between privacy enforcement authorities.  The Asia Pacific Economic Cooperation (APEC) forum, for example, has made important contributions to this space with its development of the [Cross-Border Privacy Regulation](http://www.apec.org/Press/Features/2013/0903_cbpr.aspx) system and engagement with EU-based privacy enforcement authorities in implementing the concept of interoperability. This process has entailed input from numerous government and business stakeholders – from both APEC and non-APEC member economies. It potentially may yield a practical approach to ensuring privacy of cross-border data flows that respects countries’ privacy regimes while minimizing burdens on global businesses. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - Regulation and Control of Personal Data authority.  - Personal Data Protection and Habeas Data Action Act: regulatory framework that also applies to Internet users.  - Educational guides and online course on personal data protection are available.  - EU Commission recognized that Uruguay laws are adequate personal data protection legal framework.  - Uruguay became the first non-European state to join COE’s personal data protection Convention.  - Active involvement in the Ibero-American Network of Data Protection and in the International Conference of Data Protection and Privacy Commissioners, hosted in Uruguay in 2012.  - Several laws on security and privacy on Internet and creation of specialized groups within the State. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Respect for privacy and the protection of personal information and data**  The right to privacy of person and property, including personal information is enshrined in the Zambian Republican Constitution (Article 17). Further, the ECT Act No. 21 of 2009 protects personal data by prohibiting unauthorized disclosure without following due process (Sections 41, 42, 80 to 84)  A Data Protection Act is also in the process of being drafted, which will address in detail, the privacy and protection of personal information and data. |

# **Protecting children and young people from abuse and exploitation**

|  |  |  |
| --- | --- | --- |
|  | **Member State** | **Actions undertaken or to be undertaken** |
|  | Australia [(INF/26)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0026/en) | **Protecting children and young people from abuse and exploitation**  Computers and the internet have created unprecedented opportunities for social, commercial, recreational, and political interaction. The internet facilitates trade, commerce and communication and is an essential part of the global infrastructure.  As with all types of advancement however, the threat of exploitation of those advancements and the risks associated with those threats are ongoing and persistent.  For instance, the internet and mobile technologies are being used to facilitate the sexual abuse and exploitation of children globally.  The Australian Government recognises online safety of children is an important area of responsibility, especially for parents and teachers, and has committed to a range of policies to help protect Australian children online. These include establishing a Children’s e-Safety Commissioner to take a national leadership role in online safety for children; implementing a legislative based complaints system for the fast removal of material from large social media sites that is harmful or distressing to a child; investigating options for a simplified cyber-bullying offence; consulting with industry to improve safety options and software for smartphones, other devices and internet access services; establishing an advice platform with guidelines for parents about appropriateness of individual media items for children; providing funding to support Australian-based research and information campaigns on online safety; and improving support for schools through a stronger online safety component within the National Safe Schools Framework, establishing a voluntary process for the certification of online safety programs to be offered in schools, and funding for schools for the provision of online safety programs.  The Government has also established an Online Safety Consultative Working Group to bring together representatives from industry, government and non-government organisations with an interest in child welfare to provide expert advice to the Government and the Children’s e-Safety Commissioner (once established) in developing online safety policies and programs. In addition to these initiatives, the Government provides a number of online safety resources to help protect children and young people online, such as a *Cybersafety Help Button* which provides fast and easy access to online safety information and assistance, and *the Easy Guide to Socialising Online*, which provides tips and online safety information for using different social networking sites, search engines and online games.  The Australian Federal Police (AFP) seeks to combat the threat of exploitation of children online in partnership with State, Territory and International law enforcement agencies, government and non-government organisations and industry. The AFP’s Child Protection Operations teams monitor, investigate and target those associated with these offences and in conjunction with relevant agencies. The AFP through its Cyber Crime Prevention Team is instrumental in implementing cybercrime prevention strategies aimed at educating and raising awareness of online risks and empowering all online users on how to protect themselves online. The ThinkUKnow Cyber Safety program is one such example. This is a successful partnership between law enforcement (AFP, and Northern Territory Police), and Industry (Microsoft, Datacom and ninemsn) in raising awareness amongst carers, parents and teachers on how they can keep their children safe online (see [www.thinkuknow.org.au](http://www.thinkuknow.org.au)).  The Australian regulator, the ACMA, administers a co-regulatory scheme for dealing with prohibited online content under Schedules 5 and 7 of the Broadcasting Services Act 1992 (that is, the ACMA Hotline for reporting offensive and illegal online content). The scheme provides a range of citizen and consumer protections, including a power to take-down prohibited content  hosted in Australia, referral to law enforcement of illegal content and, under industry codes of practice, the availability of optional end-user filters for use by Australian families.  Under the scheme, Australian residents may make complaints about online content they believe to be prohibited, including child sexual abuse material. Prohibited content is defined in relation to the National Classification Scheme (NCC) that applies to films and computer games. It includes Refused Classification (commonly referred to as ‘banned’) material, X18+, and certain R18+ and MA15+ content. Child sexual abuse material falls under the Refused Classification provisions as it contains ‘offensive depictions of children’ (as defined by the NCC). The majority of complaints to, and investigations by, the ACMA regarding online content relate to child sexual abuse material.  When prohibited content is found to be hosted in Australia, a take-down notice is issued after the content has been formally classified by the Classification Board. When prohibited content is found to be hosted overseas, it is notified to industry accredited filter providers (filters are available from industry at or below cost and are optional for end-users).  Additionally, all content that is potentially illegal is notified to law enforcement in Australia, with one exception: where child sexual abuse material is found to be hosted overseas in an International Association of Internet Hotlines (INHOPE) member country, the ACMA reports it through the INHOPE network for rapid law enforcement notification and take-down in the host country. (Nearly all child sexual abuse material investigated by the ACMA is hosted in INHOPE member countries.) The mechanism to enable the ACMA to notify child sexual abuse material to INHOPE, rather than law enforcement in Australia, is provided by a formal service-level agreement with the AFP. This Memorandum of Understanding enables and provides a legal mechanism for the ACMA to report highly illegal content to an overseas body.  The ACMA’s role, in conjunction with the effective operation of the international system, effectively acts as a frontline response to online child abuse material by assisting to:   * prevent inadvertent access to highly offensive illegal content by Australian citizens * ensure such material is rapidly brought to the attention of law enforcement agencies around the globe * help stop continued re-victimisation of child abuse victims through the removal of the evidence of their abuse * disrupt access to content by paedophiles and others involved in criminal activity who wish to access child sexual abuse material. |
|  | Belarus [(INF/18)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0018/en) | Governments should develop and adopt legislation aimed on protecting children and young people online. Teachers at schools and professors in academia should be trained appropriately. It’s also necessary to actively cover this topic in mass media to make parents informed. |
|  | Botswana [(INF/7)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0007/en) | The national Cybersecurity Reference group also handles issues related to Child Online Protection, however, there is still a lot to be done regarding this issue such as development of policies and guidelines as well as public awareness to ensure young people are protected online. |
|  | Brazil [(INF/38)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0038/en) | **Protecting children and young people from abuse and exploitation**  Brazil actively participates in the ITU Council Working Group on Child Online Protection, regularly contributing with its own experience in raising awareness of this very relevant issue. Recent contributions by Brazil to ITU CWG-COP were presented in 2011 and 2013 and are available at:  <http://www.itu.int/council/groups/wg-cop/pd/013E_BDT.docx>  <http://www.itu.int/council/groups/wg-cop/pd/COP_KIDS%20ONLINE%20BRAZIL_PPT_FINAL.pdf> |
|  | Bulgaria [(INF/36)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0036/en) | Within the context of the EC initiative, the Safer Internet Programme, a National Safer Internet Center has been established in Bulgaria since 2005. The main purpose of the Center is to educate children, teachers and parents, thus providing them with a safer, more useful and more pleasant cruise across the World Wide Web. The activities of the Center are assisted by a Public Council for Safer Internet, which includes representatives from all sectors of society: the Government, private sector, NGO’s, etc. One of the most active contributors to the activities of the Safer Internet Center is ISOC-Bulgaria. |
|  | Denmark [(INF/19)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0019/en) | **Protecting children and young people from abuse and exploitation** Safer Internet Centre Denmark consists of three well established and experienced organizations. The Media Council for Children and Young People is appointed as the Awareness Centre with the main task to serve as a knowledge hub and mediator of the newest developments within the area of children and young people’s use of online technologies and therebywe inform and educate on a safe and positive use of digital media. Save the children Denmark upholds the task as a hotline where anyone can report online child abuse images. Centre for Digital Youth Care is the centre’s helpline as they offer online counseling to all children and young people in Denmark.  Since 2004 Safer Internet Centre Denmark has established a strong national stakeholder network of different organizations in Denmark – all with a focus and interest in children and young people’s use of online technologies. The network is an important resource and knowledge base for the Safer Internet Centre Denmark, just as the centre plays an important role in the organizational and political landscape of children and young people’s use of online technologies. The Safer Internet Centre Denmark has established a national advisory board to steer and inspire the centre in the right direction. This board consists of representatives from academic institutions, the industry, governmental bodies and law enforcement.  Besides the day-to-day activities, the main focus is set on empowering children, parents, primary, secondary and high schools in all aspects of Media Literacy. A part of these activities corresponds closely to point 11 regarding “Respect for privacy and the protection of personal information and data”, in the sense that the Safer Internet Centre Denmark encourages the dialogue between generations on children and young people’s digital culture and their understanding of privacy and fundamental rights in the digital age.  For the time being the future of the European network of Safer Internet Centers is uncertain. It is possible that the Safer Internet Network will continue within the framework of EU’s Connecting Europe Facility Program, but the situation is not clarified. |
|  | India [(INF/37)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0037/en) | **Providing a consistent domestic legal framework for :**  **Protecting children and young people from abuse and exploitation**  It is the role of the Indian government to determine how strictly such norms are being followed in the cyber world through proper policy formulation and regulation. The Information Technology Amendment Act 2008 under Section 67B deals with Child Pornography i.e. persons who have not completed 18 years of age, for the purpose of this Section. |
|  | Iraq [(INF/9)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0009/en) | * Preparation of a special blog on protecting children on internet named “Guidelines for the protection of our children from internet risks”, see [www.cmc.iq/ar/pdfcmc/childsafty.pdf](http://www.cmc.iq/ar/pdfcmc/childsafty.pdf) |
|  | Japan [(INF/23)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0023/en) | **Actions undertaken by governments**  The government of Japan has established basic frameworks for this issue and the government has promoted voluntary actions taken by multi-stakeholders.  For example, to improve Internet literacy in young people, the government of Japan intends to uncover the actual state of the Internet literacy. To that end, Japan develops an indicator (Internet literacy Assessment indicator for Students), conducts tests and utilizes their results for educational activities to improve literacy.  In addition, the government of Japan supports several voluntary actions implemented by the private sector:  For example,   * The government of Japan established “Act on Development of an Environment that Provides Safe and Secure Internet Use for Young People” in order to support private sector’s voluntary actions and promote diffusion of filtering technologies. * The government of Japan participates in private-led voluntary meetings on measures to prevent the distribution of child pornography　(ICSA oversight committee), as an observer.   **Actions to be undertaken by governments**  As basic principles, governments should review the implementation situation of past policies and establish basic frameworks and promote voluntary actions by multi-stakeholders.  So, governments should continuously implement programs on online youth protection. |
|  | Korea [(INF/25)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0025/en) | * + - * 1. **Protecting children and Young People from Abuse and Exploitation**   This section is described in the Section VII (Use and Misuse of the Internet). |
|  | Lithuania [(INF/11)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0011/en) | **Protecting children and young people from abuse and exploitation** (issuse 12 in Annex 1)   * **Implementation of the Safer Internet Project**   In view of potential online threats to the children, the need for public awareness raising in this area and control for illegal and harmful content, since 2007 RRT implements the European Union Safer Internet programme and, in cooperation with the Centre of Information Technologies in Education (ITC) and other partners executes the Safer Internet project. The main tasks of the project are public awareness raising on the issues of safe use of the Internet, fighting illegal and harmful content and behaviour, especially images of sexual abuse of children, cyber bullying, sexual harassment and grooming on the Internet.  In 2007, a hotline was established by RRT, which responds to reports of illegal content and aims at its elimination from the Internet as soon as possible. When performing the hotline functions, in 2013 RRT received and investigated 650 reports on illegal or harmful content on the Internet. In cases, whereby the hotline identified that the Lithuanian laws might have been violated due to illegal or harmful Internet content, the collected materials were submitted to the competent institutions in Lithuania and abroad for further investigation and in most cases removed from the Internet as a result of the investigation.  The Safer Internet project comprises such awareness raising tools as educational events and series of classes to school students throughout Lithuania, dissemination of educational information on safe use of the Internet, the Internet hotline activities and the Safer Internet helpline, which was established in 2011. The aim of the helpline is to provide emotional help to the parents and to the children over the phone and internet when encountered with an intimidating contact, behaviour, harmful content and other unpleasant or intimidating experience using internet technologies.  Starting with October, 2012 RRT is a partner in implementing a new Safer Internet 28-month project in Lithuania and RRT is responsible for operation of the internet hotline. A hotline established by RRT is a member of the International Association INHOPE since May 2008. The membership in this association paves the way for closer cooperation with hotlines of other countries and facilitates information exchange in order to eliminate illegal or harmful content from the Internet more efficiently. INHOPE is the International Association of Internet Hotlines coordinating a network of Internet Hotlines all over the world, comprising a network of 46 Hotlines in 40 countries. Major attention is devoted by INHOPE for prevention of sexual child abuse on the Internet. RRT takes part in INHOPE General Assemblies, its Executive Board and other meetings. |
|  | Mauritius [(INF/20)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0020/en) | (a) To protect children online and young people from abuse and exploitation, a Child Safety Action Plan was endorsed by Government and its implementation started in 2009. Since then, a number of activities are being organised e.g. awareness campaigns in the context of the Safer Internet Day.  (b) The ICT Authority launched an Online Child Sexual Abuse Reporting Portal (OSCARP) on 24 October 2013. The portal enables Internet users in Mauritius to report any websites depicting Child Sexual Abuse (CSA) content. The ICT Authority signed a Memorandum of Understanding with the Internet Watch Foundation, UK in that context. |
|  | Moldova [(INF/12)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0012/en) | **Protecting children and young people from abuse and exploitation**  Law Nr. 30 dated 07.03.2013 on child protection against harmful effect of information was approved. |
|  | Morocco [(INF/32)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0032/en) | **Protecting children and young people from abuse and exploitation in Morocco**  Internet is now an interesting element of children and young people’s lives. It can bring considerable benefits for their education and development; however it also exposes them to online risks such as access to inappropriate content, abuse and online exploitation … Protecting children and young people from the online risks is a priority for the Moroccan government.  In the Moroccan National Strategy for Information Society and Digital Economy “Digital Morocco 2013”, the Government within the framework of the digital trust plan sets the following initiatives and actions in order to protect online children and young people and help them to use the cyberspace safely.  **Initiative 1: Update and reinforce the legislative framework**   * Upgrade/update the legal and regulatory framework related to the protection of children and young people from the risks of Internet abuse and online exploitation.   **Initiative 2: sensitise parents, citizens, and education staff to information systems security**   * Raise awareness within the children, young people and parents of the Cybersecurity and cyberconfidence issues, * Implement a sensitization and a communication program about ISS in order to raise awareness within the children, young people, parents and education staff of Cybersecurity and cyberconfidence issues,   **Initiative 3: International cooperation**   * Strengthen the international cooperation on protecting children online and combating cybercrime   **Realizations**  As a result of actions undertaken within the framework of the digital trust program to protect children and young people from the risks of Internet, abuse and online exploitation, government has succeeded to:  **Initiative 1:**   * Adopt the law no 07-03 related to the information Systems infractions, * Adopt the law no31-08 related to the protection of on line consumers, * Adopt the law no 09-08 related to the protection of the personal data, * Elaborate a global study of the legal instruments related to the information technology and cybercrime to strengthen the Moroccan legal act and fill existing gaps that may be an obstacle to ensure the digital trust, combat cybercrime and protect children and young people from the risks of Internet, abuse and online exploitation.   In addition, and in order to strengthen its legislation governing ICT / digital confidence and ensure its harmonization with international / regional conventions, Morocco has adopted the following laws:   * Law No. 136-12 approving the Convention No. 185 of the European Union on Cybercrime and its Additional Protocol, * Law n°75-12 approving the Arab Convention against information technology crimes.   **Initiative 2:**   * Implement an awareness and communication program about cybersecurity and safe internet for parents, education staff, children and young people, * Develop an information website that content advices and recommendations for parents, children and young people to develop their skills about information system security and help them to adopt the internet and networks security tools   **Initiative 3:**   * Moroccan government is developing and enhancing his International partnership to protect children online and combat cybercrime |
|  | New Zealand [(INF/34)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0034/en) | *Please refer to Section 5.* |
|  | Norway [(INF/35)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0035/en) | **Protecting children and young people from abuse and exploitation**  Norway has for many years worked coordinated with many stakeholders in protecting children from online abuse. Norway established in 2004 cooperation between law enforcement and Internet Service Providers to implement a filtering service to fight sexually abusive images of children on the Internet. Almost all Internet Service providers now work collectively with the law enforcement in maintaining this service.  Norway has taken active part in relevant EU programs such as Safer Internet plus program and Safer Internet programme from 2005-2013, where the intentions where aimed at promoting safer use of Internet and other communication technologies, to educate users, particularly children, parents and carers and to fight illegal content and harmful conduct online such as grooming and bullying. This work have also resulted in good cooperation between government agencies, businesses, software providers, the technical community and other stakeholders in establishing and maintaining online resources to raise awareness, arrange national conferences and meetings focusing on protecting children online.  Norway also appreciate the work of the Council Working Group on Child Online Protection and their effort to raise awareness on protecting children online and to provide assistance and support to the Member States, especially developing countries, in developing and implementing roadmaps for the Child Online Protection initiative. |
|  | Oman (ITA) [(INF/2)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0002/en) | OCERT Child Online Protection (COP) initiative is aiming at protecting children online through adopting the ITU GCA measures (org structure, legal measures, capacity building, technical and procedural measures and international cooperation). The program includes educating children, teachers and Parents about children Security Risks and equipping them with tools, knowledge to manage the risks. |
|  | Paraguay [(INF/29)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0029/en) | **Protecting children and young people from abuse and exploitation**  The Constitution, international conventions and agreements approved and ratified by Paraguay, Public Ministry (Attorney General office) ([www.ministeriopublico.gov.py](http://www.ministeriopublico.gov.py)) and the Ministry of Children (<http://www.snna.gov.py/seccion/4-marco-normativo.html>), work together with internet access providers in monitoring sites that might harbor child pornographic content. Furthermore, these ministries ask for information to owners of servers that are outside of Paraguay with related storage. |
|  | Poland [(INF/17)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0017/en) | **Protecting children and young people from abuse and exploitation**   * 1. **UKE** * On 2 July 2009, the President of UKE signed an Agreement on Safety of Children on the Internet. This agreement is a voluntary contribution of all signatories to ensuring children's safety on the Internet. Special emphasis was put on fighting illegal Internet content, such as illegal pornography and hate speech. * On 23 December 2009, the Office of Electronic Communications concluded an Agreement on cooperation with F-Secure Sp. z o.o. under which an information and education website was established at [**www.przyjaznynet.pl**](http://www.przyjaznynet.pl)**.** The website contains information on safety on the net, taking particular account of the children, as well as information on technological solutions, such as parental control, ensuring maximum protection of the user and of end user's terminal devices against cybercrime. In addition, [www.przyjaznynet.pl](http://www.przyjaznynet.pl) promotes certification of telecommunications services in the "Safe Internet" category. * Certification of telecommunications services is a programme managed by the Office of Electronic Communications from 2009 onwards. The ITU Council resolution 1305 of 2009 is implemented as part of the certification programme of telecommunications services for the "Safe Internet" category. The certification in this category aims at encouraging activities from telecommunications undertakings to ensure safety to network users, including primarily children and young people, and to improve the quality of services provided. The President of UKE in this way wants to stress the problem related to their safety on the net and to create the need for using tools available in the market that may ensure the highest possible protection against cybercrime. * As part of implementation of the ITU Council resolution 1305 of 2009, the President of UKE joined on 23 September 2013 the Action Programme for protection of children against Internet pornography that is led by the Ministry of Administration and Digitization. The programme aims at increasing parental awareness of issues related to the Internet use and at improving their digital skills, which should result in more effective use of technical solutions that protect children against harmful content on the net. * Moreover, there is a permanent section on safety on the net on the website of the Office of Electronic Communications – [www.uke.gov.pl](http://www.uke.gov.pl) → Konsument → Bezpieczeństwo w sieci. This section contains up-to-date information on incidents related to Internet safety as well as advice to draw the attention of users, primarily children, their parents and guardians and Internet website creators, to the issues of children's safety on the net. Different contests promote also solutions which make the Internet use safe. * In addition, in order to increase protection of telecommunications services (including the Internet) consumers’ rights, the President of the Office of Electronic Communications operates a Consumer Information Centre (a hot line and a website at [www.cik.uke.gov.pl](http://www.cik.uke.gov.pl)) where subscribers may receive help and advice on safe use of the net or basic protection against specific risks.   1. **NASK**   + Resilient participant of European Commission’s programmes Safer Internet and BIK Net   + Co-founder of the KURSOR educational project promoting use of new technologies at school, as well as student protection literacy on-line.   + Co-founder of other projects in that field: “*Adventures of File and Folder On-line*”, “*Senior for senior*”, “*Safe Internet Avenue*”, “*Science Festival*”, “*Science picnic*”   + Direct trainings targeting the young, teaching staff, parents and police officers   + The ABIT programme (*Safe Internet Academy*) – a series of free trainings (co-financed by European Union funds) for the 50+ and the visually impaired aiming at enhancing computer literacy.   + Co-organizer of Safer Internet Day   + Series of nation-wide conferences “Innovative Education” organized in all 16 voivodships;   + Expert seminars on cyberbullying, sexting, addictions   + Organizer of the international annual event “Safety of children and young people on-line”   + Carrying out of a joint research study on the use of video-chats by minors for explicit contents. |
|  | Portugal [(INF/5)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0005/en) | **Protecting children and young people from abuse and exploitation**  Please refer to section 7.  The Portuguese law criminalizes various actions while using electronic communications that violate the rights and interests of children.  Besides the Budapest Convention, Portugal has ratified the 2007 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Decree n.º 90/2012 of the Presidency of the Republic, 27 of October). Portugal is also member of the Global Alliance against Child Sexual Abuse Online launched in 2012. |
|  | Qatar [(INF/14)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0014/en) | **Protecting children and young people from abuse and exploitation :**  MICT is committed to helping people in Qatar stay safe online, with a primary focus on children. Staying safe online requires the involvement of the entire community. MICT is working directly with teachers and parents to educate them about keeping their children safe online, while being smart in their own practices.  MICT Cyber Safety program is working closely with Q-CERT team to launch [safespace.qa](http://www.safespace.qa), a comprehensive online safety resource to help protect children online. This website provides educational games and tips, along with up-to-date information to help parents and teachers protect kids from cyber-bullying and other dangers. To further supplement these efforts, ictQATAR is creating a hotline for families and educators to report online threats and receive guidance on how to handle specific situations. |
|  | Russian Federation [(INF/27)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0027/en) | Governments should develop and adopt legal and regulatory frameworks protecting children and young people from abuse and exploitation.  Coordinate efforts with other countries to combat terrorism ideas in the Internet, taking also in consideration that terrorist groups use the Internet not only to advocate their ideas, but to recruit new supporters and sometimes coordinate their activities.  Support efforts to improve the media literacy. Citizens should have skills and capabilities to keep private their personal data, safeguard their children from information harmful for their life and health, and avoid becoming the victims of fraud. As well as to distinguish credible information from fiction outright misinformation distinguish verified information from dubious sources. |
|  | Rwanda [(INF/13)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0013/en) | **Protecting children and young people from abuse and exploitation**  In 2007, Rwanda took a step towards its long-term goal when it became the first country in the East African Community and the third on the African Continent to join “One Laptop per Child” program. This international initiative aims to introduce computers to the pupils of developing countries in an effort to bridge the global digital divide. With this achievement, Rwanda is now on track to achieving the 2015 MDGs and Vision 2020.  The Government of Rwanda established the National Commission for Children (NCC). The establishment of that Commission represents a major fulfilment of the commitment made to ensure protection of Children.  In 2012, Rwanda enacted the Law relating to the Rights and the Protection of the Child. The penal code has specific provisions that deal with offences regarding abuse and exploitation of children.  Rwanda ICT regulator took initiative to ensure that all subscribers of mobile cellular services be registered. The SIM cards registration exercise intends to address several security and social issues including abuse and exploitation of children. |
|  | Saudi Arabia & Bahrain [(INF/31)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0031/en) | **Actions to be undertaken by Governments**  Develop international public policies to deal with protecting children and young people from abuse and exploitation and prosecute abusers. Actively seek out abusers operating within their territories and cooperate with other nations who are victims of abuse.  **Actions which have been undertaken by Governments**  A number of countries are actively involved in discussions of protection of young people and/or have national policies and laws related to such protection. However, no mechanism exists yet to put in place meaningful, agreed and enforceable international public policies in this area. Though some amount of bilateral or multilateral cooperation is being developed based on the evolution of existing discussions and forums, bilateral agreements are not the answer. |
|  | Sudan [(INF/3)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0003/en) | The Sudanese CERT (cert.sd) was established by NTC to undertaken these issues. |
|  | Sweden [(INF/28)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0028/en) | **Protecting children and young people from abuse and exploitation**  Sweden supports industry self-regulation. The ITU working group on child online protection can have a role to follow up and publish which social networking providers have policies and corrective actions that aims to protect children and young people from abuse and exploitation.  Sweden participates in and supports the Financial Coalition of banks against child pornography that counteract sexual abuse images of children by preventing payments in the financial systems. The Swedish government supports the private led project where network providers in voluntary cooperation with police block access to child porn websites. Sweden continuously follows the development in the area. |
|  | Switzerland [(INF/4)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0004/en) | In 2012 the Swiss federal council adopted a national program on youth media protection and media skills. The objectives of the program are the promoting of the safe, age-appropriate and responsible use of digital media by children and young people. On the website [www.jugendundmedien.ch](http://www.jugendundmedien.ch) (in French, German and Italian) targeted information for parents, teachers and specialist personnel is published for appropriate mentoring of children and young people in media education. The update of the information and specific projects in the field of youth media protection are realized in collaboration with representatives of the federal, cantonal and scientific institutions, the Cybercrime Coordination Unit Switzerland (CYCO) as well as with representatives of the media and private sector, teacher training colleges and parents and students associations. |
|  | United Kingdom [(INF/22)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0022/en) | The UK government’s view is that issues around addressing online abuse is everyone’s responsibility. The UK Council for Child Internet Safety (UKCCIS), brings together more than 200 organisations across UK government; ICT industry; regulators; law enforcement; academia and relevant charities has provided a good basis to coordinate appropriate responses and actions on this issue.  The UK government is also working with industry partners to ensure the availability of tools to enable parents to take more active control over the content their children see.  The UK government has also given a proactive role to the UK Internet Watch Foundation (IWF) to detect offending websites and passing on relevant information on to enforcement agencies where appropriate. |
|  | United States [(INF/33)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0033/en) | **Protecting children and young people from abuse and exploitation**  Governments have a clear responsibility to protect children and young people from abuse and exploitation. Online exploitative behavior should be criminalized and strictly enforced. The United States has strong record of investigating and prosecuting online criminal activity that endangers children.  With respect to protecting children from online content that might be objectionable, but is otherwise legal, the United States encourages user education and awareness raising activities that give parents and guardians (as end users) the tools they need to encourage responsible online behavior and protect children. The United States strongly supports such voluntary and collaborative efforts that empower users and protect children without filtering or blocking content.  There are a number of international resources to assist governments in establishing criminal frameworks and protecting children online. UNODC is the sole venue within the UN system for member states to address the policy, investigation and prosecution of cybercrime, including crimes against children. Global Alliance Against Child Sexual Abuse Online is a joint initiative by the EU and the United States, which was launched in December 2012. Over fifty countries are now participating, and have committed to step up their efforts to protect children from online sexual exploitation. ITU-D’s Question 22-1/1 provides a venue for member states to share national experiences and discuss best practices in protecting children online. |
|  | Uruguay [(INF/21)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0021/en) | - National awareness campaign “safe-connected”, with recommendations for the use of Internet.  - Protection in navigation through the Red Ceibal (Uruguay’s OLPC program network) and training of teachers on safe navigation.  - National awareness campaign “Your data are worth. Take care of them” and the contest “How do you explain what Personal Data are?”, aimed to children and young people in public and private schools.  - Addition of a module on children and adolescents to the Survey on ICT access and use.  - Under the scope of the Inter-American Telecommunication Commission, Uruguay and other Latin American countries are working on having a website where children can contact the specialized agency of each country, including IP toll-free calls.  - Participation in Regional SG2 ITU-T to promote the CITEL initiative on using a smartphone app as a viable alternative to the unique global number identification for the “Child Helpline International” project.  - Specific regulation on children and young people abuse, pornography and sexual violence. |
|  | Zambia [(INF/16)](http://www.itu.int/md/S14-RCLINTPOL4-INF-0016/en) | **Protecting children and young people from abuse and exploitation**  Criminal law in Zambia generally protects children from any form of abuse (Penal Code, Chapter 87). Further, Zambia is a signatory to the United Nations Convention on the Rights of the Child. The Government has enacted the ECT Act No 21 of 2009 which has enhanced a safe, secure and effective environment for the consumer, business and the the government itself of effectively use the internet.  The regulator also conducts regular awareness programs targeted at the young primarily conveying the importance of taking responsibility for their actions in cyberspace, and teaching them “good” practices while not restricting them from enjoying the benefits thereof. |

1. under the Ministry of Science and Higher Education, www.nask.pl [↑](#footnote-ref-1)
2. http://www.oecd.org/sti/ieconomy/50305352.pdf [↑](#footnote-ref-2)
3. www.man.poznan.pl [↑](#footnote-ref-3)
4. www.pionier.net.pl [↑](#footnote-ref-4)
5. http://www.oecd.org/internet/innovation/48289796.pdf [↑](#footnote-ref-5)
6. http://a4ai.org/policy-and-regulatory-best-practices/ [↑](#footnote-ref-6)
7. www.pg.edu.pl [↑](#footnote-ref-7)
8. www.pw.edu.pl [↑](#footnote-ref-8)
9. Facilities to manage geographically dispersed data with a view to making it available to research centers. [↑](#footnote-ref-9)
10. www.abw.gov.pl [↑](#footnote-ref-10)
11. www. msw.gov.pl [↑](#footnote-ref-11)
12. http://n6.cert.pl [↑](#footnote-ref-12)
13. National regulatory authority, www.uke.gov.pl [↑](#footnote-ref-13)
14. www.uke.gov.pl/badz-swiadomy-zagrozen-w-sieci-12885 [↑](#footnote-ref-14)
15. www.cik.uke.gov.pl [↑](#footnote-ref-15)
16. http://www.uke.gov.pl/nie-tylko-cena-przejrzyste-wskazniki-jakosci-uslug-13191 [↑](#footnote-ref-16)
17. www.uke.gov.pl/files/?id\_plik=10272 (sample report). [↑](#footnote-ref-17)
18. www.uke.gov.pl/files/?id\_plik=7350 [↑](#footnote-ref-18)
19. www.uke.gov.pl/files/?id\_plik=10826 [↑](#footnote-ref-19)
20. Tromboning is a common process whereby local ISPs exchange traffic over transit routes provisioned by international backbone operators [↑](#footnote-ref-20)
21. https://www.netacad.com/web/about-us/about-networking-academy [↑](#footnote-ref-21)
22. “Socio-economic Impact of Internet in Emerging and Developing Economies.” The Boston Consulting Group commissioned by Telenor (2009). [↑](#footnote-ref-22)
23. Lifting barriers to Internet development in Africa: suggestions for improving connectivity, The Internet Society; May 8, 2013; http://www.internetsociety.org/doc/lifting-barriers-internet-development-africa-suggestions-improving-connectivity [↑](#footnote-ref-23)