The Internet Governance Forum (IGF)

Inaugural Meeting

Athens, 30 October – 2 November 2006

Background Report

Prepared by the IGF Secretariat

Contents

I. Introduction

1. The second phase of the World Summit on the Information Society (WSIS) held in Tunis, 16 – 17 November 2005, requested the Secretary-General of the United Nations to convene "a new forum for a multi-stakeholder dialogue" – the Internet Governance Forum (IGF). The IGF was given the mandate to discuss the main public policy issues related to Internet governance in order to foster the Internet's sustainability, robustness, security, stability and development. The mandate of the IGF is set out in Paragraph 72 of the *Tunis Agenda for the Information Society*[1]. A Secretariat was established in Geneva to support the IGF.

2. The preparatory process for the inaugural meeting of the IGF was conducted in an open, inclusive and transparent manner. Two rounds of public consultations, open to all stakeholders, were held in Geneva on 16-17 February and 19 May 2006 From these consultations emerged a common understanding of how the IGF should operate and what issues it should address. The consultations allowed all stakeholders, including individual participants with proven expertise and competence, to take part on an equal footing.

3. At the outset, there was a clear convergence of views that the IGF should have development and capacity building as its overarching objective. It was also established that, consistent with its mandate, the IGF should aim to provide a knowledge facility regarding issues related to Internet governance. A common understanding emerged that the IGF should meet once a year for a duration of two to five days.

4. The preparatory process for the convening of the Internet Governance Forum (IGF) started a broad-based discussion on the substantive agenda. At the first round of consultations, participants were invited to list the top three policy issues they would like the first meeting of the IGF to address. After the consultations, a short synthesis of the public policy issues discussed during the meeting and also reflecting responses to a questionnaire was released by the IGF Secretariat.

5. This synthesis included:

- A recognition of an emerging consensus that the activities of the IGF should have an overall development orientation.
- A recognition of an emerging consensus that capacity building to enable meaningful participation in global Internet policy development should be an overarching priority.
- A recognition that meaningful participation included both assistance to attend meetings and training in the subject matter of Internet governance.

6. Following the February consultations, a call for comment was issued. A total of 43 contributions were submitted by governments, private sector, civil society, the academic and technical communities as well as intergovernmental organizations. The contributions addressed a wide variety of public policy issues. Many of them included not only a description of a public policy issue, but also included an expanded discussion on the importance of the issue, the actors involved in the issue and an explanation of reasons why the issue should be included in the agenda of the first IGF meeting.

[1] *The Tunis Agenda for the Information Society*, available at:http://www.itu.int/wsis

7. The emerging consensus, originally reported after the February consultations, that the IGF needed to maintain an overall development orientation was reinforced by many of the contributions. Capacity building was the most frequently addressed issue. It was presented not only in terms of the growing consensus for its priority in enabling meaningful participation but also as a specific policy issue. When looking at capacity building it was pointed out that access to education, culture and knowledge was a recognized human right. Other authors pointed out the necessity of fostering the ability of all stakeholders from all countries to participate in the process of Internet governance. The discussion of capacity building also extended to consideration of technical standards and the need that they be developed in such a way as to not hinder capacity building. It was suggested that explicit action should be taken to explore the offering of relevant Internet Governance educational resources online.

8. Additionally, a cumulative listing of priority issues since the beginning of the preparatory process confirmed the general importance stakeholders attached to issues and themes such as spam, cybercrime, privacy and data protection, multilingualism as well as issues related to the access to the Internet, such as international interconnection costs and the affordability and availability of the Internet.

9. Different views were held with regard to the structuring of the agenda of the inaugural meeting of the IGF: one approach favoured a focus on a small number of issues to be dealt with in depth, while another approach favoured a broad discussion on any issue that was considered to be important.

10. The preparatory process also addressed organizational aspects, in particular how the preparatory process should be managed. In light of the opinions expressed, the Secretary-General on 17 May 2006 established an Advisory Group to assist him in convening the IGF. The group includes 46 members from government, the private sector and civil society, including the academic and technical communities, who represent all regions of the world. Its chair is Nitin Desai, the Secretary-General's Special Adviser for Internet Governance.

11. The Advisory Group met on 22-23 May and 7-8 September in Geneva and proposed the programme and substantive agenda for the Athens meeting as set out in the paragraphs below.

12. **'**Internet Governance for Development' was chosen as the overall theme of the meeting, with capacity building as a cross cutting priority. The following four broad themes were proposed as the main topics for discussion:

- Openness - Freedom of expression, free flow of information, ideas and knowledge;
- Security - Creating trust and confidence through collaboration, particularly by protecting users from spam, phishing and viruses while protecting privacy;
- Diversity – Promoting multilingualism, including IDN, and local content;
- Access - Internet connectivity: Policy and cost, dealing with the availability and affordability of the Internet including issues such as interconnection costs, interoperability and open standards.

13. General sessions on the first and the last day were set aside to allow participants to address horizontal themes as well as institutional aspects of the IGF and look at emerging issues and discuss future priorities.

14. Following the meeting of the Advisory Group, a call for contributions was issued on the IGF Secretariat Web site and 2 August was set as a deadline for submitting contributions. There were 79 submissions from 45 different contributors within that deadline. This paper is organized in terms of the four broad key themes of the Athens meeting and concludes with a review of the submission on institutional issues. It summarizes the submissions along with a synthesis of the main arguments made in the formal consultations process. This background paper does not necessarily cover every argument in every submission; all the submissions can be found, in full, on the IGF Secretariat Web site: http://www.intgovforum.org//contributions.htm.

II. General aspects

15. Issues surrounding the nature of Internet governance were raised by many of the contributions to the IGF consultation process. These contributions focused on several themes, in particular the general organizational setting of existing Internet governance mechanisms, the processes they invoke as well as the management and tasks of Internet governance organizations.

16. Many of the contributions discussed the ways in which Internet governance mechanisms can only be understood in a broader set of issues and international and national policy frameworks. Thus, for example, the Council of Europe pointed out that Internet Governance, for its members, incorporated the principles and frameworks which are designed to ensure development of the Internet and the Information Society. Thus Internet governance issues embrace The European Convention on Human Rights and other Council of Europe instruments, like the Cybercrime Convention, which provides a framework on the European level for examining State responsibilities and guiding State policies.

17. The role of the IGF was debated in several of the submissions. Some[2] emphasized that the IGF mandate was clearly set out in the WSIS Principles and Tunis Agenda. The Russian Federation in its contribution would like the IGF to address the principles and future mechanisms of international Internet governance and discuss issues relating to the administrative management of the Domain Name system (DNS) and IP addresses.

18. There was broad consensus on the importance of the development agenda as a focal devise for the IGF, in particular issues such as capacity building, and increasing the level of democracy and transparency of Internet Governance[3]. The South Centre identified two broad types of capacity building: the first type related to improving the institutional knowledge and understanding of Internet governance issues for governments and their representatives with the aim of enabling developing countries to advocate their needs more effectively with other governments and the private sector; the second related to improving the ability of citizens to fully utilize the benefits of the Internet.

19. There was some concern expressed in the consultations about the balance of interests in a multi-stakeholder environment. Some argued that the IGF could be in danger of being captured by dominant political and business interests[4]. As a result the IGF should focus on the development issues surrounding the Internet as a public infrastructure with a strong public goods perspective.

[2] e.g. the Internet Governance Project (IGP) and the South Centre
[3] The South Centre
[4] IT for Change

20. The Council of Europe noted that the IGF could help explore and map out unanswered questions regarding the interpretation of rights in online situations. Important issues that needed to be addressed were privacy of correspondence or communications over the Internet and in particular how the State should deal with third party interference, the right for freedom of expression and information and the role of third party actors, such as Internet service providers and their notice and take down actions. The Council of Europe also noted that it was important to explore security and stability through the human rights prism. Others[5] emphasized that up to this point existing Internet governance arrangements had been successful in keeping the technological core infrastructure from political and commercial manipulation and expressed their hope that this should continue in the era of multi-stakeholder Internet governance.

III. The four broad themes of the inaugural IGF meeting

A. Openness

21. Throughout the preparatory process, many speakers and contributors highlighted the importance of openness as one of the key founding principles and characteristics of the Internet. The open nature of the Internet was seen as part of its uniqueness, and its importance as a tool to advance human development. The Internet provides for a robust and unencumbered exchange of information, and welcomes millions of individuals as users from all corners of the world. Internet users trade ideas and information and build on both, thus increasing the wealth of knowledge for everyone, today and in the future. The openness of the Internet was also seen as a key feature to ensure its stability and security.

22. Many submissions pointed out that the Internet made it possible for more people than ever before to communicate and therefore to express themselves (i.e. to hold, receive and impart information and ideas regardless of frontiers) as clearly and as quickly at such a low cost. Access to knowledge and empowering people with information and knowledge that is available on the Internet was described as a critical objective of an inclusive Information Society and to continued economic and social development.

23. There was a wide spread acceptance across the contributions that because the Internet was designed for efficiency and not control, it has enabled millions of people all over the world to educate themselves, express their views, and participate in democracy to an extent never before possible. Moreover, there was also wide spread recognition of the fact that the distributed nature of the Internet whereby control is placed at the ends, or in the hands of users, rather than at a centralized point, is a key architectural feature of the Internet that has ensured that freedom of expression and the free flow of information. Hence there was a consensus around the importance of openness in fostering processes of development.

24. There was a general understanding that one of the most important set of rules governing online behaviour is the body of law dealing with intellectual property rights (IPR) in cyberspace. Because of the unique digital nature of the Internet – copies of data are necessarily made to engage in just about any online activity – almost all uses of the Internet automatically trigger intellectual property rules. However, there was no common understanding on how these rules should be shaped to protect the openness of the Internet and the free flow of information.

[5] The Oxford Internet Institute (OII)

25. For some[6], the real concern was that the direction of current policy development with regard to IPR and technological innovation, such as with regard to digital rights management (DRM) and technology protection measures (TPM) were capable of undermining the free flow of information and the openness of the Internet. However, others held the view that these rights were essential for protecting the rights of creators and stimulating innovation.

26. The need to maintain an open Internet was also seen as a prerequisite to sustainable development. Several contributions[7] focused on the role of free flow of information as a mechanism for sustaining development and inhibiting the 'brain drain' from poorer to richer countries. Critical to these types of arguments is the view that openness of the Internet is about looking at ways to ensure a fairer distribution of scientific knowledge between countries. Such flows of information are axiomatic to the innovation process and support the development of small and large businesses in developing countries. Specific proposals include metadata standardisation, a freely available Digital Object Identifier (DOI) system, peer-to-peer networks as a possible solution to publish scientific information, the creation of a World Language Diversity Network and semantic Web gTLDs.

27. The importance of open and online education resources was highlighted by a number of contributors. The challenges here are not only in defining and fostering open educational resources online but also ensuring that such resources are developed in line with the WSIS principles and the Millennium Development Goals (MDGs)[8]. These arguments were reinforced by others who highlighted guiding principles for the free flow of information, namely: public access to works created by and funded by public authorities; to ensure the smooth migration of content into new formats for purposes of preservation; lending and copying those materials that still have a copyright but are not under commercial use; measures to encourage individual research and study by allowing copying of protected material/content by individuals for personal use (research and study) and measures to harmonize copyright legislation.

28. The rights of minority groups and indigenous peoples with regard to both access to information and the protection of their cultural heritage were raised by some contributors. Amongst the points made were that the free flow of information and access to knowledge ensured the development of the Internet and freedom of expression as well as being a vital human right, also contributing to a growing public domain. One group argued that unauthorized use of indigenous people's cultural heritage, like the use of indigenous names and terms as Internet domain names, could cause economic and social harm to those people[9].

B. Security

29. Many contributors and speakers throughout the preparatory process emphasized that Internet security was a key element of building confidence and trust among users of ICTs. They argued that the Internet had the potential to enable users to access and generate a wealth of information and opportunity. Achieving the Internet's full potential to support commercial and social relationships required an environment that promotes and ensures users' trust and confidence and provides a stable and secure platform for commerce.

30. It was pointed out that although each new device and interconnected network increases the capacity for users and their communities to make beneficial economic and social advances,

[6] IP Justice, Electronic Frontier Foundation, Janet Hawtin-Reid
[7] WSIS Civil Society, Special Libraries Association's (SLA)
[8] WSIS Education, Academia and Research Taskforce submitted a paper on Open Educational Resources
[9] The Indigenous Peoples ICT Taskforce

they also increased the exposure of individuals and organizations to potential harm from unintentional, intentional and also illegal behaviour. Security and privacy breaches such as phishing, viruses and spam undermine users' confidence and trust. Concern for network and information security therefore detract from the Internet as a medium delivering economic and social development. These threats also create enormous cost burdens for users around the world, reducing the continued growth and utilization of the beneficial aspects of the Information Society.

31. There was a general understanding that solving these problems depended on a heightened awareness and understanding among all stakeholders of the importance of a secure Internet infrastructure. It would involve a combination of initiatives (national, international, private sector, and technological) and doing so required enhancing the users' abilities to control their data and personal information. One major concern was to find the appropriate balance between security and ease of use and openness. There was also need for a balance between measures to fight crime and protecting privacy and freedom of expression. Ultimately, the responsibility for ensuring Internet security rested with all stakeholders and required cooperation among them.

32. Several contributions focused on the issues of security[10]. Many of these papers presented well-established work that had been done in other contexts, but was relevant to the work of the IGF.

33. A recurrent theme of the papers submitted was the need to adopt international best practices and to ensure greater international cooperation in a multi-stakeholder environment. Thus, for example there was a widely held view that with respect to preventing cyber-crime the IGF should promote cooperation between different stakeholders and agencies, educate the users of ICTs, taking care to explain security threats in a plain language to the end-users and award individual contributions making the Internet a safer place[11]. The contributions also illustrated the extensive nature of existing work done to increase security and confidence in the Internet and combat harmful and illegal activities. It was widely accepted that the poor levels of security (such as, phishing, spam, malware and leakage of personal information) was a major cause of concern for business and users and could ultimately undermine trust in the Internet.[12]

34. One of the intergovernmental organizations dealing with security issues, the Orgnisation doe Economic Co-operation and Development (OECD), explained in its contributions its mandate to conduct research and analysis and develop policy frameworks to sustain trust in the global networked society, with a primary focus on information security and privacy[13]. The OECD also established a Task Force on Spam[14]. Each of these initiatives produced substantial results, for example the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002) and the Anti-Spam Toolkit – the focal point of the OECD submission to the IGF. *The Toolkit* includes sections on recommended policies and measures addressing regulatory interventions, enforcement and cooperation, industry driven activities, technical solutions, education and awareness initiatives, spam measures and international cooperation and exchange. The OECD Council adopted recommendations on cross-border cooperation in the enforcement of laws against spam (2006).

---

[10] e.g. ITU, OECD, Nippon Keidanren, the Japan Business Federation (JBF), Marc Perkel
[11] e.g. Eurim
[12] e.g. JBF
[13] Current areas of focus by the OECD include security risks such as malicious software ("malware"), national policies for the protection of critical information infrastructures, e-authentication and identity management, privacy law enforcement cooperation, and RFID, sensors and networks (www.oecd.org/sti/security-privacy).
[14] www.oecd-antispam.org

35. A common thread to the contribution papers was that many measures are available to tackle spam. To reduce the amount of spam, the OECD argued that national anti-spam regulation should attempt to preserve the benefits of electronic communications by increasing user trust in the Internet; prohibit and take action against the act of spamming, as defined by national law. To achieve these goals, national legislation should follow some key principles: the legislation should have a clear policy direction; the enforcement of the law should be effective and, as spam was a cross-border issue, the legislation should foresee appropriate international linkages.

36. Similar arguments were voiced by the Secretariat of the International Telecommunication Union (ITU) in their submissions. In particular, the ITU drew attention to the following priorities:

- to address cybersecurity concerns in order to provide secure and accessible e-service;
- to develop a common understanding of the issues of spam and cyberthreats, including countermeasures;
- to promote cooperation and outreach to support the collection and dissemination of cybersecurity related information to minimize prevent and detect cyberthreats;
- to facilitate regional and interregional cooperation and support appropriate capacity building, which could include the development of Memoranda of Understanding among interested member States to enhance cybersecurity.

37. The OECD 'Anti-Spam Toolkit' also stresses the importance of the Internet Service Providers (ISPs) and the need for governments and regulators to support the development of ISP codes of best practice that complement and are consistent with legislation. This view was echoed in the comments of others, for example, the International Chamber of Commerce (ICC)[15]. For some, the extension of what can be seen as self-regulatory measures could be extended into 'quality assurance' measures, such as Internet quality labels.[16]

38. Many contributors argued that issues of cybersecurity were so clearly international that it was important to build mechanisms through which the international community could co-operate against security threats. Underlying this view was the need to focus resources on a widely diffused issue; it was felt by some that the efforts of a single company or country were no longer sufficient to combat increasing security threats[17] [18]. In this regard there were suggestions as to the activities that could be undertaken and supported by the IGF. Hence there was a view that the IGF should start a discussion about non-geographic reporting and policing, enabling to report and monitor crime across the borders; that the IGF should encourage the allocation of more resources in order to identify the scale and nature of current cybercrime[19].

39. Whilst the notion of spam was widely seen as an abuse and misuse of the Internet, there was clearly a need, as argued by some[20], to distinguish between the legitimate business needs and benefits or commercial electronic communications and spam. If spam was seen as harmful, fraudulent, malicious, misleading or illegal communications, generally sent in bulk, then it should

[15] According to ICC the business is keen to allow self-regulation to demonstrate its efficacy – filtering, labelling and self-regulation on the Internet should be carefully considered as alternatives to legislation.
[16] The Swiss Internet User Group proposes the introduction of Internet Quality Labels, which would be based on the work of existing organizations, such as the Web Accessibility Initiative of the World Wide Web Consortium (W3C).
[17] Nippon Keidanren, op cit
[18] Eurim argues that there is disparity between public and private resources; the law enforcement agencies do not have sufficient resources and knowledge to fight the cybercrime while, in contrast, private business have the resources but are unable to implement solutions on a large and general scale. Hence the group suggest the cooperation across law-enforcement boundaries and between private and public sector has to strengthen
[19] Eurim, op cit
[20] e.g. ICC

be possible to differentiate between other forms of mass communication on the Internet. Such a differentiation between these two could help the relevant institutions dealing with this issue to focus on the harmful effects of spam.

40. Interwoven into the debate on security were several other significant issues, such as human rights and the protection of privacy. The Council of Europe argued that although multi-stakeholder cooperation was undoubtedly the most effective way to respond to many of the security and stability related issues, it was necessary to think about abuse and misuse of the Internet in terms of the denial of human rights. Thus, according to Council of Europe, there may be scope for international sanctions against those that host (or fail to combat) cybercriminal or cyberterrorist activities. These sanctions would be similar to international sanctions currently employed with countries in armed conflicts or involved in terrorism.

41. One contribution[21] asked whether the current security measures were about democratically accountable partnerships or self-protection of special interest groups. It argued that the scale of cybercrime was not accurately measured at the moment as phishing of spam were inadequately reported. IPR reform and/or technical re-engineering was suggested as a way forward to improve the security of the Internet.

42. Other key issues on privacy raised in the consultation process included the rights of business to collect and use personal information from and about employees to comply with labour tax and other laws, to administer benefits, to operate their businesses and to serve their customers[22]. The argument was that businesses should not be prevented from making appropriate, focused and reasonable use of pre-employment screening procedures for prospective employees, provided that the employees know that this may happen. It was noted that companies were increasingly legally required to vet employees in the areas of health, childcare, teaching, finance, or privately provided security and law enforcement provisions. As a consequence there was the need for flexibility to facilitate access to information, communications, and commerce on global scale and the ability to accommodate differences in interpreting privacy in the workplace.

43. One of the very specific debates about privacy raised in the consultation process was with respect to the WHOIS database[23]. The core of the argument was that the current policies of ICANN/IANA for the administration of the WHOIS database, requiring both accurate data and public access to those data, was seen to be in direct conflict with broadly accepted principles and regulations for privacy protection in some jurisdictions. As a result it was argued that ICANN, in collaboration with others, should establish the official purpose of the WHOIS database in accordance with its original and specific purpose, *i.e*, that of enabling the reliable resolution of technical problems surrounding domain registration.

44. Some of the contributions sought to look at innovative solutions to issues of security[24]. One such approach centred on the concept of 'trusted computing'; a process designed to increase security as well as prevent computer users from making any un-authorized operations. Whilst 'trusted computing' may neither be good or bad *per se*, it could have large implications on competition, privacy and consumer rights. The proposal suggests starting a public process discussing the concept of 'trusted computing'.

[21] Eurim
[22] ICC
[23] ICANN's Non-Commercial Users Constituency (NCUC)
[24] Vittorio Bertola

C. Diversity

45. While it was generally applauded that by now almost one billion people use the Internet, it was also pointed out that many of these people could not read or write in English, and they used languages that do not use the Latin alphabet. It was generally recognized that everybody should be able to use the Internet in their own language. A multilingual Internet would foster an inclusive, democratic, legitimate, respectful, and locally empowering Information Society.

46. Many contributions emphasized that a key element of promoting multilingualism on the Internet was creating the availability of information in local languages. A number of different organizations submitted papers under this theme and discussed the benefits of a multilingual Internet to the local communities[25].

47. Several submissions stressed the importance of linguistic and cultural diversity as essential elements for the development of the Information Society[26]. However, in their view the lack of access to the Internet in indigenous languages was detrimental to many potential and existing users. These detrimental effects were typically most commonly felt in developing countries. Some contributions argued that governments should design policies to support the creation of cultural, educational and scientific content (in line with the UNESCO Universal Declaration on Cultural Diversity) and, in particular, develop national policies that encourage the use of information stored in archives, museums and libraries to provide content in the Information Society.

48. One submission focused on the use of keywords[27]. The paper suggested that it was essential to look now at the future of keyword systems. The future could hold multiple variations to a single keyword lookup. Thus, keywords could be iconic, oral, non-verbal sounds or translated into other multiple keywords in any other language, which would open interesting avenues for handling multilingual web contents.

49. Many of the papers discussed the management of the DNS and various ways to turn it into a system that allows multilingual use, but each arrived at different recommendations. The issues surrounding Internationalized Domain Names (IDN) were addressed by several of the submissions [28]. It was recognized that as technical solutions to address issues of multilingualism became more localized, questions of global interoperability became more complex and harder to guarantee.

50. One of the key questions raised was about the use of 'aliases' and how such tools could be used for presenting and processing native language TLD names in sub-level DNS names[29]. This approach would provide both a better user experience and reduce the load on the DNS, rather than trying to install multiple names for each domain in the DNS itself. The paper argued that this approach would avoid adding complications to the operation of DNS database. The key argument was that from a user standpoint, the issues around languages were all about what was seen and typed, not what was in the DNS or visual form of the URL. The question of internationalization of the domain name system was not what was happening to the underlying technologies but " what should the user see (or enter) and what was the best way to accomplish that?"

---

[25] Eurolinc
[26] Eurolinc and WSIS Civil Society Working Group on Scientific Information
[27] The Native Language Internet Consortium
[28] i.a. the ITU Secretariat, the ICC and ISOC.
[29] ISOC discussion paper "Internationalising Top Level Domain Names: Another Look"

51. The ITU Secretariat provided an overview of its activities on IDN based on the work of Study Group 17 (Security, languages and telecommunication software). ITU was given the mandate by The World Telecommunication Standardization Assembly to study IDN as it was considered that implementation of IDN would contribute to easier and greater use of the Internet in those countries where the native or official languages are not represented in International Reference Alphabet (IRA) characters.

52. However, some expressed the view that the issue was now not one of establishing multilingualism but one of ensuring consistency across the national registries[30]. There was a need to ensure that the processes for development, maintenance, upgrade and resolution could proceed in a manner that would preserve the stability, integrity and security of the Internet.

D. Access

53. Many contributions, in particular from developing countries, reminded that, despite the rapid spread of the Internet, five billion people remained without access to this important tool for economic growth and social development. They recalled that access could therefore be the single most important issue to most people, in particular in developing countries.

54. Some contributions[31] underlined that there were several factors that conditioned the availability and affordability of the Internet. The appropriate regulatory environment (sometimes referred to as the enabling environment) at the national level could do much to foster the deployment and growth of the Internet. National policies could encourage investment in capacity and growth, support the establishment of Internet exchange points (IXPs), create a favourable legal climate for supporting e-commerce, promote the extension of broadband networks, and encourage competition in the ISP industry that would lower prices.

55. It was pointed out that another element that could influence the availability and affordability of the Internet were international connectivity prices and costs. Interconnection standards and agreements, including peering arrangements, were seen to be critical to the successful functioning of the Internet and for maintaining its end-to-end and cost effective availability and reliability.

56. Submissions dealing with access focused on three key issues. The first was the overriding significance of access to the delivery of an information society and how access was so unevenly distributed across and within countries. The second area was the importance of open standards in maintaining the openness of the Internet, fuelling innovation and supporting the rapid diffusion of new services and technologies. The third area of focus was the cost of access.

57. There was a concern that the topic of access within WSIS as well as other Internet governance discussions had focused on access as an issue of infrastructure rather than issues of quality, content and affordability[32]. The key argument was that infrastructural access was of little use to end users if access to content and services and the level of prices was not included in the concept and discussion of access. It was commented that access and openness of information were linked concepts.

[30] ICC
[31] The Global Internet Policy Initiative (GIPI)
[32] IT for Change

58. Some submissions[33] developed the argument that access was more than infrastructure and pointed to the interplay between the digital divide, access and multilingualism. Often the indigenous languages were not written languages, so for indigenous people to gain access needed unconventional solutions from software and hardware point of use.

59. Those submissions that addressed the question of open standards all focused on the positive outcomes from the longstanding custom with the Internet technical community of openness and strongly argued against any moves to weaken the norm of open standards.

60. Many of the submissions argued that open access processes had driven growth and connectivity in the Internet and that this foundation stone of the Internet should be borne in mind as issues of Internet Governance became major public policy debates. For some the biggest threat to the stability, growth and global reach of the Internet could come from lack of understanding of the way in which the Internet's technologies and resources are developed and coordinated[34]. It was therefore important for policy makers, both in the public and private sectors, to have an understanding of how the Internet developed and what made it so successful.

61. Other submissions focused on the significant positive 'network effects' that were delivered through open standards and how these network effects were fundamental to understanding why the Internet and the World Wide Web were such powerful communication and collaboration tools[35]. Some papers drew attention to the existing balance between IPRs and public goods and the ways this balance was being challenged by a combination of elements including the growth of software patents, the failure of so-called "reasonable and non-discriminatory" licensing, and competitive business strategies and trade relations.

62. Another dimension, discussed by some contributors, was the role of open standards in promoting competition on an equal basis across a wide range of Internet markets. One contribution[36] set out some guidelines for providing effective open standards and interoperability policies and promoting open standards for eGovernment services.

63. Many submissions stressed the need to differentiate between two distinct issues: how to define and uphold open standards on the one hand and the debate over proprietary versus free and open source software (F/OSS) on the other. The proponents of F/OSS[37] argued that the Internet and free and open source software went hand-in-hand. It was F/OSS that made the Internet and the World Wide Web possible and continued to shape and develop it. The contribution regretted that F/OSS and its representatives had been all but excluded from the debate on Internet governance so far, first in the framework of the Working Group on Internet Governance (WGIG) and subsequently in the IGF processes.

64. One submission[38] argued that Internet standards were the mediators between competing economic interests reflecting multi-stakeholder tensions (such as the tension between access to information and IPRs). It also noted that Internet standard bodies shared no common procedural norms, as there were numerous organizations setting standards in the Internet space and also that,

[33] The Indigenous ICT Taskforce
[34] ISOC
[35] Sun Microsystems, Consumer Project on Technology, IP Justice, University of Maastricht and Electronic Frontier Foundation submitted a contribution entitled "A Positive Role for Government in Promoting Open IT Standards, the Network Effect and the Information Society"
[36] Rishab Ghosh, Univeristy of Maastricht
[37] Free Software Foundation Europe (FSFE)
[38] The Information Society Project of Yale Law School submitted a paper on "Best Practices for Internet Standards Governance for the consideration of IGF

procedural and informational openness varied by organization. There were barriers of entry to the standard setting procedures as some of the standards bodies tended to exclude non-members and powerful interests sometimes dominated standards setting processes and procedures. For example, it was argued that some entities had used IPRs to unfairly maximize royalty revenue from adopted standards while others had used standards as part of product marketing strategies, creating barriers to interoperability and restraints on competition.

65. Several of the submission stressed their own role in the debate over open standards and standard making processes. For example, ISOC submitted an article from its news bulletin which emphasized that as the "organizational home" of the Internet standards processes, it had a unique position to help policy makers to understand the implications of Internet technologies and to develop effective and fair Internet coordination policies. Similarly the ITU Secretariat highlighted its long-standing formal role in the international community in the standards making processes.

66. The question of interconnection costs[39] was addressed by several submissions, in particular the way in which the costs of the network and access and the associated revenues were distributed between the different players. In its submission on this subject matter, the ITU Secretariat presented the recommendations of the World Telecommunication Standardization Assembly, recognizing the need for compensation between the providers carrying the traffic. The paper stressed that such arrangements for Internet traffic interconnection should be agreed upon on a commercial basis when direct international Internet links are established. The paper also presented the ITU's work in progress, such as the study on efficiency and cost of Internet connectivity around the world for the period 2005-2008.

67. Others argued that the issues of Internet interconnection and especially international connectivity could be addressed by the liberalization of telecommunication markets which have over recent years successfully supported access growth, service innovation and dramatically lowered the price of Internet access[40]. In the OECD's experience, concerns raised in respect to Internet traffic exchange have been overcome as commercial solutions have been applied but they also note there is pressing need to develop human capital, particularly inter-networking skills, along with infrastructure such as Internet exchange points[41].

IV. Institutional aspects

68. Many submissions focused on institutional aspects related to the IGF or proposed new arrangements with regard to Internet governance. Common to most of these submissions was a focus on the importance of developing and maintaining multi-stakeholder processes at both the national and international levels. Thus, for example, the importance of multi-stakeholder processes was underscored by the contribution of the National Telecommunications Regulatory Authority of Egypt who argued that in emerging markets, such as Egypt, the creation and development of an Information Society was not a task carried out by a single entity, rather it was a national task carried out by multiple agencies, public private partnerships, community initiatives and cooperation between all the stakeholders.

[39] e.g. Baher Esmat and Juan Fernandez
[40] GIPI paper on Internet Exchange Points
[41] OECD paper on IXPs

69. Others[42], noted that multi-stakeholder approaches were relevant, as the Internet itself was a collection of technologies and services. However, it was also observed that the inherent diversity in multi-stakeholder cooperation could result in increased complexity and fragmentation of the governance processes.

70. The role of individuals and groups and 'policy learning' between these groups were also developed in other contributions. Thus for example, there was a widely held view that the IGF could learn from technical bodies already involved in Internet governance, such as the Internet Engineering Task Force (IETF), with regard to collaborative governance and decision-making and deliberative democracy[43]. Similarly other contributors focused on the deep knowledge already held by the global intellectual community and highlighted the role of the IGF in bringing this knowledge into play with respect to Internet governance[44].

71. Several contributions addressed the modalities of managing a multi-stakeholder process. One contribution[45] linked the broad theme of openness as set out in the agenda for the IGF meeting in Athens, to the essence of multi-stakeholder participation and suggested articulating an appropriate process or accountability mechanism to address diverse substantive issues and stakeholder needs in order to ensure the effectiveness of the multi-stakeholder governance model. Managing distinct or even conflicting viewpoints, interests, values, cultural and political understandings was described as "tough challenges". However, the implementation of the WSIS principles (multilateral, transparent and democratic) depended on the establishment of a multi-stakeholder participation system. One proposal[46] called for legal frameworks for multi-stakeholder partnerships (MSP) for governance and suggested setting up a "lightweight agency in the spirit of ongoing UN reforms" that would facilitate an easy formation of MSPs within an international public law framework, by a simple decision of its assembly without the need of lengthy multi-lateral treaty negotiations.

72. Another contribution proposed developing an "Internet Bill of Rights" as an important corollary to the multi-stakeholder process of Internet Governance. Such a bill of rights could build on the WSIS principles and define succinctly the rights and duties from the point of view of the individual[47]. One proposal[48] called for developing a UN Framework Convention as way to deal with Internet governance and ground it in international law. Such a Convention would provide a framework for establishing additional agreements, whenever they were needed. As the policy issues related to Internet governance differed widely in scope, impact and substance, they would require different solutions.

73. The Council of Europe argued that State responsibility could be reduced by promoting new forms of solidarity, partnership and cooperation, in particular multi stakeholder processes and international cooperation. It noted that multi-stakeholder governance would help shape regulatory and non-regulatory models and, in a timely manner, address challenges and problems arising from the rapid development of the information society. The Council of Europe also recognised the need for oversight of such multi-stakeholder processes and argued that it was not practicable for every State to exercise an oversight function, so organizations entrusted with global Internet governance responsibility ought to be subject to oversight by the international

[42] The Oxford Internet Institute (OII) "*Addressing the Issues of Internet Governance for Development: A Framework for Setting and Agenda for Effective Coordination*".
[43] Such as Jeremy Malcolm
[44] David Allen
[45] Kuo-Wei Wu, Member of Executive Council, Asia Pacific Network Information Center (APNIC)
[46] WSIS Cicil Society Working Group on Scientific Information
[47] Vittorio Bertola
[48] IGP

community. Similarly individual nation States were not precluded from oversight, for example, with respect to responsibilities under human rights obligations.

_____

Annex I

List of Submissions

1. National Telecommunication Regulatory Authority in Egypt
2. Proposals of the Russian Federation to the Agenda of the Internet Governance Forum
3. UNESCO 'Information for All' Programme National Committee of Russia
4. International Telecommunication Union (ITU) Secretariat
5. An Overview of ITU work on International Internet Interconnectivity
   - The ITU-T Study Group 17 work plan on countering spam
   - The ITU-T Study Group 17 work plan on Cybersecurity
   - An Overview of ITU-T Internationalized Domain Names activities
   - An Overview of ITU-T Security Initiatives
   - ITU/BDT/HRD - Youth Programme
   - ITU/BDR/HRD - Youth Programme
   - An Overview of ITU-D Mandate and Activities in Cybersecurity
   - An Overview of ITU-D Mandate and Activities related to Access
   - An Overview of ITU-D Mandate and Activities in Measuring Access to telecommunication/ICTs and the Information Society
   - An Overview of ITU-D Mandate and Activities relevant to WSIS
   - An Overview of Some Relevant ITU Activities
6. Council of Europe
7. Orgnisation doe Economic Co-operation and Development (OECD)
   - OECD Anti-Spam Toolkit
   - Internet Traffic Exchange: Market Developments and Measurement of Growth
   - A summary of OECD work relevant to the IGF
8. The South Centre - Internet Governance for Development
9. Government of Quebec
10. International Chamber of Commerce/Business Action to Support the Information Society (BASIS)

- ICC framework for consultation and drafting of Information Compliance obligations
- Issues Paper on Internationalized Domain Names (IDN)
- Employee privacy, data protection and human resources [policy statement focused on European Union context]
- Information security for executives
- Privacy Toolkit
- Securing your business
- Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries
- The impact of Internet content regulation
- ICC policy statement on 'spam' and unsolicited commercial electronic messages
- Revised and updated matrix of issues related to the Internet and organizations dealing with them

11. Nippon Keidanren (Japan Business Federation)

12. Internet Society (ISOC)

    - Internationalising Top Level Domain Names: Another Look
    - Names and Naming for the DNS
    - DNS Root Name Servers
    - DNS Root Name Servers FAQ
    - The Genius of the Internet: Open Processes Drive Growth and Connectivity
    - Capacity Building: Enabling Sustainable Development of the Internet

13. ICANN's Non-Commercial User Constituency (NCUC) - Privacy Implications of WHOIS Database Policy

14. The European Information Society Group - Policing the Internet: Democratically accountable partnerships or self-protection groups?

15. WSIS Civil Society Working Group Scientific Information

16. WSIS Civil Society Human Rights Caucus

17. Free Software Foundation Europe (FSFE)
    - Sovereign Software
    - Free Software Essentials Reference Sheet

18. IT for Change - A Development Agenda in Internet Governance

19. Consumer Project on Technology, Sun Microsystems, IP Justice, Professor Ghosh of the University of Maastricht and the Electronic Frontier Foundation - A Positive Role for Government Procurement in Promoting Open IT Standards, the Network Effect and the Information Society

20. Electronic Frontier Foundation (EFF)
    - The Impact of Technological Protection Measure Regulation on Participation In The Information Society And The Free Flow of Information on The Internet
    - Unintended Consequences: Seven Years under the DMCA

21. Swiss Internet User Group - Internet Quality Labels

22. Native Language Internet Consortium (NLIC)

23. EUROLINC

24. Indigenous ICT Taskforce

25. The Association for Progressive Communications (APC) - Reducing the Cost of International Internet Connectivity

26. Centre Africain D'Echange Culturel (CAFEC), Coordination Nationale Du Reprontic Coordination Sous Regionale Afrique Centrale (ACSIS)

27. Foundation for a Free Information Infrastructure (FFII)

28. Global Internet Policy Initiative
    - Redelegation of Country Code Top Level Domains
    - Internet Exchange Points: Their Importance to Development of the Internet and Strategies for their Deployment – The African Example
    - Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime
29. Native Language Internet Consortium - An Academic's Perspective on Promoting Multilingual Internet in India

30. Spanish Experts Group on Internet Governance and of Telefonica Foundation and Politécnica Madrid

31. Yale Information Society Project - Best Practices for Internet Standards Governance

32. WSIS Academia, Education and Research Task force - Open Educational Resources (OER)

33. Internet Governance Project

- General Contribution
- Framework Convention
- Political Oversight of ICANN

34. IP Justice - Realizing the Internet's Promise of Universal Access to Knowledge and Development

35. Baher Esmat and Juan Fernandez - International Internet Connections Costs

36. David Allen, Co-principal, World Collaboration for Communications Policy Research - The role of intellectual / academic work in a policy forum

37. Professor William H. Dutton, Director, Oxford Internet Institute - Addressing the Issues of Internet Governance for Development: A Framework for Setting an Agenda for Effective Coordination

38. Vittorio Bertola, Turin, Italy - Chairman, ICANN At-large Advisery Committee & Former Member of the Working Group on Internet Governance (WGIG)

    - An introduction to Trusted Computing
    - The Internet Bill of Rights
    - Intellectual Property and the Internet: Issues, disagreements and open problems

39. Rishab A Ghosh, Senior Researcher at the United Nations University Maastricht Economic and social Research and training centre on Innovation and Technology (UNU-MERIT) - An Economic Basis for Open Standards

40. Janice R. Lachance, CEO, Special Libraries Association - Transparency and Openness in a Global Economy

41. Jeremy Malcolm, PhD candidate in law researching the IGF - Multi-Stakeholder Policy Development within the IGF

42. Kuo-Wei Wu, Member of Executive Council, Asia Pacific Network Information Center (APNIC)

43. JFC Morfin, INTLNET President

44. Janet Hawtin-Reid , Computing and information design, Bettong.org - Promoting Principles which Encourage Innovation and Participation

45. Marc Perkel, Owner, Junk Email Filter dot com and Computer Tyme Hosting, The Problem with Spam on the Internet

Annex II

Glossary of Internet Governance Terms

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)
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
ICC	International Chamber of Commerce
ICT	Information and communication technology
ICT4D	Information and communication technology for development
IDN	Internationalized domain names: web addresses using a non-ASCII character set
IETF	Internet Engineering Task Force
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
IRA	International Reference Alphabet
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXPs	Internet exchange points
MDGs	Millennium Development Goals
NAPs	Network access points
NGN	Next generation network
NRO	Number Resource Organization, grouping all RIRs – see below
OECD	Orgnisation doe Economic Co-operation 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. These not-for-profit organizations are 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
SMEs	Small and medium-sized enterprises
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 Information Society