# Internet Governance Forum 2010:

# Developing the future together

Fifth meeting of the Internet Governance Forum

*Vilnius*

*14-17 September 2010*

Internet Governance Landscape
Background paper

Prepared by the secretariat of the Internet Governance Forum

August 2010

# Introduction

1.        This background paper is intended to provide information for discussion during the fifth meeting of the Internet Governance Forum (IGF). It gives an overview of the topics on the agenda and builds on the discussions at the first four IGF meetings and the papers that were submitted for discussion at those meetings. The transcripts of sessions, workshop reports, Dynamic Coalition statements and submissions can be found, in full, on the IGF website.[1] Those materials should be consulted by anyone seeking a more comprehensive picture, as the present background paper cannot do justice to the full breadth of the discussions and submissions.

2.        The agenda for the meeting was announced by the United Nations Under-Secretary-General for Economic and Social Affairs in his invitation[2] to all stakeholders. The agenda is as follows:

a)   Managing critical Internet resources;

b)   Security, Openness and Privacy;

c)   Access and Diversity;

d)   Internet governance for development (IG4D);

e)   Taking stock of Internet governance and the way forward;

f)   Emerging issues: cloud computing.

## I.        Internet governance Forum 2010: Developing the future together

3.        The theme for the current meeting, "IGF 2010: Developing the future together", marks a progression when viewed against the themes of the previous IGF meetings,

- "Internet governance for development" (2006 and 2007),

- "Internet for all" (2008)

- "Internet Governance – Creating Opportunities for All" (2009).

Those earlier themes have been linked to the cross-cutting priorities of development and capacity-building. They are derived from the World Summit on the Information Society (WSIS) and in one form or another have motivated all IGF discussions to date.

4.        Since the inception of  the IGF, there has been a general understanding that it should have an overall development orientation that includes capacity-building as a cross-cutting priority. Discussions on capacity-building in development have centred on the importance of fostering the ability and knowledge of all stakeholders to participate in Internet governance processes.

5.        Development in the context of Internet governance has meant more than providing access to the Internet to the billions of people currently unable to use it. It has meant providing access to such people in their own languages and with content relevant to diverse cultures. Development has also been discussed as critically important to persons with disabilities and those who are otherwise disadvantaged, such as minorities and elderly people, as a means of ensuring that the Internet provides services that improve their lives and help to make them more fulfilling. The Internet has been seen as a platform for greater dialogue aimed at encouraging tolerance, mutual cooperation and social cohesion. Among the important considerations frequently emphasized has been the importance of using universal design principles in designing future applications, so that they are useable by people who have disabilities or are otherwise disadvantaged.

6.        Participants at previous IGF meetings have observed that there is a link between sustainable development and Internet governance. Decisions by policymakers on how to expand infrastructure to reach the billions of underserved people have long-term implications for the environment, which in turn affect the sustainability of the infrastructure itself. Specific discussions have been held on green Information and Communication Technology (ICT), which juxtapose the environmental impact of the ICT industry with the contribution that the industry can make to reducing the environmental impact of other industries through, for example, monitoring, measuring and tackling climate change and enabling behavioural and economic changes aimed at reducing industrial carbon demand. With the current meeting approaching, global concerns again came to the fore with regard to the economy and global environmental issues and energy

---

problems. Many contributors said that the Internet and ICT should have a major role to play in solving those global challenges.

7.　　　　Speakers have noted that the success of the Internet had been based on collaboration. In the same way, the IGF had managed to bring on board all the relevant stakeholders and key players to work cooperatively on the crucial development role of the Internet and especially on the removal of barriers to participation by developing countries.

8.　　　　Speakers over the years have acknowledged that with opportunities came rights and responsibilities, and that in the future, the IGF should address important issues such as cross-border security, young people's Internet experience, multilingual content, and enhanced broadband capacity in developing countries.

9.　　　　During the 2009 IGF meeting, Sir Tim Berners-Lee, creator of the World Wide Web and Director of World Wide Web Consortium (W3C), emphasized the importance of a single Web that could be shared and used by all. He noted the importance of the Web to enhance the lives of people with disabilities. The theme of enhancing the lives of people with disabilities has been apparent in the discussions of the IGF since the beginning.

10.　　　　Over the years, as the discussion of the subject deepened, the participants have begun to speak about the interrelation of many of the themes discussed in the IGF. The participants have also spoken of the importance of discussing the themes in relation to actual cases so that the interaction of the thematic elements can be better understood.

11.　　　　 During the 2010 preparations the focus was on several areas including:

- The balance of security with rights in the context of ICTs;

- The issues involved in the emerging topic of Cloud Computing;

- The specific issues involved in Internet governance for development.

## II.　　　Managing critical Internet resources

### A.　　　Overview

12.　　　　The theme "critical Internet resources" was first introduced at the second IGF meeting, held in Rio de Janeiro, Brazil, in 2007. It was also dealt with at the third meeting in Hyderabad, India, in 2008 and the fourth meeting held in Sharm El Sheikh in 2009. There is no universally recognized definition of the term "critical Internet resources". It was introduced into the international debate by the Working Group on Internet Governance in 2005, whose report (paragraph 13 (a)) gave the following description of a policy area connected to critical Internet resources:

> Issues relating to infrastructure and the management of critical Internet resources, including administration of the domain name system and Internet protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multilingualization.

13.　　　　The Tunis Agenda, in paragraph 58, refers to critical Internet resources as follows:

> We recognize that Internet governance includes more than Internet naming and addressing. It also includes other significant public policy issues such as, inter alia, critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet.

14.　　　　The discussions at these meetings often referred to the Geneva Principles and the Tunis Agenda regarding Internet governance, in particular the notion that the "international management of the Internet should be multilateral, transparent and democratic, with the full involvement of Governments, the private sector, civil society and international organizations".[3]

15.　　　　The discussion of critical Internet resources has covered many issues and has extended to the cross-cutting theme of capacity-building and the other IGF themes of access and security, in addition to Internet routing and the basic need for electricity. Those issues have all been said to be critical to the Internet's development in its continuing deployment and evolution. The primary focus, however, has remained on domain names and Internet Protocol (IP) addresses, and the Internet Corporation for Assigned Names and Numbers (ICANN) as the organization responsible for their management.

---

[3]　Geneva Declaration of Principles, para. 48 and Tunis Agenda, para. 29.

16.　　　　Some have argued that ICANN should be placed under intergovernmental oversight, rather than under the oversight of a single Government. Others have pointed out that the Internet has evolved securely and flexibly and that it functions well under the current governance structure; they advised against any sudden introduction of an intergovernmental governance system.

17.　　　　Arguments made over the years have called for a fair distribution of resources, facilitating universal access and ensuring the sustained and secure functioning of the Internet, with due allowance for multilingualism.

18.　　　　The discussions on critical Internet resources in IGF meetings have also covered, among other issues:

　　　　(a) Management of root servers;

　　　　(b) Standards;

　　　　(c) Interconnection points;

　　　　(d) Telecommunications infrastructures, including converging and innovative technologies;

　　　　(e) Digital object identifiers;

　　　　(f) ENUM (Electronic Numbering);

　　　　(g) Radio spectrum, backbone and Internet service providers (ISPs);

　　　　(h) Regional management activities such as Regional Internet Registries (RIRs);

　　　　(i) Transition to multilingualism.

19.　　　　The issues to be covered in the 2010 critical Internet resources session include:

- Priorities for the long term stability of the Internet;
- New gTLD and IDNs for development: Importance and Obstacles;
- Strengthening ccTLDs in Africa;
- IPv6 around the world: surveying the current and future deployment of IPv6;
- Resilience and contingency planning in DNS.

20.　　　　During 2010 several milestones have occurred in the Internet including the DNSSEC signing of the root and the introduction of the first IDN ccTLDs into the root. These changes in the Internet are expected to affect the discusions in Vilnius.


## B.　　　Transition from IPv4 to IPv6

21.　　　　The eventual exhaustion of unassigned IPv4 addresses has been a recurrent theme of IGF meetings. Projections were reported that, at the present rate of depletion, IPv4 address space could be exhausted by next year, 2011. While it was made clear that this depletion would not cause the Internet to fail, it was used to indicate the importance of the effort to bring the IPv6 network online and the need for full interoperability between the IPv4 and IPv6 networks. Some suggested adopting policies that would encourage IPv6 connectivity among all ISPs. Others expressed the view that there was no need to impose a deadline to forestall the inevitable, because the market was dictating IPv6 deployment. It was also noted that there was a great need for the private and public sectors and civil society to be involved in the process. It was a shared responsibility and one that required the promotion and enabling of a smooth transition from IPv4 dominance to IPv6 dominance.

22.　　　　It was felt that there was a need for public awareness and education, in addition to training. IPv6 needed to be highlighted as part of the national agendas of all countries. It was also said that it would be useful and helpful if, as part of the education process, case studies were made available and published, for example on the IGF website.

23.　　　　IPv6 was seen as a continuation of IPv4 with additional addresses. There was also, however, a discussion of the impact that the transition would have on technical processes. Because of incompatibilities between the two versions, every IP-based product would be affected; IPv6 equipment was on the market and vendors were supporting and migrating applications to IPv6. It was explained that the use of dual IPv4 and IPv6 protocol stacks and a focus on developed countries taking the initiative in promoting the use of IPv6 addresses was a response to the limited availability of IPv4 addresses.

24.　　　　IPv6 addresses were being deployed and a lot of IPv6 equipment, devices, and applications were available. Governments in particular had paid more attention to IPv6, and many had led deployment initiatives. Operators had been slow to take up IPv6. That was attributed to the number of challenges that

they were facing, such as there being no obvious commercial driver for network operators to move to IPv6 and there being expenses but no revenue associated with the migration to the new address format. There was also no initial customer demand and operators were believed to have perceived that there was insufficient vendor support. Operators were, however, beginning to recognize that the time for migrating had come and were doing so incrementally. There would be a need to resolve hardware and software issues in their customer-premises equipment and in customer equipment and there would be costs associated with migration, hardware and software ,and training, together with labour costs of converting.

25.        In such an emergent environment, it was felt; the role of RIRs might be changing. The scarcity of IPv4 would demand that RIRs look at and develop policies for the transfer of IP address space, reclaiming and obtaining control of unused address space, ensuring the security of and managing new IPv6 addresses and handling the emergence of possible secondary markets. There was also discussion of how to deal with the many unused and unaccounted for IPv4 addresses. Some were in favour of creating a legal market for those addresses, thereby preventing sales from being limited to the black or grey markets.

26.        In the future, IPv4 would remain, even when IPv6 became dominant. It was noted that it was important not to think of the transition as a single event like Y2K, but rather as a process of deployment.

27.        Many speakers in the past, including governments and the ITU, have emphasized the importance of training and awareness raising on this topic.

## C.        The Affirmation of Commitment, the Internet Assigned Numbers Authority contract and the role of Governments

28.        Over the years, there have been discussions on the future of ICANN in the context of the discussion of the joint project agreement between that body and the Department of Commerce of the United States of America. With the expiration of the agreement in September 2009, and the signing of the Affirmation of Commitments, 2010 has seen the creation of the first one of the Affirmation of Commitment review teams dealing with accountability and transparency. The Vilnius meeting offers a good opportunity for an initial view into how this is working and whether it is meeting expectations.

29.        A number of speakers over the years have said that the United States Government should step down from its pioneer role in the oversight of the DNS. In general, they held the view that the agreement should not be continued. Opinions were expressed, however, that some method of accountability should be introduced as a replacement. It was suggested that the IGF could provide a space for further developing such ideas.  The ITU has also expressed interest in such a role.

30.        A number of comments from government representatives have been recorded indicating caution about subjecting the Internet to intergovernmental controls.  Some governments, however, have indicated that intergovernmental controls are required.

31.        Among the topics discussed during previous IGF meetings was the essential bottom-up nature of the ICANN processes and the requirements for their regular external review. Other points covered the relationship of Governments with ICANN and whether it was appropriate for the Government Advisory Committee (GAC) to play only an advisory role as opposed to one that would entail fuller powers in terms of international public policy, such as oversight or review. It was argued both that the participation of Governments in GAC was one of the most important features of ICANN, and, on the other hand, that the current model with GAC as part of ICANN was unstable.

## D.        Internationalization of critical Internet resources management

32.        The subject of internationalizing the management of critical Internet resources has been discussed frequently during IGF meetings, with a variety of voices and positions being heard.

33.        One of the frequent arguments made against a system of governance for critical Internet resources by a Government-led international body is that it would not be capable of the rapid decision-making that is necessary in the management of the Internet. Others have commented that the current processes are not very rapid as they need to take the time to take into account the views of all stakeholders. Some speakers have voiced support for the largely unregulated environment that allowed the Internet to grow, pointing out that the Internet has been able to thrive in a wide variety of market environments under competitive conditions and should therefore remain free of centralized regulation. Others have spoken about the need for regulatory process to be introduced into the Internet environment.

34.        While some participants generally supported ICANN being independent of Governments, others said that Governments should play a more significant role and that they should be allowed, on an equal footing, to play their sovereign role in global public policymaking. In that respect, current ICANN reforms, and the perspectives for the recognition of ICANN as an international entity and its independence from any Government, have been followed with interest.

35.    The proposal was made that the Secretary-General should establish a special multi-stakeholder working group on critical Internet resources within the IGF framework. That group's work would include discussion of the gradual transfer of Internet governance to the authority of the international community.

36.    Various speakers have described the process by which policies that control the allocation and management of numbers within RIRs as one developed through an open, bottom-up process that engages the entire Internet community. That is seen as a self-regulating process that could serve as an example for other governance processes.

## E.    Importance of new top-level domains and internationalized domain names for development

37.    Over the years there has been much discussion during IGF meetings of Internationalized Domain Names (IDN) in the context of enabling diversity and as a prerequisite to multilingual development goals of bridging the digital divide. During 2010 new Internationalized Domain Name Country Code Top-Level Domains (IDNccTLDs) were released by ICANN.

38.    The first few ccTLDs are the start, there have been discussions on the need to support ccTLD technical operations and management in developing countries. Concern has been expressed that as new TLDs were introduced, the rich culture of Africa would need to be protected, so that the values, culture and history the identifiers might seek to represent could be managed by people from those countries and regions.

39.    Some of the more visible issues in the area have included:

(a) Stability and security of the Internet as the number of names increases;

(b) Protection of trademark rights;

(c) Risks of increased malicious use of the Internet;

(d) Competition and the respective roles of IDN, generic TLDs (gTLDs) and IDN country code TLDs (ccTLDs).

## F.    Enhanced cooperation

40.    During the first two IGF meetings there were varying views expressed on whether the concept of "enhanced cooperation", as defined by the Tunis Agenda, should be discussed. While some felt that that topic did not fall within the purview of IGF, others agued that it was an essential responsibility. Discussions at the third IGF meeting for the first time covered enhanced cooperation.

41.    All speakers highlighted aspects of how discussions of enhanced cooperation were having a positive impact. Examples mentioned included actions to combat child abuse images in Brazil, the extended involvement of stakeholders in the 2008 Organisation for Economic Cooperation and Development (OECD) ministerial meeting and improvements in the way in which IP address registries interacted with relevant stakeholders.

42.    The third meeting left participants with a broader understanding of various stakeholder positions on the issues. It was suggested that IGF had a valuable role as a non-threatening environment for discussion, where participants could talk, share practical experiences from various perspectives and move to the point at which people listen to one other, progressing from a disconnected series of statements to an engaged conversation.

43.    Some speakers considered IGF itself to be an example of enhanced cooperation. Some suggested that the concept was about bringing together various stakeholder points of view across traditional boundaries, while others said that it was about achieving development objectives. One speaker noted that the Tunis Agenda indicated that enhanced cooperation was not about creating new institutions. Speakers also suggested that it could be an IGF function to help to reach agreement on the meaning of enhanced cooperation.

44.    Participants heard that the United Nations Department for Economic and Social Affairs had written to relevant organizations asking them to provide annual performance reports, in accordance with the Tunis Agenda. The organizations included the International Telecommunication Union (ITU), the United Nations Educational, Scientific and Cultural Organization (UNESCO), the World Intellectual Property Organization (WIPO), OECD, the Council of Europe, ICANN, the Internet Society (ISOC), the Number Resource Organization (NRO) and the World Wide Web Consortium (W3C).

45.    The information reported by those organizations showed a focus on four main areas:

(a) The meaning of "enhanced cooperation" to most organizations concerned facilitating and contributing to multi-stakeholder dialogue;

(b) The purpose of such cooperation, which ranged from sharing information and experience, building consensus and raising funds to transferring technical knowledge and providing capacity-building;

(c) The thematic focus of the arrangements covered by the reporting organizations, which were very much in line with those being discussed at IGF;

(d) Cooperative arrangements that had already taken place among the organizations, and more of which were being developed with other partners.

46. The various speakers shared their understanding of the meaning of the term "enhanced cooperation". One speaker referred to what he termed "creative ambiguity", which had enabled various stakeholders to discuss a difficult set of issues in ways that were mutually acceptable. Another panellist emphasized the phrase "Governments, on an equal footing" from paragraph 69 of the Tunis Agenda, saying that it supported the view that "enhanced cooperation" meant a process involving Governments. In response, it was suggested that paragraph 71 of the Tunis Agenda referred to the participation of "stakeholders in their respective roles". From that perspective, the paragraph supported the position that WSIS created no new areas of competence for existing organizations.

47. There was equal uncertainty among speakers about in which organizations "enhanced cooperation" should take place. One speaker suggested that it should be understood as an evolving concept.

## III.    Security, openness and privacy

### A.    Overview

48. The agenda for the current meeting includes the following topics:

- Managing the network;
- The future of privacy;
- Sexual rights, openness and regulatory systems;
- Freedom of Connection – Freedom of Expression;
- Freedom of Expression or Access to Knowledge: are we taking the necessary steps towards an open and inclusive Internet?";
- Freedom of Expression & Internet Intermediaries: where do we go from here?;
- Protecting the Consumer in an Online world;
- Developing a Policy Understanding on Information Security: Glocal (Global and Local) Perspective;
- Legal aspects of Internet governance: International cooperation on cyber-security;
- Public -Private Cooperation on Internet Safety/Cybercrime.

49. The discussion on the related themes of security, openness and privacy has evolved since the inaugural IGF meeting, in 2006. In the first two years that cluster of issues was dealt with in two main sessions, one on security and one on openness. At the third IGF meeting the subject evolved under the title of "promoting cybersecurity and trust." During the fourth IGF, the focus was on recognizing that security, openness and privacy were interlinked and the key question was to find the right balance among access to knowledge, the freedom of expression, and intellectual property rights.

50. Discussions during previous years have demonstrated that there is a strong relationship between the issues that has led to a formulation that today links security, openness and privacy in particular issues. The issue in 2010 is explored in terms of looking at how the linkages are involved in particular cases.

51. The challenge in that dialogue was seen to be how to convert areas of tension or conflict into areas of convergence so that the issues of security, openness and privacy could be resolved in the proper perspective. Previous debates had shown that those issues were as complex in nature as they were important.

52. Some of the discussion related to the difficulty that many countries and organizations faced in fulfilling the commitments of the Universal Declaration of Human Rights[4] when balancing protected freedoms with the need to protect society against misuses of the Internet such as terrorism or paedophilia. There was a clear sense that, while the rights set forth in the Declaration might be difficult to meet, all countries had the obligation to uphold them.

---

[4]  The Universal Declaration of Human Rights, article 12, states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

53.     The discussions pointed toward an emerging consensus that dealing with cybercrime, cybersecurity, privacy and openness was the joint responsibility of all stakeholders. There was a need for further information about where victims of cybercrimes could go to find a remedy.

54.     While there was some scepticism about whether a decision on solutions could be reached at IGF meetings, there appeared to be a general feeling that the IGF discussion could provider greater understanding. It was pointed out that all stakeholders involved in that area were not yet part of the debate. As the discussion moved forward, there was a need to bring those communities and interested parties into the discussion to enrich the debate and to help to understand the implications for other users of some of the cybersecurity measures being considered. There was a feeling that, whatever the way forward, it had to be achieved through multi-stakeholder cooperation, dialogue and partnership in the spirit of shared responsibilities. In that regard it was said that it was necessary to enable developing countries to participate fully and to share their needs, challenges and concerns. There was some feeling that discussion had matured enough in that area so that a common environment could be created in which all relevant stakeholders could build trust and work together.

## B.     Security

55.     Discussions on security recognized that it was a critical issue that varied from country to country. It was a multi-dimensional issue with multi-stakeholder involvement and cooperation being essential ingredients towards finding a solution. A key factor was that no broad agreement on a single definition of the term "security" existed. Several speakers offered their own definitions; those included national security, security for business and users, network security and network reliability. The need to prevent security breaches and to find solutions quickly after breaches occurred was stressed. Resilient and secure networks were also mentioned as key elements.

56.     The discussions began with a reminder of how much the Internet had grown and how critical it had become for Governments, for commerce, for the economy in general, for civil society and for researchers. It was pointed out that the Internet was originally built for openness rather than security and that, while intrinsically good, also made the Internet vulnerable. It was noted with considerable concern that those engaged in maliciously causing security problems were often one step ahead of the users and maintainers of the Internet. Quite often they were more technically advanced then those engaged in solving the problems, especially in countries with developing economies.

57.     One of the major issues discussed was the protection of children on the Internet. It was said that there was a need for a more nuanced debate on what was meant by terms such as "child", "harm" and "harmful content". The discussion also raised the conflict between freedom of sexual expression over the Internet and the need to protect children. As part of the Vilnius program, more young people are encouraged to participate in the discussions to bring a fuller understanding of the young person's experiences and opinions.

58.     It was noted that most offline crimes had now also moved online. There were also new forms of crime that were specific to the Internet, such as hacking or phishing. In addition, there were attacks on countries' critical infrastructure, such as distributed denial of service attacks. Attacks on sewerage and air traffic control systems were also mentioned in that context. There was general acceptance that crime and criminality in any society was dealt with through law enforcement, but it was also noted that law enforcement was made difficult by the Internet's borderless nature. While in the offline world the perpetrator of a crime could be traced to the locality where the crime was committed, that was not necessarily the case in the online world. Law enforcement was, therefore, confronted with problems of transnational jurisdiction and geographical boundaries. In addition, legislation, in general, was slow to adapt to a fast changing technological environment.

59.     Many speakers emphasized the legal dimension of the security debate. It was widely recognized that a crime was a crime and that the online and offline worlds should not be treated differently. It was mentioned that 95 per cent of the crimes committed online were covered by existing legislation. While some called for additional legislation, there was also a warning against over-regulation. Many speakers pointed out that collaborative, multi-stakeholder efforts on cooperation could be sufficient. It was noted that both hard law and soft law solutions were needed to enhance security. There was a strong call for harmonizing legislation between countries and also for bringing into force new legal instruments that applied to the online world. The Council of Europe Convention on Cybercrime was mentioned as an example of a promising approach that more nations should adopt.

60.     In terms of soft law solutions, the OECD guidelines in fields such as the security of information systems and networks, electronic authentication, cryptography policy, protection of privacy and transborder flows of personal data and cross-border cooperation in the enforcement of laws protecting privacy, were mentioned as possible solutions. It was pointed out that representatives at the OECD ministerial meeting held in Seoul in June 2008 had concluded that there was a correlation between information flows, ICTs,

innovation and economic growth, while recognizing that there were risks associated with the use of those technologies and the need to tackle them in an appropriate fashion.

61. The ITU Global Cyber Security Agenda was presented as a possible solution. ITU based its work on five pillars:

(a) Legal measures;

(b) Technical and procedural measures;

(c) Organizational structures;

(d) Capacity-building;

(e) International cooperation.

62. While the problem was global, there was also a need for action at the local level. For that reason ITU had employed a combined bottom-up and top-down approach.

63. Some of the issues discussed can be summarized as follows:

(a) Need for prevention in addition to remediation. Prevention was defined as proactive measures to make attacks harder;

(b) Need for more resilient architecture;

(c) Need to establish a feedback loop between prevention, analysis of incidents and remediation;

(d) Need to coordinate many actors, for all categories of stakeholder, involved in the prevention, remediation and related issues;

(e) Essential to build trust networks among those actors;

(f) Time required to build such a network.

64. The importance of Computer Security Incident Response Teams (CSIRT) as part of an effective framework against current and future threats was generally recognized. The role of ISPs was seen as crucial. For some the key issue here was ISP liability, which needed to be considered in further detail.

65. The need to consider security when designing and implementing network systems was also mentioned, as was the need to consider security in the context of the operational process as a whole. A culture of cybersecurity was seen as relevant to any solution. The importance of security at the international level was confirmed during the Sixty-Second session of the General Assembly, when its members voted unanimously in favour of a proposal by the Russian Federation on how to achieve security for information at the international level.

66. Many have spoken of the importance of securing the root with DNSSEC as a step in building trust in the Internet. The process of signing the root was initiated in 2010.

67. There was a need for raising awareness and for training people to handle security problems. There was also a need for international collaboration and for the training of law enforcement officials and the judiciary. In many discussions the problems were represented as challenges not only to law enforcement agencies but also to parliamentarians, civil society, intergovernmental organizations, the private sector and the technical community. Several speakers highlighted the need for high levels of cooperation among law enforcement agencies – a process that needed to be enhanced in respect to online criminals. There was a discussion of the various definitions of cybersecurity and the notion that law enforcement might not always be the best option, especially when dealing with cases of access to information. Several speakers observed that in some cases law enforcement officers might be part of the problem rather than the solution.

68. One of the themes that emerged from the discussions was that creating a sustainable environment of trust for all stakeholders was essential in the pursuit of security, the achievement of which required everyone's cooperation. There was a general understanding that there was a need for multi-stakeholder collaboration, cooperation and coordination at all levels, including national, regional and international.

69. It was also recognized that building trust required that security not be used as a reason for abrogating the openness of the Internet and that government had to take care when using the threat of terrorism or the threat paedophilia as an excuse to introduce measures that went against other international norms.

## C. Openness

70. In the sessions on openness there was a generally held view that openness was multifaceted and multidimensional, not so different in that respect from most issues discussed during IGF meetings.

Participants portrayed it as a cross-cutting issue with linkages to other IGF themes, namely, diversity, access and security, with legal, political and economic dimensions.

71.        Apart from the stability of the Internet, data integrity and content reliability, user protection and the fight against cybercrime, it was stated that utmost priority should be accorded to the building of "a people-centred information society". In that regard, the right to privacy and the due process of law should always be taken into account. It was recommended that the possibilities for legal harmonization on cybersecurity should be evaluated in the light of specific national priorities and the distinct realities of developed and developing countries. Governments had a fundamental role in making cyberspace a secure environment for human interaction and should count on the help of civil society and the private sector for that purpose.

72.        Several contributors wrote of the importance of open access to the Internet, freedom of expression and access to knowledge. They said that there was a need to strike a balance between government regulation and private self-regulation to combat harmful content on the Internet while promoting freedom of expression. Contributors also wrote of a need to establish a new balance between copyright protections and practical use of content to foster new and creative endeavours.

73.        Several declarations and documents were mentioned as points of reference with regard to the free flow of information:

      (a) Universal Declaration of Human Rights;

      (b) International Covenant of Civil and Political Rights;

      (c) Tunis Agenda (paragraphs 4 and 42);

      (d) OECD ministerial meeting in Seoul in 2008;

      (e) Resolution 69 on non-discriminatory access and use of Internet resources, by which the ITU World Telecommunication Standardization Assembly invited member States to refrain from taking unilateral or discriminatory actions that could impede the access of other member States to public Internet sites;

      (f) Global Network Initiative, which brought together a number of non-governmental organizations and companies to discuss protecting freedom of expression and privacy for users;

      (g) Declaration of the Rights of the Child;

      (h) Convention on Cybercrime.

74.        Several speakers pointed out that openness involved several questions of balance. There was a balance between the two IPs as referred to by several speakers: the IP for Internet protocol and the IP for intellectual property. It was pointed out that while on the surface there might appear to be a dichotomy, that was not the case. There was also a question of balance between freedom of expression and free flow of information and the freedom to enjoy the fruits of one's labour. Moreover, there was the issue of balance between privacy and freedom of expression.

75.        The various panels and discussions accorded a strong emphasis to the fundamental freedoms, the freedom of expression and the free flow of information, as enumerated in article 19 of the Universal Declaration of Human Rights, the Geneva Declaration of Principles and the Tunis Agenda in the WSIS context. It was said that a human rights perspective should go beyond paying lip service to those universally accepted principles. The observance of human rights was not only for Governments, but also for businesses and other stakeholders. It was said that compliance with human rights obligations was a journey rather than a destination. One speaker was concerned that human rights had slipped down the Internet governance agenda and that issues such as child pornography, credit card fraud or terrorism were treated as priority issues. It was felt that an "either/or" approach should be eschewed and that solutions to those genuine problems should build on human rights. The principles that were accepted by all needed to be translated into practical solutions based on respect for human rights.

76.        It was also pointed out that law was generally a product of society and often reflected commonly held standards. With regard to the protection of intellectual property and copyright it was always possible to make exceptions, as in the case of education. One speaker pointed out that open access to scientific knowledge was an essential element in the development process and therefore very important for developing countries. Movements such as the creative commons were mentioned in that context.

77.        The discussions also covered open standards and free and open source software. It was said that they might lower the barriers of entry and promote innovation and were therefore important for developing countries. It was underlined that there was no contradiction between free and open source software and intellectual property. It was also recalled that, in the WSIS outcome documents, both open source and proprietary software were seen as equally valuable and having merit.

78.     There was a discussion on what kind of regulation was needed. Several speakers emphasized the usefulness of self-regulation and many favoured a mix of hard and soft law instruments.

79.     With regard to the economic dimension, there was discussion of market dominance and virtual monopolies and their relationship to openness and freedom of expression. It was pointed out that the IGF discussion had a relationship with discussions held in WIPO, in particular with regard to its Development Agenda, and UNESCO with regard to the Convention on the Protection and Promotion of the Diversity of Cultural Expressions.

80.     Participants mentioned that legislation needed to be adapted to cyberspace. It was said that legislation was not something taking place outside society but something that needed to reflect the wishes of society and be adapted to what society wanted. Freedom of expression was described as a fundamental human right that should be ensured and that required the free flow of information and content from diversified sources. More than any other means of communication, the Internet was described as capable of embracing the cultural diversity and pluralism that characterized democracy. The conversion of that potential into reality required the preservation of the open architecture features of the Internet.

## D.     Privacy

81.     It was noted that interest in the right of privacy increased in the 1960s and 1970s with the advent of information technology. The surveillance potential of powerful computer systems prompted demands for specific rules governing the collection and handling of personal information. Two crucial international data protection instruments, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, set out specific rules covering the collection, storage and dissemination of electronic data.

82.     The discussions indicated that user protection should be accorded high priority in building a people-centred information society. In that regard, it was argued that the right to privacy and the due process of law should always be taken into account. The connection was made between security issues and human rights and privacy. It was said that developing privacy laws was actually a contribution to enhancing security. It was pointed out that this was especially the case with regard to identity theft, which was greatest in nations that had the weakest privacy protection. The role of anonymity on the Internet was discussed, especially in relation to privacy in spheres such as medical information.

83.     Increased awareness of the importance of data protection was mentioned in relation not only to the protection of the private sphere of individuals, but also their very freedom. Internal and international security requirements and market interests could lead to the erosion of fundamental safeguards of privacy and freedom. It was discussed how data that were collected for one specific purpose were often made available for others to bodies, both public and private, that were not the intended recipients.

84.     Developing countries and regions would be affected by privacy regulation. There, external constraints such as the European Union data protection regime or trade agreements, in addition to the lack of capacity among developing countries' lawmakers, might have an impact that should be reviewed. In addition, people in developing countries tended to use technology in other ways (e.g., connecting in cybercafés much more than through their own computers) therefore their needs for privacy protection were considered different. Global technical and legal standards should include the perspectives of developing countries.

85.     Participants in various discussions and workshops pointed out that the basis for the protection of individual privacy was the Universal Declaration of Human Rights,[5] in particular its article 12. Nearly every State included a right of privacy in its constitution, either directly or in relation to another right. At a minimum, those provisions included the inviolability of the home and the secrecy of communication. It was also noted that most recent constitutions included specific rights to access and control of personal information.

86.     During the Sharm El sheikh meeting there were many discussion on the privacy aspects of the Social networking. While this was discussed in the context of emerging issues, the problems that come from the sharing of information within social networks was mentioned frequently. No solution other than informing users of the issues was presented in these discussions.

---

[5]   http://www.un.org/Overview/rights.html

# IV.    Access and diversity

## A.    Overview

87.    While the issues are covered separately in the sessions, speakers have emphasized that they are two sides of the same coin as they were issues that affected billions of people involved in the internet conversation.

88.    During each of the IGF meetings, the scope of the Access and Diversity topic has broadened and deepened based on advances in the Internet and new issues that came into clearer focus based on the outcome of workshops.

89.    Issues mentioned for the session in Vilnius included:

- Use of Latin and Native American languages on the Internet;
- Protecting women's rights: Internet content from a gender perspective;
- A multilingual Internet in the light of the sovereign rights of language communities;
- Use of ICT by people with migrant background;
- Digital inclusion: reaching the most socially excluded people in society;
- Mobile Internet Application Facilitating Access for Persons with Disabilities.

90.    Issus covered in previous IGF meetings included:

- National and international regulatory issues;
- National and regional backbones;
- Infrastructure;
- Interconnection costs;
- Enabling Internet Exchange Points (IXPs);
- Modes of access and regulatory challenges;
- Safety and redundancy of access, e.g., cable cuts;
- Issues in mobile access;
- Multilingualism and IDNs;
- Access for persons with disabilities.

## B.    Access

91.    Panellists at past meetings highlighted that the issue of access to the Internet remained the single most important issue for many countries, in particular in the developing world. Speakers stressed the Internet's development impact. A theme that emerged during the first IGF meeting was that, while having one billion Internet users was considered a huge success, the focus should shift towards the next billion and the billions after that. The discussion eventually moved on to considering the last billion.

92.    Several panellists questioned who the next billion people to connect to the Internet might be. One asserted that talking about one billion Internet users would have seemed unthinkable 10 years earlier. Providing statistics, another speaker pointed out that, since the first IGF meeting, much progress had been made in terms of broadband, quality of access and those actually connected to the Internet. By the end of December 2009, the number of users on the Internet had increased to nearly one point eight billion – a significant growth since the beginning of the WSIS process, well on the way to the second billion. Questions had been raised, however, concerning the nature of the Internet experience of the new users, with many of them being mobile Internet users who are restricted in their access to the walled gardens provided by their service providers. The issues of what information an Internet user can access has been one that has been explored under various names including network neutrality.

93.    Participants demonstrated that the underlining IGF theme – multi-stakeholder cooperation – was also extremely important with regard to access. There was acknowledgement that Governments had an important role to play, but had to work closely with the private sector, civil society and the Internet community in that regard. Many participants spoke of the need for innovative solutions, including public-private partnerships, and for private companies to work with Governments and civil society to provide access to those living in rural areas.

94.    There was a general understanding that every country had to find its own solution and that no solution fit all circumstances. In that regard, the size of local markets was mentioned as a problem for small countries. One speaker pointed to the African experience, where a large continent had only an extremely small portion of the Internet, noting that each country had endeavoured to go it alone instead of adopting a regional approach.

95.	The importance of regional multi-stakeholder collaboration in terms of creating regional Internet Exchange Points (IXPs) was stressed by many speakers. The experience of the regional IXPs was recognized as a good example of ways in which collaboration could enhance access for users, support local content and reduce costs.

96.	There was a clear convergence of views that Governments had an important role to play in creating a solid regulatory framework and in ensuring that the rule of law was well established and respected. Many speakers stressed the need for open markets, while others emphasized that market forces alone could not solve the issue of accessibility and Governments bore the responsibility of designing and implementing universal access policies.

97.	International connection costs were described as a burden for developing countries. In that respect, it was considered that a fair environment for business competition on a global scale would contribute to an overall improvement in access conditions. Governments should stimulate the establishment and maintenance of such an environment whenever possible and take action to correct market imperfections, if necessary. It was also suggested that international financing arrangements should be developed to support investment in areas in which it was not commercially viable. Regional cooperation and Internet Exchange Points were particularly valuable resources to help to reduce demand on intercontinental backbones, thus reducing access costs.

98.	Many speakers mentioned the particular issue of backbone networks and noted that this remained an important issue. Local initiatives to enhance access depended on the provision of backbone networks, both nationally and internationally.

99.	On the demand side, many contributors had observed that access was much broader than connectivity. The link had to be made between access and development and that the needs of users must be understood. It was generally felt that access could not just be measured in terms of technological parameters. Clearly prices, quality, availability and content were also significant issues.

100.	Many speakers maintained that providing access to the next billion people required new business models and partnerships to support users who were living on two dollars a day or less. As one speaker observed, that probably meant less than two dollars a month to spend on telecommunications and Internet services. The appropriateness and value of access was therefore seen as a key issue in shaping and integrating the use of ICTs into the development process. It was noted that Governments were often the single largest buyer of ICT services, which meant that demand could be used to anchor new access projects in under-served areas.

101.	During the global e-governance and access to information community of practice meeting in Hyderabad, several points were made:

(a) Empowerment was critical and access was critical to empowerment. The Internet was not just about business, but also empowerment, which was dependent on access;

(b) Access depended on a number of factors, some related to connectivity, others to affordability. It was stated that affordability not only meant low-cost devices and that ownership of devices was not equivalent to access. Affordability could also be achieved through new business models where access was effectively paid for by somebody else;

(c) There was a need to consider both the demand and supply sides and position those in a development framework. A demand-pull might be as effective or sometimes more effective than a supply-push, but the two probably needed to work together to achieve development needs.

(d) Connectivity was a means to an end, providing access to information and content.

102.	During the Sharm el Sheikh meetings a strong concern was expressed for ways in which connectivity could be provisioned for rural population. Topics that have been explored include regulatory policy, technological developments and spectrum management. One speaker suggested spectrum should be used more effectively, for example reclaiming unused spectrum space. Also, new technology that used spectrum more effectively should be adopted in the developing world, not just developed markets. A participant proposed developing government policies that would leverage and extend mobile technologies into the Internet sector in Africa and Latin America. This model had proven to work in South Asia.

103.	Overall, there was general agreement through all of the years of the IGF that issues of access remained central to the IGF agenda and that, as the third billion people came online, new challenges and opportunities would emerge. As the IGF discussions progressed, it was pointed out that the opportunity existed to provide ideas and food for thought about affordable access

## C.	Diversity

104.	The discussion on diversity evolved into a very strong plea for diversity in all its facets. There was recognition that the digital divide was also a knowledge divide and that respect for diversity was a global issue.

105.	Speakers identified various dimensions of diversity: linguistic, cultural, media and relating to persons with disabilities. Several speakers remarked that the notion of diversity extended to the need to include all people, including immigrants living in a country with another language and culture and native peoples living in countries with a dominant culture that was not their own.

106.	Discussions also underlined the challenge of making the Internet available to people in all scripts and languages. India provided a good case study of a region in which many languages and scripts were in use and where the Internet would not spread to the whole population until it had become fully multilingual. Another example offered was Africa where it was pointed out that 2000 languages were spoken by one billion people, with 200 of those languages spoken by more than 500,000 people and 15 African languages spoken by more than 10 million people. Yet, it was pointed out, these languages were almost not present in a significant way in the information age.  A number of interventions in Sharm el Sheikh noted that the inability to access information online in a locally understood language could be life-threatening.

107.	To include persons with disabilities, use of universal design and assistive technologies were important. Representatives were reminded that an important aspect of supporting diversity is that consideration should be given to spoken languages that were not written and to sign languages that were not spoken and that, when written, used iconic representations.

108.	One speaker said that culture was at the core of any discussion of identity, enabled social cohesion, and was critical to the development of any knowledge economy. An example was given of the loss of freedom of African children when they were forced to learn in a foreign language that ignored their culture when they first entered school.

109.	During the discussion, a parallel was drawn between linguistic diversity and biodiversity; linguistic diversity was as important for human freedom as biodiversity was for nature. It was recommended that the precautionary principle, i.e., that actions involving possible irreparable harm should not be taken, should also be adapted to Internet governance.

110.	The impact of standards and the importance of open, non-proprietary standards were mentioned, together with the use of free and open source software as important elements. Adhering to standards was described as another way to promote diversity, especially with regard to accessibility standards.

111.	When IGF discussions on diversity first began, the primary topic was the Internationalized Domain Name system (IDN). Over the years, the topic has evolved and speakers have pointed out that there has been less need to discuss issues related to IDNs, especially now that the first IDNs are in the root. Some speakers stressed the need to distinguish between content in various languages and the role of the IDN system. It was apparent that the debate had moved on, though IDN, and especially the widespread deployment of IDN, remained an important aspect of diversity.

112.	It was also mentioned that the Internet, if available in a local language, could help to change society. Bringing together the network culture with local culture through a narrowing of the knowledge gap facilitated that change. Some speakers saw a need to find economically sustainable ways to balance protecting property while allowing the free spread of knowledge to the diverse populations who needed it to flourish.

113.	There was some discussion of the urgency of the need to provide for content in diverse languages and formats. Not only was that described as necessary for the world's people, but as necessary to prevent the loss of the world's languages and the cultures they represented.

114.	There was a general feeling that the Internet provided an opportunity to protect cultural diversity. For that to be possible it was said that it should be managed for the benefit of the whole of humanity, so that all people could use their own languages with their own values and cultural identities. To that end, the Internet needed to expand to reflect in its content and naming systems the cultural and linguistic diversity and regional and local differences that characterized civilization.

115.	As one speaker put it, there was not only a need to get the next billions online, there was also a need to get them online with economically, culturally and socially relevant content in their own language, to truly reflect the diversity of the human race.

116.	Full and active participation of all, in particular persons with disabilities, was mentioned as the yardstick to measure whether diversity had been achieved.

117.	In the Sharm el Sheikh meeting the accessibility aspect was brought into the mainstream of the discussion of diversity.   Speakers covered issues of how much of the information on the Internet does not

become accessible to many people until specific efforts are made. Demonstrations were also done to show that making information accessible does not interfere with aesthetic considerations or general functionality. Speakers indicated that this was an important consideration since one tenth of the world's population was impacted by disability.

118.     Speakers have discussed that the UN Convention for People with Disabilities included stipulations that provided rights of accessibility on the Internet. If the principles of the convention were properly followed, the needs of people with disabilities would be largely addressed. One such principle was that of Universal Design, which called for the design of products, environments, programmes and services in a way that addressed the needs of people with disabilities and included assistive devices where needed. It was pointed out, however, by one comment that the Millennium Development Goals (MDGs) had not included disability as a priority. This was not seen, however, as lessening the requirement for accessibility.

119.     It was frequently mentioned that the Internet offers unprecedented opportunities for the expression of cultural content from all corners of the world and for the creation, dissemination, recombination and diffusion of content. The conversion of that potential into reality was seen as requiring that the Internet be managed for the benefit of mankind as a whole. Every individual should be able to take part in the Internet in his or her own language and in forms that are in harmony with his or her values and cultural identity. Speakers mentioned that the Internet should expand in a way that reflects, in its content and addressing system, existing cultural and linguistic diversity, including regional and local differences, which characterizes civilization. The particular needs of people with disabilities should be addressed through the creation and dissemination of specific peripherals at affordable prices in addition to the adoption of accessibility standards by the industry.

## V.     Internet governance for Development

120.     Issues for this session include:

- Internet Governance and the wider world: building relationships between the Internet governance and other domains;
- Transnational (or trans-border) enforcement of a new information order – Issues of rights and democracy;
- Social networking and e-participation; what do young citizens look for (18+)?;
- International Trade and Internet Governance;
- Internet governance in Africa: Impact on Africa;
- A Development agenda approach to Internet Names and Numbers;
- Internet governance viewed through different lenses, with emphasis upon the lens of economic and social development.

121.     This session is the outgrowth of several year's workshops on this theme.  These workshops brought out the notion that development should be more central to the IGF and that being listed as a cross-cutting theme was not allowing sufficient focus.  Even though development was an overarching objective and concern throughout the WSIS process and a goal for the IGF, many commented that the relationship of Internet governance to development had not been adequately explored by the IGF.

122.     One concern expressed with establishing a theme on Internet Governance for Development was that it would be difficult to separate ICT for Development issues from those that were properly speaking Internet governance issues.  The relevant issues were those that centre on the linkages between global Internet governance mechanisms and development specifically focusing on the institutional arrangements, the resulting policy procedures and policy outputs generated at the global level, and on how those relate to development concerns.

123.     One goal of the session is to mainstream development considerations into discussions about global Internet governance as one of the set of parameters. It is reported that in most Internet governance venues outside of the IGF, the topic of development is rarely covered and the question of the relevance of policies to development is rarely asked.  There was also mention that the perspective of development may be an aid in understanding issues such as Internet infrastructure, critical Internet resources and use of the Internet for commerce, communications and information.

124.     The session to be held in Vilnius will explore the possible effects of global Internet governance arrangements on the development of the Internet and people-centred information societies in developing countries.  The discussion will consider the institutional processes and substantive policy outputs of governance arrangements and whether these may raise developmental concerns that have not received sufficient attention to date. The session will divided into four parts:

- What do we really mean by Internet Governance for Development (IG4D);

- Examples of specific global governance issues that may have particular relevance to development. Possible topics include, among others, the governance of names and numbers, technical standardization, security, international interconnection, intellectual property, and transnational consumer protection, as well as the procedural or institutional aspects of key governance arrangements;

- How developing and other countries organize and manage their national-level engagement with global Internet governance in the context of their wider national ICT strategies; and

- How to take an IG4D agenda forward in the IGF and other international settings.

125.    One focus of the Internet Governance for Development themes is to make sure that all stakeholders in all regions have a voice in governance topics, especially those that deal with Internet development in the regions.  It was pointed out that in discussing developing country actors, including the private sector, civil society, and the technical community from developing countries, the purpose was to advance development in a people-centred way that engages all of those actors.

## VI.    Taking stock of Internet governance and the way forward

126.    This session will take stock of the evolution of the Internet governance landscape since the first IGF meeting in Athens in 2006. It will serve as a checkpoint on the changes, if any, in the practice of Internet governance over the first five years. It will also serve as a baseline from which to measure the changes over the next five years leading up to the ten year review of the implementation of and the follow-up to the outcome of the World Summit on the Information Society in 2015. In preparation for this session, a request for contributions on this theme was issued on the IGF Web site.

127.    The contributions were asked to focus on the status of the Internet governance in the Internet of 2010 and how it has changed since the IGF was created. In particular, the following questions were explored:

- Are the main themes of 2005 still relevant today?

- Are there new themes that are being overlooked in Internet governance discussions?

- From Athens to Vilnius. Has the context of the discussions changed, and, if so, how?

- Has Internet governance globally advanced over the five years of the IGF?

- Capacity building: where were we five years ago and where are we now?

128.    Three responses were received to these questions, from ISOC Ecuador, ICANN and the ICC.

129.    The ICC wrote that the topics were still relevant but that the interconnections between issues had evolved.  ICANN indicated that while the themes had remained relevant, as a whole the depth of discussion had varied over the years based on participant interests and concerns. ISOC Ecuador wrote that the themes required a permanent and continued discussion.

130.    The yearly session on emerging issues was mentioned as having given an opportunity for new issues to come into the IGF discussion.  Issues such as social networking, online child safety and cloud computing were examples of subjects that were treated as emerging issues. Additionally it was pointed out that each year, new themes were added to the schedule, and that within the core themes, new sub-themes were frequently added.

131.     It was pointed out that the discussions have deepened over the years of the IGF as the trust of the participants in each other has deepened and the familiarity with the IGF modalities has increased.  In some cases, such as security, openness and privacy there was a realization over the years that the subject could not be treated separately, but had to be seen as interrelated.  It was also commented, however, that the same participants are still coming and that the level of compromise has not changed with a marked perception by some in the developing countries that only big organizations, big companies and big countries had the tools to make effective decisions and proposals.

132.    It was pointed out that the views represented in workshops have become more balanced over the years. The sharing of good practice examples was also mentioned as one of the strong developments in the IGF. The IGF is seen as instrumental in building bridges across organizations and groups enabling them to share views and experiences.

133.    ICANN points out that the IGF has inspired people to return to their homes after the meetings and "work on enhancing policy and technical frameworks pertaining to the Internet."

134.     The ICC saw the emergence of the national and regional IGF initiatives as a "testament to the increased human and institutional capacity building and the involvement of all relevant stakeholders in Internet governance discussions at all levels."

135.     It was pointed out that since WSIS, there have been many initiatives in capacity building. This has been enhanced by the increased remote participation capabilities in the IGF and IGF related meetings. It was also pointed that this dynamic field will always require more work on capacity building.

## VII.     Emerging issues: cloud computing

136.     Cloud computing has been designated as the emerging issue for Vilnius. This session will bring together an overview of the issue from both the policy and the technical perspectives of the area and will provide an initial exploration of the possible Internet governance considerations within cloud computing:

- Concept: what is "cloud", how can it be used and why should users use the cloud?;
- Infrastructure, hardware, and environment;
- Privacy, integrity, confidence in the cloud, public policy, regulation.

137.     Specific issues to be discussed in the session include:

- Implications of Cloud Computing;
- The Role of Internet Intermediaries in Advancing Public Policy Objectives;
- How green is the Internet cloud? Policies to unleash the potential of cloud computing in tackling climate change;
- Engendering confidence in the cloud - answering the questions of security and privacy;
- Data in the Cloud: Where do Open Standards Fit In?

138.     A definition of cloud computing was offered by NIST as "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

139.     Some see cloud computing, with its new found efficiencies, as an example of the good the Internet can do: providing the opportunity for users to pay only for the computing resources they use rather than maintaining all their computing needs and resources themselves. This was said to allow innovators to have increased access to the market at a reduced startup cost, thus increasing competition in the market because in the cloud computing model, consumers only pay for the resources they use and avoid capital expenditures which can be difficult to finance.

140.     However some have argued that cloud computing is a return to old centralized models of network usage. It is said to be an hybrid of technologies old and new, with new advances making old techniques more efficient and practical.

141.     One of the areas where there has been must debate is on the privacy and security of information stored in the cloud.  Bruce Schneier, Chief Technology Officer of British Telecom points out that cloud computing means that people's private information is on other people's disk drives.  Privacy protection thus depended on the jurisdiction in which these disk drives were located. This has been a concern for national regulators. The US Federal Trade Commissioner and the Ontario Privacy Commissioner discussed the issue in 2008-2009.  The Council of Europe raised the concern of jurisdiction and international law enforcement and the OECD has organized workshops of the subject.

142.     The regulatory framework for cloud computing has remained a topic of discussion.  Security is often expressed in terms of trust. In the cloud-computing model, it is hard to know who is being trusted and under which regulations they are operating. Some have suggested the need for effective law enforcement mechanisms to deal with issues of security and privacy for data stored in the cloud.  The discussion of the responsibility of various actors involved in cloud computing is still a very open topic.

143.     One of the concerns of experts in the field is the unawareness of most users to the conditions under which their data is stored and accessed.  Often users do not even know that their data is no longer in their country.  Not only is data often used for marketing purposes, personal data is available for other uses and can sometimes be legally sold.

144.     A common question is if data posted on cloud computing platforms is secure. The risks potentially continue to increase with transnational cloud computing. Some companies do not know which law enforcement rules apply to their data.

145.     People also wonder if the data will be secure and what law enforcements have access to the information. Questions asked include:

- If someone is in the one country, but their data is in another country, does that make their data more or less available to third parties?

- Will the laws of other countries decrease the freedoms and rights the users may currently have when they put their data on cloud computing platforms.

# Annex

## Glossary of Internet governance terms

| | |
|---|---|
| **AfriNIC** | Regional Registry for Internet Number Resources for Africa (Member of NRO) |
| **ASCII** | American Standard Code for Information Interchange; seven-bit encoding of the Roman alphabet |
| **ccTLD** | Country code top-level domain, such as .gr (Greece), .br (Brazil) or .in (India) |
| **CoE** | Council of Europe |
| **CSIRTs** | Computer Security Incident Response Teams |
| **DNS** | Domain name system: translates domain names into IP addresses |
| **DRM** | Digital Rights Management |
| **DOI** | Digital Object Identifier |
| **F/OSS** | Free and Open Source Software |
| **GAC** | Governmental Advisory Committee (to ICANN) |
| **gTLD** | Generic top-level domain, such as .com, .int, .net, .org, .info |
| **IANA** | Internet Assigned Numbers Authority |
| **ICANN** | Internet Corporation for Assigned Names and Numbers |
| **ICT** | Information and communication technology |
| **IDN** | Internationalized domain names: Web addresses using a non-ASCII character set |
| **IETF** | Internet Engineering Task Force |
| **IGF** | Internet Governance Forum |
| **IGOs** | Intergovernmental organizations |
| **IP** | Internet Protocol |
| **IP Address** | Internet Protocol address: a unique identifier corresponding to each computer or device on an IP network. Currently there are two types of IP addresses in active use. IP version 4 (IPv4) and IP version 6 (IPv6). IPv4 (which uses 32 bit numbers) has been used since 1983 and is still the most commonly used version. Deployment of the IPv6 protocol began in 1999. IPv6 addresses are 128-bit numbers. |
| **IPRs** | Intellectual property rights |
| **IPv4** | Version 4 of the Internet Protocol |
| **IPv6** | Version 6 of the Internet Protocol |
| **ISP** | Internet Service Provider |
| **ITU** | International Telecommunication Union |
| **IXPs** | Internet exchange points |
| **LACNIC** | Latin American and Caribbean Internet Addresses Registry (Member of NRO) |
| **MAG** | Multi-stakeholder Advisory Group |
| **MDGs** | Millennium Development Goals |
| **MoU** | Memorandum of Understanding |
| **NAPs** | Network access points |
| **NGN** | Next generation network |
| **NRO** | Number Resource Organization, grouping all RIRs – see below |
| **OECD** | Organisation for Economic Cooperation and Development |
| **Registrar** | A body approved ("accredited") by a registry to sell/register domain names on its behalf |

| | |
|---|---|
| **Registry** | A registry is a company or organization that maintains a centralized registry database for the TLDs or for IP address blocks (e.g. the RIRs — see below). Some registries operate without registrars at all and some operate with registrars but also allow direct registrations via the registry. |
| **RIRs** | Regional Internet registries. Not-for-profit organizations responsible for distributing IP addresses on a regional level to Internet service providers and local registries. |
| **Root servers** | Servers that contain pointers to the authoritative name servers for all TLDs. In addition to the "original" 13 root servers carrying the IANA managed root zone file, there are now large number of Anycast servers that provide identical information and which have been deployed worldwide by some of the original 12 operators. |
| **Root zone file** | Master file containing pointers to name servers for all TLDs |
| **TLD** | Top-level domain (see also ccTLD and gTLD) |
| **UNESCO** | United Nations Educational, Scientific and Cultural Organization |
| **WGIG** | Working Group on Internet Governance |
| **WHOIS** | WHOIS is a transaction oriented query/response protocol that is widely used to provide information services to Internet users. While originally used by most (but not all) TLD Registry operators to provide "white pages" services and information about registered domain names, current deployments cover a much broader range of information services, including RIR WHOIS look-ups for IP address allocation information. |
| **WSIS** | World Summit on the Information Society |

———————————————