Wolfgang Kleinwächter (Ed.)

The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment

Titi Akinsanmi, Johannesburg · Adiel A. Akplogan, Port Louis Peng Hwa Ang, Singapore · Seiiti Arata Jr., Sao Paulo · John Carr, London · Olga Cavalli, Buenos Aires · Vint Cerf, Marina del Rey · Bertrand de la Chapelle, Paris · Dirk Cordel, Potsdam Veronica Cretu, Kishinev · Steve Crocker, Stanford · Kenneth Neil Cukier, Tokyo · Willie Currie, New York · Nitin Desai, New Delhi · Avri Doria, Lulea · William J. Drake, Geneva Anriette Esterhuysen, Cape Town · Philipp Grabensee, Düsseldorf · Kaili Kan, Beijing · Sarbuland Khan, New York Wolfgang Kleinwächter, Aarhus · Elmar Knipp, Frankfurt Ronald Koven, Paris · Latid Latif, Luxembourg · David Maher, Chicago · Koïchiro Matsuura, Paris · Christian Möller, Vienna Ram Mohan, Vancouver · Annette Mühlberg, Berlin · Milton Mueller, Syracuse · Pier Carlo Padoan, Paris · Claudia Padovani, Padova · Elena Pavan, Trento · David Piscitello, Los Angeles · Louis Pouzin, Paris · Jean Réveillon, Geneva George Sadowsky, Washington · Guy Sebban, Paris · Fatimata Seye Sylla, Dakar · Hamadoun Touré, Geneva · Michael Yakushev, Moscow

Germany
Land of Ideas

Wolfgang Kleinwächter (Ed.)

The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment

Wolfgang Kleinwächter (Ed.)

The Power of Ideas: Internet Governance in a Global Multi-Stakeholder Environment

The “Germany - Land of Ideas” initiative which was launched in 2005 by Germany’s political and business communities, under the auspices of Federal President Horst Köhler, aims to present Germany as a creative and innovative place for business and investment. The initiative enjoys broad support not only from business and academia, but also from the arts community and society at large.

The opinions expressed in this publication do not reflect the views and policies of “Germany – Land of Ideas”, but those of the authors.

Editor: Wolfgang Kleinwächter

Copyright© 2007 Marketing für Deutschland GmbH, Berlin
All rights reserved. No part of this publication may be reproduced in any form or by any means without the prior written consent of the publisher, excepting brief quotes used in reviews.

Jacket design and typesetting: dot.blue – communication & design
Editorial office: Wagner Translations, Ltd.
Printing and binding: Druckerei J. Humburg GmbH, Berlin
Printed in Germany

Foreword

Nitin Desai,
Special Adviser to the UN Secretary-General
on Internet Governance

The Internet is a product of partnerships. It began as a collaboration between the US Government and academia and research institutions. Soon NGOs like the APC joined in and, with the development of the world-wide web, a wider class of users became a part of the venture. Commercial users spotted the potential of business to business and business to consumer communication and started using the Net Governments also recognized the potential of the Net and, as part of the effort to make governance more transparent and more efficient, made many public services Net-accessible.

Today the Net is qualitatively different from what it was in its Arpanet days. It has outgrown its origins as a network run by and for computer specialists:

- It now has over a billion users worldwide and even those who are not users are affected by the potential of the Net.
- It began in the USA and then spread quickly in the OECD countries. But now the expansion is taking place in China, India, Brazil and other countries in the developing world.
- The languages that the new users are familiar with and which the Net must accommodate are very different from English and other Latin-scripted languages that dominated its early years.
- The software and other technologies that are essential for using the Net come more and more from commercial enterprises rather than not-for-profit research bodies.
- The use of the Net is now a central part of the business model of manufacturing and service companies, public administration, education, health care, news dissemination and entertainment.

- Internet-enabled services are transforming the landscape of the global economy by creating extraordinary capacities for disaggregating production processes and locating them flexibly to respond to comparative advantage.
- The Net is no more a one-way exercise in communication. With Web 2.0 the users of the Net are no longer merely receiving information, but are creating and disseminating it with a variety of peer-to-peer initiatives.
- The convergence of the Net with telephony, television, films and music is creating new issues for law and regulatory structures.

The purpose of this potted history is to establish two crucial points. First, the Net is a product of partnerships and therefore its management has to reflect a modality of cooperation between stakeholders who normally operate on different sides of the fences that define the traditional structures of governance and of the market economy. Second, the Net is a new phenomenon and is changing and evolving very rapidly and hence its governance must be flexible enough to allow for change in response to new technologies, new uses, new users and new challenges.

There are no standard models of governance that can help us to find our way here. The Net is not a corporation because it is not owned by anybody. Models of corporate governance therefore are of little relevance. The Net is also not a part of public infrastructure owned and operated by some authority. Hence a traditional approach to the management of public monopolies is of limited relevance. Even the model of a cooperative does not apply fully since most cooperatives are organized as a grouping of producers or of consumers and seldom of both groups together. Hence we have to find our way to a flexible modality of managing the Net by trial and error.

The exercise of finding a model for Internet governance began with the debates on the subject in the first phase of the World Summit on the Information Society (WSIS) in Geneva in 2003, continued with the Working Group on Internet Governance which submitted its report in 2005 and culminated in the outcome of the second phase of the WSIS in Tunis in 2005. The

Internet Governance Forum (IGF), which met for the first time in Athens in 2006, is part of this exploration.

These exercises have led to some meeting of minds. First, there is a wide acceptance of the need for a multi-stakeholder forum to provide a space for a dialogue amongst different stakeholders on Internet public-policy issues. Second, most participants in the debate accept that enhanced cooperation amongst stakeholders for oversight or governance should deal with matters which are within the remit of public policy and not with the technical and operational management of the Internet. Third, a range of views has been articulated on what needs to be done to make arrangements for Internet governance multilateral, transparent and democratic.

Taking its cue from the report of the Working Group on Internet Governance, the Tunis Agenda defines Internet governance as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet."(Para 34 Tunis Agenda)

The goals have been set by governments in the Tunis Agenda for the Information Society which states 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. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism." (Para 29 Tunis Agenda)

We are still working towards these goals. However no one wants to disrupt a system which is clearly working well. The issue is more one of recognizing the changing profile of Net use and Net users. More particularly there is a need to secure a greater engagement individuals and institutions from developing countries in Internet governance. In these countries, much of the technical capacity to participate in global processes of Internet management lies with the public sector. The justification for spending public money on the infrastructure for the Net is its use for public purposes like education, health and public administration. That is why governments from these countries are so much more insistent on gaining a role in Internet governance.

The Internet Governance Forum is an exploratory effort. It is an open-access environment not designed to take decisions but to function as a forum for airing different views and stimulating dialogue and discussion. Such a deliberative forum with no decision-making powers can make a difference for the better by showcasing good and successful efforts that can help to set a standard of good practice for the management and use of the Net. It can raise awareness about the governance implications of new developments like the recent explosion of user-defined content.

The IGF can lead to practical results if the contact between stakeholders leads to new partnerships for sharing knowledge and experience and, where relevant, to joint action. This happened in Athens at the first IGF where a number of dynamic coalitions were launched.

The IGF is a bit like a village or town meeting and relates to the established processes of Internet management as such a meeting relates to municipal governance. It gives voice to the users of the Net and helps to identify emerging issues which need to be tackled in the formal processes which are managed by Internet specialists. We saw in Athens at the first IGF how this forum can connect the Internet technical community with a wide class of users and stakeholders.

A forum where all stakeholders participate on an equal footing can be made to work. The experience with the Working Group on Internet Governance demonstrates this. The WGIG was a multi-stakeholder process, bringing together forty people who reflected the diversity that we saw in the Athens IGF. First, a protocol of dialogue developed where the group members listened to one another, responded to the points raised in a constructive manner and thus allowed mutual understanding to develop. Second, the process was very open and the group met with all stakeholders in open consultations at every meeting. Third, the effort was not to try and negotiate a compromise but to understand different points of view, and then to try and agree on the range of options which needs to be looked at by the preparatory process.

The IGF poses a great challenge for the organizers because a variety of cultures have to interact constructively. It is a forum which brings together governments who are used to the polite protocols of inter-governmental discussions, businesses who look for practical results from such meetings, NGOs, consumer rights groups and human rights activists who want to give voice to their concerns loudly and clearly, internet specialists who are familiar with the structured approaches to consensus building in their technical processes, the media which is there to cover the proceedings and to participate as a stakeholder. For the dialogue to work, all the participants have to adjust their expectations to take account of this diversity of cultures that are present in the forum. There must be as much listening as talking for a forum like this to work.

The "Land of Ideas" initiative must be commended for recognizing the importance of the IGF. It has sought to contribute to building a dialogue of good faith in diverse ways, including the preparation of this book.

The Internet is a new and rapidly evolving system. The dialogue on Internet governance is even newer. We are at an early stage of development, and with goodwill and understanding the stakeholders in the Internet will be able to find their way to a workable arrangement. The role of the IGF is to contribute towards this end by building bridges of trust and confidence and practical partnerships between the stakeholders. If it does that, it will have played a role not just in the evolution of the Internet but more broadly in the development of a new form of multilateral cooperation, and the ground rules for a novel form of diplomacy for a new type of global interdependence.

Introduction

Wolfgang Kleinwächter,
University of Aarhus, Special Adviser to the Chair of the Internet Governance Forum (IGF) and former Member of the UN Working Group on Internet Governance (WGIG)

When Bob Kahn und Vint Cerf developed the TCP/IP protocol in the early 1970s, nobody imagined that this technical protocol would revolutionise the world of communication and its governance. Just fifteen years later, in the late 1980s, the number of individual Internet users had soared to nearly a million. Another fifteen years later, there were more than one billion people online. And by 2015 – as projected by the UN World Summit on the Information Society (WSIS) - half of humankind will be connected, or more than three billion people.

Never before since the invention of the printing press by Johannes Gutenberg has a communication technology spread faster and deeper than the Internet. With the Internet there is now a material infrastructure available which allows everybody to communicate with everybody anytime and anywhere using text, date, images, voice and video. The vision of Article 19 of the Universal Declaration of Human Rights, adopted in 1948, that the individual right to freedom of expression includes the right "to seek, receive and impart information and ideas through any media and regardless of frontiers" had finally found its enabling technology. The Internet is penetrating all areas of life. It affects the way we live and work, learn and do research, shop, socialise and entertain ourselves.

However, even if more than one billion people are online today, this means five billion have no access to the Internet. Consequently, bridging the digital divide is one of the great challenges of our time. There is a need to develop policies, build infrastructures and educate people so that everybody can enjoy their right to communicate in the information age via access to the Internet. The explosion of borderless online communication among individuals and institutions has also produced a host of new problems, from managing critical Internet resources to fighting cybercrime, from promoting multilingualism on the Internet to protecting human rights and intellectual property in cyberspace, from introducing new applications for eGovernment or eHealth to managing eCommerce.

When representatives from governments, private sector and civil society came together to discuss the emerging issue of "Internet governance" during the first phase of the UN World Summit on the Information Society (WSIS), the difference in their approaches to dealing with the new Internet challenges became visible. While one group argued that the Internet should be globally governed by an intergovernmental UN organisation, others pointed to the fact that the Internet emerged bottom-up in the shadow of governmental regulation and is rather successfully self-organised by non-governmental entities representing the developers, providers and users of Internet services themselves.

Reorganising a trans-border mechanism with more than one billion users on a global level is a rather complex challenge. "If it ain't broke, don't fix it" recommended Vint Cerf, the man who co-created the protocol that allowed the emergence of the Internet. On the other hand, governments cannot stand aside once the Internet becomes part of their nation's critical infrastructure, crucial to the national economy, policy development and cultural communication.

To bring more light to this new subject of global policymaking, the 1st WSIS Summit (Geneva, December 2003) decided to establish a multi-stakeholder "Working Group on Internet Governance" (WGIG) with a mandate to propose a definition on Internet Governance, to identify public policy issues related to Internet Governance and to clarify the role of the various stakeholders involved. But while the list of controversial issues was long, all partners agreed that the Internet should not be governed by a single organisation alone, and that in all stakeholders, in their specific roles and responsibilities, need to be involved in its governance.

A CALL FOR CREATIVITY

At the Global Governance Forum in New York in March 2004 – on the eve of the formation of the WGIG - UN Secretary-General Kofi Annan summarised the situation as follows: “The issues are numerous and complex. Even the definition of what is meant by Internet governance is a subject of debate. But the world has a common interest in ensuring the security and the dependability of this new medium. Equally important, we need to develop inclusive and participatory models of governance. The medium must be made accessible and responsive to the needs of all the world’s people”. He added that “in managing, promoting and protecting [the Internet’s] presence in our lives, we need to be no less creative than those who invented it. Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different.”[1]

When the WGIG took up its work in October 2004, Kofi Annan’s challenge for more creativity became its “leitmotif”. The WGIG Report produced a definition on Internet Governance, an extended list of related public-policy issues and specifications of the responsibilities of the involved stakeholders. WGIG submitted a number of models for the enhancement of multi-stakeholder cooperation for the oversight over critical Internet resources and recommended the creation of a new global discussion space for Internet policy development, the “Internet Governance Forum” (IGF).

The WGIG report, presented in July 2005, became the basis for the adoption of the “Tunis Agenda for the Information Society” by the 2nd WSIS Summit in November 2005. The Tunis Agenda recognised the fact that the Internet, along with its infrastructu-

[1] Kofi Annan, Internet Governance Issues are Numerous and Complex, New York, March, 25, 2004, in: http://www.unicttaskforce.org/perl/showdoc.pl?id=1333, see also: Wolfgang Kleinwächter, WSIS, ICANN, GBDe: How Global Governance is Changing in the Information Age; in: Bart De Schutter & Johan Pas (ed.); About Globalisation: Views of the Trajectory of Mondialisation; Brussels University Press, Brussels, 2004, p. 205 – 226, Wolfgang Kleinwächter, Internet Co-governance: Towards a multilayer multiplayer mechanism of consultation, coordination and cooperation (M3C3), in: E-Learning, Oxford, Vol. 3, No. 3, 2006, p.473 – 487

re and applications, consists of many layers where numerous governmental and non-governmental players are involved with specific roles and responsibilities, and that there is a need to enhance communication, coordination and cooperation among the various players to ensure the Internet's continued functioning, as well as its stability, security and further development. The fact that no one single organisation is responsible for the Internet, and that instead it is governed by a multilayer, multiplayer mechanism, helped in designing the IGF as an open multi-stakeholder and multidisciplinary discussion forum for all issues related to Internet governance. The idea of the IGF is to bring the various stakeholders together and enable them to discuss existing and emerging issues from various perspectives without the pressure to find a political or legal consensus and to agree on "diplomatic language" at the end of the debate. The vision is that such a high-level multi-stakeholder discussion will help the organisations and institutions involved, which hold a mandate to deal with specific elements of the Internet, to make better-informed and more qualified decisions within their individual fields of competence. From such practice a diversified multi-stakeholder governance system could emerge which would to a certain degree reflect the decentralised architecture of the Internet.

CHECKPOINT 2010

The IGF's initial mandate ends in 2010. With the IGF, the global Internet community has set out to map the uncharted, borderless territory of cyberspace. It remains to be seen whether by "Checkpoint 2010" something new has been developed that meets the high standard set by Kofi Annan in his New York speech of 2004. The IGF's innovative concept of open discussions from different perspectives on an equal footing among various stakeholders was the source of inspiration for this book project. In publishing it, the German public-private partnership "Land of Ideas", under the patronage of Germany's Federal President Horst Köhler, seeks to make a contribution to this broad multilayer, multiplayer and multidisciplinary debate, offering a space for known and unknown authors to be heard, allowing various perspectives and positions to be channelled into the global dialogue. The aspiration is to help the 2nd Internet Governance Forum in Rio de Janeiro in November 2007 to become a successful step towards the "Internet Governance Checkpoint 2010".

The publication does not reflect the "German position". Its aim is to enrich the global discussion. The articles in the book clearly reflect a broad range of different positions, including controversial approaches which probably would not be seconded by the German government in diplomatic negotiations. The point is not to deliver a final answer to a new global problem, but to stimulate innovative and creative thinking about new issues. Sustainable and workable concepts will emerge only as a result of controversial discussions in which arguments are pitted against other arguments, all perspectives are aired, and all players are allowed to make their voices heard on an equal footing.

The structure of the present volume follows the structure of the IGF itself, as developed by the IGF Advisory Group (IGF-AG) prior to the 1st Internet Governance Forum in Athens in October 2006. It has six chapters: Access, Diversity, Openness, Security, Critical Internet Resources and Emerging Issues. The authors hail from governments and intergovernmental organisations like ITU, UNESCO and OECD, from private-sector members like ICANN, the International Chamber of Commerce (ICC), Afilias Ltd. and Microsoft Russia, and from civil society organisations like ICANN's At Large Advisory Committee, the Association for Progressive Communication (APC), and the African Civil Society Information Society Initiative (ACSIS). Globally recognised technical and academic experts and well-known journalists comment on issues related to the IGF's central subject, "Internet Governance for Development". The book also gives a voice to authors from geographic regions – China, Africa, Asia, Latin America, and eastern Europe - often neglected in the mainstream of global Internet publications.

Books of this kind normally have not only an introductory chapter, but also a chapter entitled "Conclusions". This book has no concluding chapter. The conclusions will be drawn by the readers themselves. Its readers are invited and encouraged to feed the global debate at the IGF with their personal reflections or their institution's ideas. From the "Land of Ideas," we present to you an idea which we hope will stimulate debate, promote capacity building, and contribute to enhanced communication, coordination and cooperation!

The editor, who himself has been involved in the development of global Internet governance policies in various capacities for more than ten years, wishes to thank all authors who were kind enough to contribute to the book at such short notice.

Table of Contents

Chapter 1: Access

Chapter 2: Openness

Chapter 3: Diversity

Chapter 4: Security

Chapter 5: Critical Internet Resources

Chapter 6: Emerging Issues

Chapter 1

Access

Access to Access: A Development Sector Perspective on Access in Sub-Saharan Africa

Titi Akinsanmi,
Program Manager, Global Teenager Project,
SchoolNet Africa, Johannesburg

THE CONTEXT: GOVERNING THE INTERNET

Internet Governance (according to the International Telecommunication Union) consists of the collective rules, procedures, processes, and related programs that shape social actors' shared expectations, practices, and interactions and result in practices and operations that are consistent with the sovereign rights of states and the social and market interests of end-users and operators. It includes agreements about standards, policies, rules, and enforcement and dispute resolution procedures. Governance could be taken as the collection of processes that determine how power is exercised, how stakeholders are given a voice, and how decisions are made – whether in the private or public sphere. The ability of any kind of governance to be effective is strongly constrained by access to the cultural, social and economic resources necessary for participating in it. Some argue that the Internet is not or cannot be governed. Instead, it could be said to be coordinated. However, its coordination lies in the hands of those who could be termed "big players" – i.e. those who have the know-how and financial resources to shape its direction. Over the past couple of years more and more sectors of self-regulation have emerged where governance of the Internet is taking place. This has given rise to a heated debate across the Information Society, where the control and regulatory aspects of Internet Governance issues - including cybercrime, intellectual property rights, critical Internet resources and interoperability - have tended to overshadow the broader discussions of the enabling and social aspects of Internet governance.

INTERNET GOVERNANCE AND ACCESS

The UN Working Group on Internet Governance has identified various clusters of issues in relation to Internet Governance. I will focus on one of these: the issue of access. My choice of access as a focus topic was influenced by several factors including a bias to the circumstances of sub-Saharan Africa where access to physical infrastructure, linguistic diversity, and a continuing lack of infrastructure and non-implementation of government policy remain key challenges.

Technical access to ICT and in this case to the Internet is often discussed as the main prerequisite to economic and social development, whereas social access to literacy, content, applicable knowledge and health are not given much consideration. Access to the Internet in any part of the world is hindered by a complex array of factors encompassing physical, digital, human, and social resources and relationships.

In sub-Saharan Africa, access is being addressed in myriad ways from fiber optics being laid over land and across oceans, to mobile connections having a higher penetration and wireless technologies filling our airwaves. We are encumbered by a complex network of constraints characterized by a high level of disparity in Internet access and usage, low levels of digital and

INTERNET USERS AND POPULATION STATISTICS FOR AFRICA
Source: Internetworldstats.com

AFRICA REGION	Population (2007 Est.)	Pop. % in World	Internet Users Latest Data	Penetration (% Pop.)	% of Users in the World	Use Growth (2000-2007)
Total for Africa	933,448,292	14.2 %	33,545,600	3.6 %	3.0 %	643.1 %
Rest of World	5,641,218,125	85.8 %	1,139,564,325	20.2 %	97.1 %	219.7 %
WORLD TOTAL	6,574,666,417	100.0 %	1,173,109,925	17.8 %	100.0 %	225.0 %

information literacy, limited quality, availability and affordability of the physical network including telecommunications and electricity networks.

I then ask myself, now that we are providing these multiple levels of access to the Internet and to new technologies and new frontiers – have we addressed properly the people's capability to access these 'access' routes? Are they equipped to harness the technologies we offer? Are they knowledgeable enough to utilize the potential before them? Do they have the wherewithal to make accessing these 'access routes' a priority in their lives? These are the questions facing the development sector as we continue to bridge the digital by addressing the issue of Internet governance, and which the term "access to access" refers to.

"ACCESS TO ACCESS"

Access to access refers to the capability of all users of Internet technology - irrespective of creed, religion, age or gender - to take advantage of the physical "access" or connectivity that has been provided. In other words, myriad other variables, in addition to an Internet connection, determine whether the Internet is really "accessible". (I thank Maja Andjelkovic for helping to shape this definition). These variables may include appropriate legal and regulatory frameworks and policies, relevant content, available in the local language(s); the provision of training and capacity building; presence of relevant equipment and technical support; and even electricity. I refer minimally to four of these variables in this article.

THE ISSUE OF POLICY/REGULATORY FRAMEWORKS

With regard to access in sub-Saharan Africa, the key governance question continues to be more local than global. The global environment is sure to keep changing. Where a universal service regime is implemented through tax-based financing or by employing new funding paradigms through remittances and revitalized development assistance channels, improved access cannot be achieved without enabling the legal and regulatory frameworks and institutionalizing a climate for innovation and the political will of governments to constantly craft and implement policies that promote universal access and even more so put in place implementation strategies that consistently keep the public informed on what these are and how they can be of benefit.

Not to belittle the relevance of global policy or governance mechanisms, but a truly international governance regime for the Internet needs to be put in place. One that is developed and agreed to by all players, not just the status quo of largely developed countries. One that truly reflects, while not necessarily replicating, the diversity of presence the Internet has and the global tool for life it has become.

Governments need to continue to acknowledge the value of the Internet and other information technologies through positive policies. This includes everything from ensuring that freedom of expression is supported, to continued provision of funding for the infrastructural development required for adequate Internet access in all areas of a society – from remote mountain regions and seaside communities to thriving cities that serve as economic hubs.

I note though that the national policies we have seen adopted across Sub-Saharan Africa over the last few years has not automatically led to the implementation of ICT programs which promote access to access – except in countries that have the necessary financial and skilled human resources, dedicated leadership, predictable and stable investment frameworks, political stability and incentives both for the private and public sector.

THE ISSUE OF CAPACITY BUILDING: APPLICABLE KNOW HOW

The issue of capacity building has been well thrashed out and trainings have been put in place to address this. My question though is how much of it is really applicable know-how, shaped to meet ever-changing local needs?

Capacity building should aim to enhance individual as well as institutional capacities to not only make the best use of a given situtation, but also to adapt and respond to changing local needs (in the case of Sub-Saharan Africa, triggered by regularly changing government regimes and policies).

Factors that continue to impinge on the strategic use of ICTs and in particular the Internet in Sub-Saharan Africa include an enduring low level of ICT literacy and a lack of capacity to generate, adequately utilize or capture knowledge and information relevant to the local needs. Where this does happen, it is increasingly supported by relatively short-term donors and private sector funds, which in most cases creates a larger ‘gap’ once the funding tenure expires. This confirms yet again that local capacity- and skills-building is the fertile ground needed for sustainable development processes.

THE ISSUE OF COST

This is one area where we see a clear gap between how things should operate in an ideal world and how they actually operate. The theory is that the Internet, as a network of networks sharing a common protocol, almost self-organizes to find the most efficient way of sending information from one computer to another. The cost involved should be in connecting to the network.

Internet Service Providers (ISPs) offer their customers a bundle of services that typically includes hardware and software, customer support, Internet Protocol (IP) transport, information content and provision, and access to individuals and information sources on the Internet. In practice though, the cost of routing network traffic has been the largest cost inflator in this part of the world. Africa’s link to North America is 20 times less than that of Latin America, which has a comparable population. Local loops are generally outdated and unable to support reliable connections. The situation to date is that you send an e-mail to a friend or colleague in Kenya from Nigeria and it gets routed via a European or American node because the in most cases the intra-continental networks do not have a peering agreement. These costs usually end up being paid by the Internet user – whose daily priorities just might not allow for such financial commitment. This is being addressed as an ongoing concern by institutions like AFRINIC and AFNOG and the further opening of the markets to private-sector investors. The downside of the private sector driving Internet penetration in Sub-Saharan Africa is that if the Internet exists mostly in the private sector (with the final routing managed - as is the case in most Sub-Saharan African countries - by state owned agencies), the private sector's goal continues to be centered around profitability. Among other things, this creates monopolies around market segments, with businesses catering to the part of the market which yields the biggest returns, and excluding the majority of the community, which generally cannot afford such products and services.

THE ISSUE OF PARTICIPATION AND RELEVANT CONTENT

Developing local software and local-language content (in written and oral formats) is the most fundamental and urgent priority in addressing access to access: all other things remain irrelevant if the content has no relevance for the local user. One of the most significant issues has been the fact that Internet content is dominated by the written word. This excludes participation by users who lack print literacy. This has a particularly significant impact in large parts of Sub-Saharan African society, which has its roots in oral and pictoral exchange of knowledge and information, and other ways of circulating information. This is being overtaken more and more by the use of audiovisual content, particularly in social and news-based sites. Also, the media convergence fostered by technologies such as VoIP and wireless technologies potentially provides an important context for non-text-based interactions on the Internet. However, the issue of bandwidth to support such Internet content remains largely unaddressed. There are many serious human rights issues involved in the restriction of access to content. These must be carefully balanced with legitimate needs to regulate the circulation of restricted materials in the public interest (e.g. controlling obscenity). The governing structures that 'manage' the Internet continue to largely ignore this fact – as do governments, mainly because there are no applicable agreed international laws to ensure unified compliance across the world.

ONLY THE BEGINNING

“Access to access” includes all of the requirements that must be met, in addition to connectivity, before any person can realize their potential in using, adapting and creating Internet technology. Content and language, literacy and education, and community and institutional structures must all be taken into account if meaningful access is to be achieved.

If we can properly show any poor region of the world or poor person how the Internet and all issues surrounding it can help meet their basic living needs, then access can be taken to the next level and we can achieve our larger development goals – in time.

Internet Governance for Development: Actions to Take to Promote Access in Africa

Fatimata Seye Sylla,
National Coordinator of ACSIS[1], Senegal, Dakar

INTRODUCTION

The main aim of this article is to suggest some ideas for how the Internet Governance Forum could catalyze the international community to take appropriate actions to connect African countries to the Internet, for purposes of human development. Despite the constant debates about the priorities Africa must face before dealing with Internet issues, the first part of this article seeks to demonstrate the importance of Information Communication Technologies (ICT) and Internet access for Africa as a tool for accelerating development. The second will explain Internet access-related issues in Africa, underlining barriers such as: illiteracy, lack of infrastructure and local content[2], absence of appropriate regional policy. It will also present the major initiatives to provide broadband connectivity in the region. Finally, suggestions are made for how the Internet Governance Forum itself can invite the stakeholders to take immediate actions to promote Internet access in Africa.

ACCESS TO ICT AND INTERNET ARE PRIORITIES FOR AFRICA

The following are some examples taken from my own 25 years of experience in dealing with projects to provide access to Information Communication Technologies (ICT) and the Internet to underserved people in Africa, with the ultimate aim

[1] African Civil Society for the Information Society www.acsis.sn

[2] Content produced by or with African people on African related issues

of bridging the digital divide: between rural and urban areas, between men and women of different professions, between the young and the elderly, educated and illiterate, poor and wealthy, and handicapped and non-disabled people.

1. In 1982, Senegal was among the first countries to introduce computers in primary schools with the "Logo"[3] project. The aim of this project was to study the impact of computers on learning and teaching. The project demonstrated how, in an ICT-rich learning environment children were more eager to learn and to take the initiative in dealing with their teachers. A 9-year-old girl who hated mathematics ended up explaining geometry to her classmates using computer graphics. Teachers also demonstrated their ability to produce local educational content (tutorials in grammar). The results were very positive even though the Internet had not yet been introduced.
2. In 2001, in Senegal, I was a member of the multimedia caravan team set up by Osiris[4] with the support of Worldspace[5], Sonatel[6], Senelec[7] and other local private companies. The objectives of this caravan were to bring the technology to people who had never heard about it and study how they would react to it. The caravan toured Senegal and Mauritania for six months, providing information and creating awareness about ICT and the Internet among people from remote areas. The caravan's drivers, who had barely attended high school, became IT trainers, teaching people how to use ICT and the Internet. The caravan went on to Ghana under the auspices of Worldspace.

[3] The Logo project was named after the computer programming language invented by Dr. Seymour Papert of M.I.T. and developed by LCSI (www.lcsi.ca) for children's education. Logo was translated into Wolof, the most widespread local language in Senegal and The Gambia.

[4] Observatoire des Systèmes d'Information, Réseaux et Inforoutes du Sénégal: www.osiris.sn

[5] In partnership with Worldspace, digital radio stations were provided: data collected from the Internet could be translated and aired in local languages and vice versa. See www.worldspace.com

[6] Société Nationale de Telecommunication (www.sonatel.sn), the major Senegalese Telco private company

[7] Sénégalaise de l'Electricité, the national electricity company (www.senelec.sn)

3. In 2002, the Bokk Jang[8] NGO in Senegal set up training centers with Internet access for youth and women in poor neighborhoods, allowing thousands of children to use the Internet for their education in an informal environment, providing new job opportunities for the communities, and in the process helping to prevent juvenile delinquency. A young maid went on to become a cyber café manager in a suburb of Dakar.
4. In 2005, as part of the Digital Freedom Initiative[9] Program, a women's association with 3,000 members started to explore the Internet to access the international market to sell their products. Local illiterate (in western languages) merchants were assisted to use the Internet in a popular market to have access to other suppliers around the world with more competitive prices. Access to the Internet was provided thanks to a cyber center located in the heart of the market.
5. In January 2007, the NGO ENDA[10] began a 30-month research project funded by IDRC[11] on the use of ICT and the Internet, and youth participation to contribute to the eradication of female genital mutilation (FGM) in West African French-speaking countries, targeting Burkina Faso, Mali and Senegal. A virtual forum[12] will be held with the participation of youth in urban and rural areas and activists involved in this issue in Africa and Europe.

The lessons learned from these projects indicate that if access is provided, even illiterate and poor people are eager to use ICT and the Internet for their benefit. They were all inventive in using the tool to fulfill their needs. With Logo, school children became acquainted with the new technology and acquired knowledge with the teachers creating local content. The Osiris caravan proved that radio broadcasting is an appropriate means

[8] A Senegalese nongovernmental organization. Bokk Jang means "Learn together" www.bokk.org

[9] A USA presidential initiative. Senegal was the pilot country. A USAID funded program www.dfi.gov

[10] A Non Governmental Organization www.enda.sn

[11] International Development Research Center, Canada (www.idrc.ca)

[12] See http://www.famafrique.org/tic-mgf/introsforum.html for more information

for illiterate populations to use the Internet. Radio content produced by local populations or collected through the Internet was digitally stored and aired. The local languages were used in communications. Communication between local leaders, the population, and emigrants was eased thanks to the magic of Voice over Internet protocol (VoIP), images and video. Bokk Jang gave youth opportunities for income-generating activities. The Enda/IDRC project enabled youth in rural areas to hold meetings on the FGM themes and use a cyber café to post highlights of the discussions to the virtual forum. Information and awareness-building on relevant issues such as malaria or FGM, or nutritional facts about local crops have a better impact if local communities participate in the measures as actors. The Internet and ICT are great enablers.

Today, the Internet facilitates people's access to education, health, business, individual economic development and networks through different sources of related information. The Internet is a vehicle towards true development, not only for primary access to water, food, health and shelter but also to the knowledge and means to boost the economy. But very few people from developing countries have access to it to be able to profit from all the opportunities it offers. In Africa, 96 percent of the population does not have access to the Internet.[13] The barriers are serious but they can be overcome.

INTERNET ACCESS FOR AFRICA

Internet access has a specific meaning in African countries It concerns not only the availability of infrastructure, but also the skills to use the tools (equipment and software) to produce and share meaningful content. To be meaningful to Africa, any participation in the management of the Internet should facilitate access. However, the following barriers must be overcome:

- **Lack of Infrastructure:** electricity, telecommunications, computers and software, broadcasting (TV and Radio) equip-

[13] Internet Usage Statistics for Africa (Africa Internet Usage and Population Stats), 2007, http://www.internetworldstats.com/stats1.htm

ment mainly in the rural areas: more than 75 percent Africa's population is rural. The most recent statistics11 indicate that Africa represents:

1. 14.2 percent of the world population (933,448,292)
2. 3 percent (33,545,600) of the world's 1,173,109,925 Internet users

However, in Africa, the indicator "numbers of users" is wrongly evaluated because many people share accounts and computers, use corporate and academic networks, or visit cyber cafés and business centers

3. 3.6 percent Internet penetration
4. 643.1 percent growth in Internet usage

Africa is aware of the necessity to get connected to the rest of the world, and the limitations of expensive satellite systems to carry voice and data services. Several initiatives to build broadband cables have been taken:

1. SAT3/WASC/SAFE[14], launched in May 2002, is providing a faster means of connecting the continent to international markets. 36 nations are involved, among them 11 African states. (Senegal, Cote d'Ivoire, Ghana, Benin, Nigeria, Cameroon, Gabon, Angola, South Africa, Reunion and Mauritius).
2. Ethiopia has built its own fiber cable
3. South Africa is planning to build a submarine cable to be connected to other international cables in the British Virgin Islands
4. 4 fiberoptic cable sub-regional projects to connect the African east coast:
   - EASSy[15] is planned to connect 8 coastal countries in eastern and southern Africa (Sudan, Djibouti, Somalia,

[14] "SAT-3/WASC or South Atlantic 3/West Africa Submarine Cable is a submarine communications cable linking Portugal and Spain to South Africa, with connections to several West African countries along the route. It forms part of the SAT-3/WASC/SAFE cable system, where the SAFE cable links South Africa to Asia" http://en.wikipedia.org/wiki/SAT-3/WASC_%28cable_system%29

[15] "…Eastern Africa Submarine Cable System (EASSy) is an initiative to connect countries of eastern Africa via a high bandwidth fibre optic cable system to the rest of the world". http://en.wikipedia.org/wiki/EASSY

    Kenya, Tanzania, Mozambique, South Africa, Madagascar) and 11 land-locked countries (Ethiopia, Lesotho, Uganda, Swaziland, Rwanda, Malawi, Burundi, Zimbabwe, Zambia, Botswana and the Democratic Republic of the Congo)
    - The Kenyan government's TEAMS (The East Africa Marine Systems), expected to be operational by the end of 2008, will connect Kenya and the Great Lakes region
    - Flag Telecom, a project to link South Africa to Kenya via Mozambique, Tanzania, Madagascar and Mauritius by the end of 2009
    - SEACOM[16], a privately funded project that would follow the same path as the EASSy but would cost less.

- **High cost** of infrastructure and bandwidth due to insufficient intra-continental links: The only operational sub-regional cable is not yet affordable: the SAT-3 cost is between "USD$4500-$12000 per Mbps per month, over 50 times greater than bandwidth prices in the U.S."[17]
- **Illiteracy** and lack of awareness of the benefits of the Internet, along with lack of training in its use: a lack of human resources to install, operate, develop, set policy and produce content. Projections show that Africa's literacy rate will barely exceed 60 percent in 2015. In sub-Saharan Africa, it will be 59 percent.[18]
- **Lack of local content** produced by or for African populations to suit their needs (and mainly in African languages): none of the top 10 languages on the Internet is African[11]. Web content is mainly represented in areas where competencies are available such as media, art and culture, but largely lacking in education, science, technology, statistics and e-government.
- **Lack of coherent regional policy** to tackle the common problems and find transparent and sustainable solutions (create a

[16] Source: Russell Southwood, Balancing Act: http://www.balancingact-africa.com/news/back/balancing-act_349.html#head

[17] http://en.wikipedia.org/wiki/SAT-3/WASC_%28cable_system%29

[18] http://portal.unesco.org/education/en/file_download.php/b26b3b6affe7addd60f98a244b7836672adultyouthliteracy.pdf

common infrastructure with reasonable access prices): SAT3 is a good example of available but inaccessible broadband due to its extremely high cost. EASSy is another project that demonstrates the lack of trust and commitment among African countries, many of them trying to go it alone (Ethiopia couldn't wait any longer for the controversial EASSy project and has built its own fiber-optic cable. Ironically, the African Union Headquarter and the UN Economic Commission for Africa are both located in Addis Ababa).

The IT landscape may not be attractive, but Africa has strengths worth investigating. Only 3.6 percent of the population has access to the Internet but its usage growth rate is impressive (643 percent).[11] Therefore, developing the Internet to reach the next billion has to be done with the African market. Giving more people access to the Internet means more resources to manage, more online jobs for developing countries, fewer immigration problems to solve and more worldwide peace. Africa also has natural resources that need to be better managed in order to invest in other priority areas like access to the Internet. Its cultural values are a key to maintaining diversity in the world.

ACTIONS FOR THE INTERNET GOVERNANCE FORUM

Without access to the Internet, Africa and the other developing countries will be left out of the information economy. Globalization means no country should be left out; every country should be able to give and receive something in a win-win situation.

Depriving developing countries of access to the Internet is tantamount to subjugating their already weak economy with foreign products and cultural values, maintaining them in a status of eternal consumers and dependent on the developed world. For an equitable and humane global environment resulting in a peaceful world, access to the Internet must be facilitated for developing countries. If the Internet can boost people's economic development, Africa is one of the continents that need it the most, because of its poverty. 34 of the poorest 50 nations are in Africa according to the UN list of least developed countries.[19]

Internet governance is about Internet access and use for the benefit of the world population, without discrimination. Internet governance is about multi-stakeholder participation as defined by the Internet Working Group set up during the first phase of the World Summit on the Information Society[20] (WSIS). Following the WSIS Tunis phase, the Internet Governance Forum (IGF) was set up with a mandate to "Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world" and to "Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries."[21]

If participation means having every country contribute according to its knowledge about Internet issues, then the voices of more than 80 percent of the African population will always be translated by representatives who may not be aware of their real problems nor understand the languages spoken by them. For Africa to participate meaningfully, affordable bandwidth and new participation tools have to be available to its populations.

The western model of providing access to the Internet to individual homes cannot be replicated in today's Africa because of the high cost of equipment, illiteracy levels and the population's low income. "In many nations, the per capita income is often less than $200 U.S. per year, with the vast majority of the population living on much less."[22] Connecting Africa with affordable bandwidth should mostly involve taking into account the following existing facts:

[19] http://www.un.org/special-rep/ohrlls/ldc/list.htm

[20] "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." Source: Report of the Working Group on Internet Governance http://www.wgig.org/docs/WGIGREPORT.pdf

[21] Report of the Tunis phase of the World Summit on the Information Society (para 72 e & f): http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2331|2304

[22] Poverty in Africa: http://en.wikipedia.org/wiki/Poverty_in_Africa

- Our culture of “sharing” food and tools can be an opportunity to bridge the digital divide. Some cultural practices which have impacted human development, such as the extended family, must be documented and shared. With the support of the Internet Governance Forum (IGF), governments and private companies should take into account this cultural fact in their IT development programs. If the computer is set in the family bakkyard with the parents and other family members using the same tools to access the Internet and share information, there will be less privacy to visit non-recommended sites, and it might be safer for children to surf. The tools must take into account the oral tradition of the population and the weather conditions (heat, dust and humidity). Radio broadcasting systems such as community multimedia centers[23] and mobile phones should be used to provide more Internet access to remote areas, as this is the most popular information provider in Africa: in 2002, 25 percent of the population had access to a radio[24], and they are found in remote rural areas. This would boost local content production and knowledge sharing.
- IGF should promote awareness and mobilization of civil society at the national, regional and international levels, involving more youth, women and people with disabilities. Experience has shown that African women can succeed in pushing their governments and partners to take milestone decisions against the private sector or traditional leaders. Almost all the social fights for the betterment of the African populations have been led by women and youth (against various forms of violence towards women and children, malnutrition and disease). The Internet is not only a tool for economic development but also for social and cultural improvement. The universal access funds being established in many African countries should be geared more towards access to the Internet for: a) jobs (outsourcing, call centers); b) access to ideas and knowledge for students and professionals; c) access to world

[23] The Community Multimedia Centers http://www.unesco.org.webworld/cmc/

[24] Mike Jensen. “The African Internet – A status report”, July 2002. http://www3.sn.apc.org/africa

trade; d) networking for advocacy; and e) democracy (online media and interactions with mobile phones worked for more transparency in the elections in Senegal).

- IGF should recommend more private-sector involvement to bring low cost bandwidth to developing countries, as well as a strong regulatory body (at national, regional and international levels) that would enable more transparency for fair competition among telecommunication operators. New operators should have access to information about the existing cables (capacity and tariffs). Affordable international bandwidth is a must. As there are only three companies in the world that can build fiber-optic cables (Alcatel-Lucent, Tyco International and NEC), IGF could recommend the creation of a multi-stakeholder committee including these companies to study how best they could work in Africa to provide affordable access. These companies could join forces with government agencies and local private organizations to diversify their activities and invest in content production, application development and creation of technological tools with resources taking into account local languages and oral traditions. The business model should be studied to reach the bottom of the pyramid (the rural areas), putting humanity up front while still remaining profitable.

CONCLUSION

"Africa needs to invest US$11 billion per year over a ten-year period to reach its target of ten percent teledensity by the year 2010."[25] Ignoring the problem and expecting it to be solved at national level by governments and the private sector will not result in good Internet access for people in developing countries. Even though Public Private Partnership projects have achieved a good deal of infrastructure (SAT3), the results are still insignificant in relation to the acuity of the needs. This is not the time for more debates about Africa's need for the

[25] 2006 Telecoms, Mobile and Broadband in Africa, Market Overviews report Executive Summary http://www.budde.com.au/publications/annual/africa/africa-overviews-summary.html?r=51

Internet and ICT. Many pilot projects have been executed, conferences and workshop seminars organized to settle the importance of being an active member of the information society. What is needed today is action to provide access through:

1. Affordable bandwidth to connect Africa to the rest of the world, to share knowledge and other resources
2. Appropriate technical tools (digital radio, mobile phones linked to the Internet, etc)
3. Local content.

Development is not just about having access to water, food, health and shelter but also about improving the quality of life. Knowledge is key to the development of any asset. Today, the Internet is the way to obtain knowledge. The Internet Governance Forum's activities will only be meaningful to Africa and other developing countries if at least a program to promote access is undertaken by the end of its second year, towards a fair and humane information society.

Internet Access in Latin America: From Asymmetry to Universal Access

Olga Cavalli,
Ministry of Foreign Affairs of Argentina, Buenos Aires

INTRODUCTION

Telecommunication networks and services have improved since privatization and because of competition. Due to these changes in regulation during the 1990s, the total number of telephones in Latin America increased by nearly six times[1] between 1995 and 2004, driven in particular by mobile telephony services. But these improvements have happened mainly in urban areas where there is a large enough market for providing services and making private companies profitable. From a regional perspective, Latin American is unique because it is the most inequitable region in the World[2]. This inequity is related to a highly imbalanced distribution of assets (land, capital, education and technology) and unequal access to them[3]. During the last decade, regulatory changes have shaped the telecommunications and Internet industries and networks in ways that did not always benefit the region's developing countries, broadening this social and economic gap. This gap is also present in people's access to the services and networks that provide Internet connectivity. Other facts that influence this situation are related to geography, distances between the north and south, and the availability of infrastructure in rural areas. This document will explore the different factors that shape this access asymmetry and will propose some lines of action to narrow the existing gap.

[1] Regulatel.

[2] World bank, Eclac.

[3] Eclac, The Millennium Development Goals, A Latin American and Caribbean Perspective.

REGULATORY FRAMEWORKS AND THE NATIONAL GAP

Regulatory frameworks have shaped the local telecommunication markets into what they are today. Governments played a major role in this process, being the relevant actors in setting the rules. The most important changes to regulatory frameworks happened after the privatization processes. All regional telecommunication services changed dramatically. Old networks had very low penetration and after their renewal, teledensity[4] indexes surged to nearly their current levels in all the countries of the region. The higher demand for connectivity came from big cities and dense urban areas, where the biggest market for services was also found. As a result, today these areas are very well connected by several networks using diverse technologies, and can access a wide range of services. Rural areas, not being so profitable in terms of market and service demand, are to this day usually reached by just one operator, generally the incumbent one.

In order to face the challenge of opening markets to competition, the new regulatory frameworks included the concept of Universal Service, creating Access Funds to subsidize unprofitable areas or unprofitable users of services. On the other hand, licensing rules were created for newcomers to allow competition. In general, the requirements for new operators were much lower than those for privatized companies. For this reason, new infrastructure was mostly installed in profitable urban areas. These rules, which included the concept of Universal Service, were drawn up with the idea of giving citizens access to telephony services. The concept of Internet access was not directly related with them simply because the Internet wasn't as developed as it is today.

The fact that most networks were installed in urban areas means that infrastructure availability for Internet access is very low in rural areas or in those small villages of the interior that are loca-

[4] As an example figures of Argentina can be considered. After privatization of the state owned telephone company Entel, there were 3 Millions fixed telephone lines, some years after privatization there were 8 Millions of fixed telephone lines. Source: National Commission of Communications

ted far away from capital cities. This is a real challenge for access. If an ISP wants to set up a business in these villages, its price for end users must include data link costs from the small city to the capital city – which is very expensive – plus Internet connectivity charges. As these areas generally have lower income per capita, competence in Internet access services is low, almost nonexistent. Therefore, such services are usually provided only by incumbent companies.

UNIVERSAL ACCESS AND WIRELESS SERVICES

The original concept of the Universal Service Funds was established in relation to availability of fixed telephony service, but the enormous success of mobile telephony has turned into the new real universal service. Mobile telephony penetration levels are very high in all countries of the Latin American and Caribbean region, while fixed-telephony teledensity indexes have remained at similar levels for the last decade. For many rural and suburban citizens, mobile telephones are their first experience with a telecommunication service. The availability of various charging methods, such as prepaid cards and especially the development of "calling party pays", have generated a sort of subsidy between fixed and mobile telephony that has pushed serviced demand to unexpected highs in all countries of the region.

The steep growth in mobile telephony has pushed the installation of newer infrastructure to support the service, in regions that had no infrastructure before. Most of this new infrastructure is based on wireless networks using microwave links or WiMax technology. Wireless backbones are easy to install and the spectrum frequencies needed to build them are usually available in rural areas.

The high usage of mobile telephony and the growth of the supporting infrastructures raise some Internet access-related questions. Will these mobile wireless devices evolve to allow a large part of the population to access the Internet in the near future? If so, will the installed infrastructure be able to support this high demand for data traffic? 3G phones and terminals that provide easy access to the Internet for reading e-mails are still very expensive, but prices are falling constantly and this scenario may change very rapidly. If the wireless technology evolution continues, it is quite possible that rural inhabitants will be surfing the Internet and sending e-mails and files on mobile devices in the near future.

Other wireless services may become a relevant part of access networks in rural areas. Some ISPs are using satellite data links in order to avoid using expensive wired data links to access the Internet backbone. Sometimes wireless satellite is the only option available for building their service networks at their location. To avoid the installation of wired last-mile access, some ISPs are using WiFi technologies instead of renting wired copper lines; others are contacting cable TV companies for renting their last-mile network. Provided the local regulatory framework permits this, many cable TV operators have become ISPs using cable modem access technology.

Considering all these recently changed rules, the concept of Universal Service should be reviewed and rebuilt to enhance service access from a wider perspective, including Internet and voice transmission. Universal Service funds could finance the extension of the backbones to reach unprofitable areas. This would lower national long-distance data link prices and promote the ISPs business by lowering end prices and allowing more people and companies to access their services.

On the other hand, many of the Universal Service funds haven't yet been used, or not completely. Government mechanisms for granting project funding are not always easy to implement, and the rapidly changing scenario usually serves to delay the whole process further. Part of this gap is being covered by private projects, small companies and entrepreneurs which install Internet[5] private access centers offering services at very reasonable prices. The offer includes Internet, local and long-distance services as well as other features like fax printing.

In Latin America and the Caribbean, there are also many public

[5] A 2005 ECLAC study estimates that in the LAC region approximately 100,000 private telecenters were established by small firms and that there are an additional 50,000 telecenters financed with public funds.

centers for accessing the Internet free of charge. These public access centers are usually financed by local governments and non-profit organizations or educational institutions. The real challenge for these public telecenters is not the initial installation, which is easily financed through several national or international agencies; the real problem lies in sustaining them. Many projects that were started in the late 1990s did not survive as personal computers became obsolete and payments to the ISP became a problem.

There are initiatives to solve this problem and revive these telecenters with technologies that can utilize old personal computers through centralized processing capacity and connectivity. Also, countries like Argentina and Brazil[6] have started to map and identify them in order to detect the areas with the lowest access levels.

THE GEOGRAPHIC GAP: WHEN DISTANCE MATTERS

The lack of national infrastructure and backbone connectivity at the national level results in data links which are very expensive for villages located far away from capital cities. Due to a scarcity of infrastructure capacity competence, these data links are usually offered by only one operator and charged not in local money but in US dollars. At national level, the Universal Access funds do not include subsidies for national backbone infrastructure installation. At the international level, there is no way to promote installation of undersea cables or satellites other than through private investment. But these investments don't always translate to profits and revenues, and the biggest markets are not located down in southern Latin America.

The lack of telecom infrastructure in developing countries means a lack of bandwidth available for accessing the Internet. As indicated in the ITU's World Telecom Indicators Database[7],

[6] The "Instituto Brasileño de Información en Ciencia y Tecnología" IBCT, has developed a map that contains per state in Brazil all the socioeconomic information and also the public access centers available in the region. The map can be found in http://inclusao.ibict.br/index.php?option=com_wrapper&Itemid=316

in 2004 almost 90 percent of the total worldwide bandwidth was available in developed countries of the world. The indicator "bits per inhabitants"[8] shows that someone living in North America or Europe has access to approximately 25 more bits of bandwidth than some one living in Latin America. The situation in Africa is even worse. In order to cope with high international interconnection costs, many ISPs in developing countries have developed interconnection points called NAPs or Network Access Points, where they share facilities and international connections in a cooperative scheme with a non-profit objective. This is the case with NAPs in Argentina, Colombia, Ecuador and Paraguay[9]. Other NAPs are commercially motivated, like the ones operating in Brazil and Chile. There are more than 20 NAPs and Internet exchange points in the Latin America and Caribbean Region.[10]

The fact that long-distance national and international links must be paid in a foreign currency - generally US dollars-, is a relevant issue. Local economies usually face crisis and inflation, and the price of foreign currencies may change quickly, generally increasing its value in relation to local currency. Meanwhile, local and small ISPs and telephone operators must charge for their services in local currency.

THE WAY FORWARD

Access to Internet and to telecommunication networks means a number of things. But it only becomes truly meaningful if it allows people to communicate and reach new sources of knowledge and learning. Companies and countries also benefit from Internet access if it helps them to enhance their productivity and profits and generate more jobs for people.

The extreme poverty arising from the region's deep economic asymmetry could be alleviated by an intelligent usage of Internet and ICTs as a way to access new sources of informati-

[7] Jagun, Abi – Economic barriers to development. International Institute for Susteinable Development - 2007

[8] Bits per inhabitant = Internacional bandwidth / Population

[9] Source: Roque Gagliano – eLAC 2007 Infrastructure working group coordinator - 2007

[10] Lacnic - http://www.lacnic.net/sp/naps/

on. There are some initiatives that focus on childhood education, like the One Laptop per Child[11] project. The governments of Argentina, Brazil and Uruguay are evaluating its implementation on a national basis, as a tool that would allow poor children to use a special portable computer for learning, reading and playing, at school and at home. The project is based on the development of a cheap connectivity device (the laptop): its price is low because the device is produced in huge quantities and does not require any marketing, sales or publicity costs. Governments would buy directly from the manufacturer and give them to the children.

Services that are affordable for the poorest populations must be really cheap, but if they are not profitable for companies they will not last long. Sustainability is the key for this kind of projects, which may comprise Internet access services and mobile telephony. Government initiatives may fail because of difficulties related to managing hardware maintenance budgets and a lack of operating skills.

Public and private alliances, in which each actor offers its best capacity, could be the answer for these problems. One good example is the Nokia Siemens[12] "Networks Village Connection", which links local entrepreneurs with regional operators that develop very low-price access networks for mobile telephony and other value-added services like Internet access. Universal Service funds could be used to subsidize the backbone data link prices, which would make these kinds of projects much more feasible from a sustainability point of view. On the international side, private initiatives could partner with regional financing agencies in order to install more infrastructures in the south of the American continent.

In light of the changes brought by the Internet during the last decade, there is a need to revise the concept of universal access funds and universal service. New regulatory frameworks must be developed to allow new business models for cheaper, sustainable services, including new-generation networks and techno-

[11] http://laptop.org/en/index.shtml

[12] www.nokia.com

logies. Governments have a major role in this issue, and can benefit from lessons learned in Europe, North America and Asia. An open dialog between regulation agencies of different regions must be promoted to exchange experiences.

The lessons learned in the region after the privatization processes of the 1990s have shown that it is not enough for the per-capita income index to be growing; it is also necessary to consider social inclusion and to respect the environment. Territorial balance, on national and international level, is essential for closing the gap between the poorest and the rest of the society.

Finally, all these services and achievements will only have a real meaning if they mesh smoothly and in a friendly manner with local culture and identity. Only then will all our people enjoy a better quality of life.

Supporting Young Social ICT-based Entrepreneurship in Rural Areas of Moldova

Veronica Cretu,
CBM Training Center Moldova, Kishinev, Member of
ICANN’s At Large Advisory Committee (ALAC)

HOPES

Policymakers in southeastern Europe and worldwide have long hoped that the Internet would bring enormous benefits to rural communities, many of which have suffered economic problems during recent years due to the migration of their citizens to cities and suburbs. Moldova’s rural communities have suffered greatly since the proclamation of Independence in 1989, when the shift from the planned economy to the market economy has simply “blocked” developments in rural areas. Unfortunately, this situation still prevails today. More than ever, young Moldovans from rural communities are leaving the country to look for better opportunities abroad.

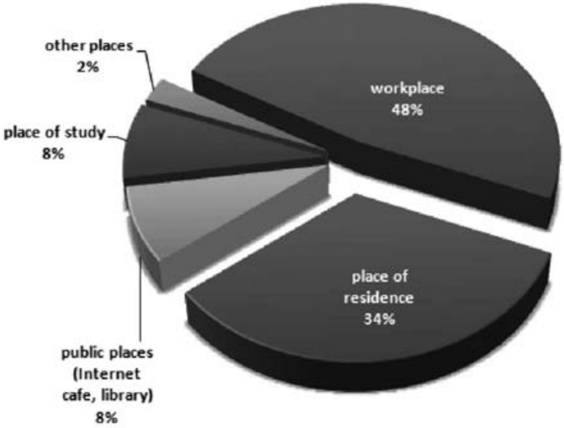
Policymakers have also hoped that technology which allows people to communicate easily and cheaply with anyone in the world, and to access all kinds of information services on the Web would enable people to remain in rural communities while building and maintaining new economic and social relationships. Moldovan rural leaders as well as policymakers and technology enthusiasts dreamed that the Internet’s capacity to make the physical location less meaningful would in one way or another make rural life more attractive.

REALITY

The current situation vividly reflects the fact that some differences in Internet adoption between rural areas and urban areas of Moldova are driven by patterns among low-income rural individuals. Living in a rural area in itself does not make much difference to whether one goes online or not. However, low-income people in rural communities of Moldova are less likely to use the Internet and/or any ICT devise than low-income people living in urban areas. In general, the current gap between rural Moldova and the country's urban and suburban areas can be explained by demographic factors such as the fact that rural residents as a group are older, less affluent, and have lower levels of educational attainment than those in urban and suburban areas. Nonetheless, recent statistics show that Internet penetration in rural Moldova has grown in recent years, though as mentioned above, the gap between rural and urban communities has remained constant over time.

STATISTICS

On the international level, Moldova has one of the lowest Internet development levels in Eastern Europe, and is ranked 109th worldwide in the U.N. Global E-readiness Survey of 2005. The number of Internet users in Moldova has tripled since 2002, and penetration currently stands at 10 percent of the population. Nearly half of users access the Internet from their place of work, 33.6 % use Internet at home, and 8.1% use public access points. Development of the Internet has been rapid, propelled by a National ICT strategy that is harmonized with the European Union as well as the large Diaspora population for



whom telecommunications and the Internet are important channels of communication, and, often, for the transfer of remittances from abroad.

Recent surveys by Internet providers show that above 80,000 persons are using the worldwide web in Moldova every month. That data is based on the summary results regarding the number of computers contacting the Internet during one month under survey. The Internet audience in Moldova is comprised of socially active urban residents, with Chisinau residents in the lead. In terms of age, social status and income levels, Internet users are mainly between the ages of 18 and 40, middle class, with average or above-average incomes.

BITS OF HISTORY ON INFRASTRUCTURE DEVELOPMENT

Since 1995, several initiatives have been launched in Moldova to establish additional satellite and fiber optic links within the country and internationally.

In October 1995, Moldova joined the Central and Eastern European Networking Association (CEENet), an organization of representatives of seven countries in the region devoted to the promotion of networking for academic and research purposes.

Prior to that, in October of 1993, the Moldovan Ministry of Informatics, Information and Communications had created the Republican Center of Informatics (RCI), as the main node of the national network and as the focal point for research and design in the field of information technologies.

Private organizations from the West have also been active in helping Moldova improve e-mail capability, network infrastructure and Internet connectivity. The Open Society Institute (OSI) has provided significant technical and financial support through its Regional Internet Program (OSI-RIP), which sponsored the first high-speed local Internet connection to universities in Moldova, connecting five campuses -- including the State University, the Technical University, and the Academy of Economical Studies -- to the State Academy of Sciences, the Soros Foundation Information Center, and RCI. In 1996, OSI-RIP provided funding to permit these organizations to connect to the Internet via satellite. In 1996-97, OSI-RIP funded Internet connectivity for universities, secondary schools, and non-governmental organizations by providing modems, e-mail and Internet services to those institutions accessing the satellite connection.

Another U.S.-based non-profit organization, ISAR (formerly known as the Institute on Soviet-American Relations) also provided assistance to improve e-mail capability, to train users, and provide technical support to Moldova. Recently joining the other organizations in Moldova is the International Research and Exchanges Board (IREX), a U.S.-based non-profit organization. Through a program called the U.S.-Eurasia Internet Access and Training Program (IATP), the organization is working to provide Internet access and training to thousands of users across the former Soviet Union. In 1996, IATP began a project to provide training and communications assistance in Moldova.

MAIN CHALLENGES seen by the Moldova IT Community policymakers regarding Internet connectivity in rural areas of Moldova:

- Poor telecommunications infrastructure. Most lines are analog and not digital.
- Expensive telephone rates and high cost of telephone lines.
- Insufficient number of telephone lines for residential use.
- High cost of computer equipment.
- Language difficulties - the preferred languages in science are still largely Russian and Romanian, not English.
- A dependence on international funding, which makes long-range planning difficult.

SUPPORTING YOUNG SOCIAL-ICT-BASED ENTREPRENEURSHIP IN RURAL AREAS OF MOLDOVA

As stated above, several initiatives have been launched in Moldova during recent years in an effort to provide people with the opportunity to gain access to the Internet and ICT and to develop ICT and Internet skills

Even if the National Agency for Regulation in Telecommunications and Informatics predicts that 2007 will see stronger growth in the Internet access market than in other sectors of telecommunications market, this will not significantly increase the use of ICT and Internet in the rural communities of Moldova. It won't do so because there are no digital lines in the villages yet, and because the cost of connection is still high, and because computer equipment is still expensive, and the vast majority of the population does not speak English...

Among the main problems seen at present is the lack of perceived need for using ICT and the Internet among members of the rural community.

The main driving force of any development is INTEREST, and especially ECONOMIC INTEREST. In this context, one of the solutions is to help the young people of the rural communities begin to use ICT and Internet for business purposes.

There are several initiatives that can be launched in the rural communities. One good example is a Rural Young Social Entrepreneurs' Competition that would reward the best business ideas with some support for starting-up small businesses, e.g. low interest rate credits for starting up businesses (Moldovan banks currently charge interest rates of 20% p.a. for business loans).

It is important to involve as many young people from the communities as possible in programs to build entrepreneurship, in programs related to the use of ICT and the Internet for business purposes, programs on marketing goods and services via the Internet, and many others … It is also crucial to stimulate the participation of young people who are currently studying at the universities and colleges in suburban and urban areas, as well as those who remain in the village after graduating from school.

Rural communities will start improving themselves as soon as there are some good examples, good practices in place, and people who start acting differently. As long as there are no good examples or leaders and initiators, the rural communities of Moldova will continue lagging behind as they have done until now…

Several strategies are currently being launched at the national level, including "E-Governance," a component in the national "E-Moldova" strategy. It is a great step forward for Moldova to be working towards an information society for all, but it is also

The case of my native village:

- A digital station was installed at the beginning of August 2007;
- There is an Internet café in the village;
- There are people who can afford to buy computer equipment; and in spite of all these, only teenagers are currently using the Internet for entertainment purposes. This, in turn, has contributed to the fact that adults perceive the Internet as "teenagers' games".
- More than half of the population of the village works abroad (around 2500 citizens) and communicate with their families back home by telephone only.
- None of the local business community representatives know how the Internet might be used for business purposes. It follows that they don't have a website to promote their goods or services;
- The village itself does not have a website, and in this context the local public administration does not see the need for having a village website.
- Many other similar examples can be provided.

important to take into account the local needs of the communities when priorities are defined.

It is also recommended that a multi-stakeholder and multidisciplinary approach be used for elaborating any strategy. The process should involve rural community representatives, including local youth, local businesses, the local public administration, and local schools.

CAPACITY BUILDING IN THE AREA OF INTERNET GOVERNANCE IN MOLDOVA

One recent example of the multi-stakeholder and multidisciplinary approach applied in Moldova, is the "Youth Leaders for Community Development through Internet Governance" pilot project, which is implemented by the "CMB" Training Center in partnership with DiploFoundation from Malta and with the financial support of the Global Knowledge Partnership, Malaysia. The priorities of this project include:

- An Internet governance capacity-building program for 16 Moldovan Young Leaders representing various stakeholders
- Establishing an Internet Governance Community of Practice (IGCoP) in Moldova
- Conducting research on the current situation and developments vis-à-vis Internet Governance and its impact on the Community Development in Moldova
- Dissemination of research results among different stakeholders both nationally and internationally, e.g. Internet Governance Forum, Rio, Brazil (November 2007) and GK3 (December 2007) in Kuala Lumpur, Malaysia
- Creating and distributing a methodological guidebook "Youth Leaders for Community Development through Internet Governance"

As of August 2007, the participants of this project have been working in four subgroups, analyzing issues related to Moldova's IT Infrastructure, E-commerce: E-payments/e-banking/e-money, Internet Users Community and Promoting Diversity and Multilingualism on the Internet, through the prism of Community Development. Each working group will identify recommendations for their research component and will develop new initiatives as a result of these recommendations. The final results of this project will be available in early February 2008.

REFLECTIONS

Moldova is far from being the only developing country in the world facing problems related to lack of IT Infrastructure, lack of skills and capacity-building, migration and "brain-drain" phenomena, digital divide, reliance on external donations and funding, and many more …

Each time we try to solve the problems we have here in Moldova, we do so because we want tomorrow to be a better day for the generations to come!

REFERENCES

1. Moldova Broadband Overview [online], April 17, 2007. Available from http://point-topic.com/content/operator Source/profiles2/moldova-broadband-overview.htm. [Accessed August 21, 2007]
2. Center for Democracy and Technology. “Bridging the Digital Divide: Internet Access in Central and Eastern Europe” Report, [online]. Available from http://www.cdt.org/international/ceeaccess/. [Accessed August 23, 2007]
3. Telecenter Knowledge Network. Moldova. ICT Overview. [online]. Available from http://community.telecentre.org/en-tc/wiki/moldova. [Accessed August 22, 2007]
4. International Telecommunication Unit. National Reporting on WSIS implementation: Moldova [online]. Available from http://www.itu.int/wisd/2007/wsis-implementation/reports/MDA.html . [Accessed August 18, 2007]
5. Ministry of Information Development of Moldova. E-readiness evaluation in the Republic of Moldova in 2006. [online]. Available from http://www.mdi.gov.md/news_dit_en/131168/. [Accessed August 22. 2007]
6. Global Knowledge Partnership. Young Social Entrepreneurs’ Competition.[online]. Available from http://www.globalknowledge.org/ysef07/index.cfm?&menuid=7 [Accessed on August 20. 2007]
7. “CMB” Training Center. “Youth Leaders for Community Development through Internet Governance” project. [online]. Available from http://www.cmb.md/en/15-current-projects.html.

Open, Universal, and Affordable Access to the Internet

Anriette Esterhuysen & Willie Currie
Association for Progressive Communications (APC)[1]

APC's approach to open access is people-oriented. We believe that access to information, content and tools is possible for all people. Bandwidth costs are lower now than ever before. The convergence of the Internet and telephony means that every person who has access to a mobile phone handset will have the means of connecting to the Internet. Yet, the vast majority of the world's people still do not have access.

INFRASTRUCTURE: LIMITED AVAILABILITY AND HIGH COSTS

Indicators from 2005 put Internet penetration in the developed world at 46 percent, and in the developing world at 5 percent, which translates to 750 million people connected in developed countries and just over 250,000 in developing countries, of which China counts for some 90 million.[2] Universal access to the Internet in the developing world is largely an issue of the limited availability of broadband networks and the high cost of access just to the physical layer of the Internet. The Tunis Agenda highlighted the importance of infrastructure and recognised the need for more financial resources to be invested in its development, but very few initiatives address the infrastructure gap systematically. Debates on whether infrastructure should be financed by public investment, or through a market-based approach continue; even though the solution is obviously a combination of both. Where governments have taken the lead, often a cumbersome bureaucracy emerges and action is repeatedly delayed.

[1] http://www.apc.org

[2] International Telecommunications Union, www.itu.int

The development and development finance sectors are still sceptical about the value of ICTs for development. In spite of a gradual integration of ICTs into development work, particularly in emergency relief, education and health, there are very few comprehensive approaches to addressing the infrastructure gap.

To keep access on the agenda globally, APC was actively involved in convincing the advisory group to the first Internet Governance Forum in 2006 to give it priority. We issued a revised and updated version of the APC Internet Rights Charter in 2006. 'Open access' is addressed in themes one and three[3]. But, in general we find that keeping access on the agenda is an uphill battle in the Internet governance sector.

Why is information and communications infrastructure so fundamental to development and social change? We believe the answer lies in the layered nature of the information and communications infrastructure. It has a physical layer (e.g. the Internet backbone, radio spectrum, computers), a protocol or logical layer (e.g. open standards to ensure all sectors of the Internet 'talk' to each other), and a content layer. We would argue that there is another layer as well, one which is made up of the social processes that are facilitated by the physical, logical and content layers. This layer can be termed the 'interactional' or 'relational' layer of ICT infrastructure, and has two primary components:[4]

First, it is where the narratives of globalisation, diversity, inclusion and exclusion are located. ICT expansion has positive and negative consequences. E-governance and the reliance on the Internet for access to information can increase exclusion and contribute to the formation of new elites. New applications and services emerge every day, but usually require access to credit cards and bank accounts. But, it is also in this layer where people, individually and in groups, appropriate the infrastructure and claim space for protest, self-expression, sharing and learning. It is a kind of macro-microcosm. Blogging, podcasting, social bookmarking, photo sharing, online campaigns, citizens' journalism are just some of the many different labels and tools.

[3] http://rights.apc.org/charter.shtml

[4] From the introduction to the APC Annual Report for 2006 by Anriette Esterhuysen http://www.apc.org/books/apc_ar2006_EN.pdf

The dynamic tension that results from the Internet becoming increasingly controlled, and commercialised on the one hand, and on the other hand people continually subverting this trend by either creating new tools and uses, or appropriating existing features on their own terms, constitutes a kind of multi-directional "tug of war" between developers, markets, individuals, communities and cultures of use.[5] What about people who do not have access? Does this process matter to them? Is the global communications infrastructure a public good to which all people should have access? APC believes the answer is 'yes'. As more and more social and cultural exchange takes place via the Internet, having access simply to stay in touch with family and friends is vitally important in a world context where there is so much displacement. People move constantly; to seek better opportunities, as the result of war, conflict, or environmental disaster. Communities living in poverty, who are socially, economically and politically disempowered, are particularly deserving of access to opportunities that will enable them to be heard, to use online services that can make things easier for them (e.g. sending or receiving remittances), and to participate in decisions that impact on their lives. This brings us to the second component of the interactional or relational layer of the infrastructure: the public participation, or social justice component. In a real sense it can facilitate transparency and accountability, participatory policy formulation and implementation, mobilisation, solidarity and protest. This does not happen because the Internet exists. It happens because people, communities, organisations use the Internet to organise and/or obtain the information they need to improve their lives.

THINKING SEQUENTIALLY

APC has always advocated an integrated approach to ICTs for social justice. We believe that community-building, organisation, content development, capacity building, learning, innovation and investment in tools and technologies should all happen concurrently.

[5] Firefox plug-ins to block online advertising is an interesting example of this, and the resulting legal tussles have long term implications for Internet policy, regulation and governance.

But in parts of the world where there is simply no infrastructure it is necessary to prioritise building it. The potential for people to appropriate ICTs to meet their own needs is greater than ever before. The convergence of mobile telephony and Internet network infrastructure neutralises the argument that more and cheaper mobile phones are all that the people in Africa need. Yes, there is a need for content and applications, but without infrastructure people won't be able to access them. And, with access to infrastructure, communities and citizens can create their own content, and more effectively demand the services and inclusion in public decision-making they are entitled to. But efforts to develop new infrastructure have to consider broader trends in Internet development and regulation if we are to ensure openness and a rights-based approach to access.

CONTESTED TERRAIN

Globalisation has been supported by communications infrastructure and has promoted its expansion. But the specific nature of the infrastructure and its resulting interaction with social processes means that there is an element of unpredictability in its evolution and its use. Appropriation by people, interest groups, and communities which are not part of the mainstream is as much part of this infrastructure as are well-heeled online shoppers. This inevitably leads to contestation between interest groups that try to restrict, control and predict access and use to increase profit, and those that want to ensure an open approach. Unless advocates for increased access remain mindful of this, market-led infrastructure development initiatives could come as package deals with limitations to openness 'hardwired' into them.

Public-interest oriented collaboration between business, the public sector and civil society in addressing the infrastructure gap cannot afford to ignore this. Most public-private partnership initiatives tend to avoid addressing openness head-on. Underlying the potential of open access are forces that work to restrict access. In some cases governments control access to content, but far more common are corporate attempts at enclosing the commons and shaping the Internet environment in ways that ultimately subvert openness. At the physical layer, there is a struggle around whether the public sector is distorting the workings of the free market; for example, by a municipality wanting to provide broadband access through open wireless networks as a public good to its citizens. At the logical layer there is the ongoing tussle between the purveyors of proprietary software and the Free and Open Source Software (FOSS) movement and its collaborative approaches to software development and usage; and advocates for open versus proprietary standards. At the content layer, there is the bitter struggle over intellectual property rights and the maximalist approach to copyright expansion; and the content and software industries to entrench an unbalanced monopoly by copyright and patent holders across the world – a global IPR regime that does not recognize the different needs of developing countries, or even recognize that there is a case for the fair use of content by consumers. In this contest, private corporate power is pitted against open public use of the Internet in what has been described as 'the battle over the institutional ecology of the digital environment'.[6] We have long known that open access to the Internet cannot be taken for granted – not by the billions of people without access, nor by the 1.5 billion people who do have access. At the same time as there is a struggle to connect people in the developing world, there is a struggle to keep the Internet open, part of the commons, a global public good for all.

WHAT ROLE SHOULD CIVIL SOCIETY PLAY IN THIS STRUGGLE?

The physical layer

Civil society needs to act as a countervailing force to private-sector initiatives which seek to prevent citizens from accessing the Internet on a universal and affordable basis. Civil society should seek to support non-market approaches to access such as are possible in municipal wireless networks and oppose private sector lobbying to make them illegal.

[6] Yochai Benkler: The Wealth of Networks: How Social Production Transforms Markets and Freedom Yale University Press 2006.

Civil society should oppose attempts currently under way by powerful private network operators in the USA to create a two-tier Internet. Civil society needs to champion Net neutrality as an important component of universal and equitable access to the Internet, and make sure that in the event of a two-tier Internet being legislated in one country, this model is not exported to the rest of the world by the global private sector.

With respect to reducing the costs of international Internet connectivity, civil society should put pressure on governments in developing countries to promote the building of fibre-optic submarine cables and Internet exchange points, the liberalisation of their international gateways and taking steps to ensure that there is an affordable national public broadband network[7] available on an open-access basis to business users and citizens. Civil society should, at the same time, put pressure on OECD countries to ensure a competitive international market for Internet connectivity in which the restrictive practice of forcing developing country Internet service providers to pay the full cost of an international circuit is outlawed.

The logical layer

Civil society should actively promote the use of Free and Open Source Software as a non-market approach to problems of affordability to the Internet through the high cost of acquiring the software needed to operate effectively in a networked environment. It may not mean much to a person who is online in an OECD country to spend $30 a year on anti-virus software but this is a lot of money in the developing world.

Civil society should advocate the internationalisation of ICANN in such a way that it can fulfil its mandate to manage critical Internet resources without fear or favour, and without being directed by government pressure or corporate interests in

[7] This does not deny a private sector role in such a network or the existence of competing network providers, only that where a competitive market does not provide an affordable public broadband network it is necessary for the government to step in. There is a growing public interest by business users, citizens and governments themselves to have open access to an affordable public broadband network for obvious reasons.

its decision-making processes. Citizen participation in decision-making regarding the governance of the Internet is limited, whether at national or international levels. Many developing country governments are authoritarian and can not be said to represent their citizens in international forums like the IGF, while some OECD countries serve as transmission belts for the interests of their major corporations. There is an urgent need for an Aarhus Convention on Access to Information, Participation in Decision-making and Access to Justice[8] regarding the institutional ecology of the Internet.

The content layer

Many Governments pay lip service to issues of freedom of expression and protection of citizens' privacy online, whether they are democratic or authoritarian. The so-called 'Global War on Terror' has become an oft-cited alibi for the abuse of human rights across many OECD and developing countries.

Civil society must take up the issue of freedom and privacy vigorously, wherever and whenever possible. Bloggers are incarcerated and physically abused in many countries. Civil society should strongly oppose allowing countries which do not fully comply with the Geneva Principles and the Tunis Declaration to host IGF meetings, and should not allow another travesty of human rights as was witnessed at the World Summit on the Information Society in Tunis in 2005.

Civil society should also oppose alliances between OECD governments and their private sectors to introduce and enforce maximalist rules for protecting intellectual property rights. The hypocrisy of the role some G8 governments play in exporting their maximalist IPR protection in free trade agreements, while leaving out the part about the fair use of content, is unconscionable.

The interactional / relational layer

Civil society should actively take advantage of the Internet to increase participation in policy and public decision-making. It

[8] http://www.unece.org/env/pp/

should use the Internet for dialogue, debate and protest, as inclusively as possible.

Civil society users (members of organisations, networks, or individuals), developers and hackers, artists and academics, should continue to create innovative tools and applications so that the Internet can be a people-oriented rather than a consumer-oriented space. Content and applications need to be shaped by people interacting with one another and collaborating not just to maintain the Internet as a global public good, but also to build egalitarian and inclusive societies.

Internet Governance: The Importance of Access

George Sadowsky,
Global Internet Project Initiative (GIPI), Washington

ACCESS: THE GOAL

Access is a fundamental sine qua non for the ability to use the Internet. To a potential Internet user who does not have the possibility of accessing the Internet, other characteristics of the Internet environment simply do not matter. The quality and attractiveness of access can be characterized by a few variables. Ideally, to reach the ultimate goal of an information society, access must be available, accessible, and affordable to as many people as possible in a given geographic region. Thus, in order to best approach the goals of having a global information society, we need to set a course that will provide the best available and accessible Internet at the lowest cost and price for as many people as possible. Such goals must be pursued at every local and national level in order that they be realized on a global scale. Access depends upon being able to use a service, supplied by a provider of Internet services that connects the user and possibly his/her computer to the global Internet. In general the service provider will offer such services either over a low speed of high speed copper local loop belonging to a telephone company, a TV cable provider, a wireless transmission provider, or a satellite communications provider. This linkage, whether wired or wireless, must be capable of being put in place for the service to work.

The Internet is, and has always been, a network of networks. The Internet has always been based upon the telecommunications infrastructure, whether it be copper local looks, copper or fiber trunks, undersea cable or satellite. The great majority of these physical transmission facilities are owned by the private sector, while in some countries they are owned by government.

Using this physical telecommunications infrastructure, the ISPs (Internet Service Providers) provide packet-switched Internet transmission services to customers in their region of service. Tier 1 ISPs provide far-reaching international services; smaller ISPs serve national, regional and local markets. The majority of ISPs are private businesses, while some ISPs are owned by educational consortia and others by government.

ISPs, especially privately owned ISPs, are the major driving force in the expansion of the Internet. Driven by a combination of motives such as competition, profit, market penetration and service to a client population, ISPs attempt to increase both their market penetration and the range of Internet related service choices that they can offer. In doing so, they are influenced by the policies of the relevant governmental unit with respect to their business behavior.

THE ROLE OF NATIONAL AND SUB-NATIONAL GOVERNMENT POLICY

Governments have the power to create an enabling policy space, consisting of laws, regulations, and unwritten codes of behavior that greatly affect the ability of their ISP community to help provide access for the greatest possible number of its citizens. Governments can empower their private sectors and citizens by:

- Providing training opportunities for technical professionals
- Encouraging ISP formation and growth, and creating a business environment conducive to entrepreneurial activity
- Implementing policies that encourage foreign investment in the sector in the country
- NGO activities in the country
- Aggressively exploring bilateral and multilateral assistance programs for activities that would help to strengthen the ICT sector and develop human capital
- Providing targeted governmental assistance for sector growth and support

It is worth noting the relative importance of private sector entrepreneurs and NGOs, as well as the lesser role of government in these activities

Governments can also disempower the Internet industry and disadvantage users by a variety of means, including the following.

- If there is a monopoly PTT majority-owned by the government, lack of competition will result in higher prices for Internet service.
- If regulatory processes are closed or non-transparent, ISPs will have a more difficult time entering the market and competing. Similarly, if ISPs have high entry barriers, strict licensing requirements, or high fees, competition will be imperfect
- If the PTT or other organization has a monopoly on the Internet gateway, it can charge monopoly prices for the rest of the ISP industry
- If IXPs (Internet Exchange Points) are prohibited or restricted, transport costs between ISPs in the country will be higher because of the need to transit outside the country.
- Difficulties in starting a business, or long delays in doing so, will weaken competition in the Internet services market
- High prices for computers and networking equipment can be the result of prohibitive import duties, high local tax rates, or slow, inefficient or corrupt customs clearance
- If existing networks are closed to competitors, or if they are open but with a non-level playing field, then the market is biased with consequent higher prices
- If ISPs are liable for ensuring that the content they store and transmit reflects legal behavior, this will discourage entries into the ISP industry and lessen potential competition
- E-commerce legislation that is non-transparent or arbitrary will slow the growth of e-commerce
- Unpredictable licensing requirements will discourage entry into an industry
- Lack of guarantees of information confidentiality and privacy will substantially discourage people, organizations and businesses to use the Internet for any type of confidential data. Insecure e-business transactions will drive down demand for the Internet
- Information services subject to content restrictions or censorship may be difficult to provide and may not be trusted as authoritative

- If security tools such as encryption are forbidden, confidentiality of information becomes possibly suspect, dampening, inter alia, the growth and level of e-commerce activity.
- If there is any tradition of laws or regulations not published or not available, there will be a degree of uncertainty in engaging in specific actions
- If e-government developments discourage or limit active public participation?
- If intellectual property rights are not respected, both the domestic software industry and international software will be reluctant to make their products available locally for fear of
- If digital contracts and transactions are not formalized in law, they may not form a sufficient basis upon which to grow an e-commerce industry

In all of the above cases, it is government, at the national and sub-national level, that has the power to make and change policy that directly and indirectly either helps or hurts users who want to have access to the Internet. National and sub-national governments have a very large effect upon whether affordable and available access will become available to its inhabitants.

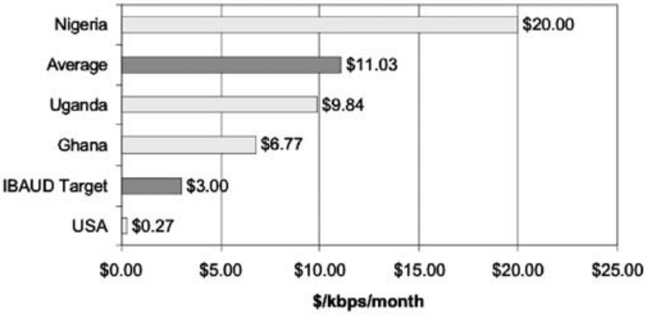
EXAMPLE: AFRICAN HIGHER EDUCATION

Education is a particularly important area in which access is critical. The development of human capacity in young people, and especially their preparation for contributing to and benefiting from an information society, is one of the fundamental skill sets that a country must inculcate in its students. In addition to obtaining a potentially inferior education, graduates of an education system who do not have exposure to and productive use of the Internet are not ready to assume their position in an information society.

This is particularly true of university education. A nation that does not have a competent university system cannot educate and retain the professional class so necessary to build emerging economies into self-sufficient economic units. Particularly at the university level, where sources of knowledge are international and studies increasingly depend upon those sources, lack of effective access to the Internet and its global contents can pose a serious restriction upon the quality of that education. Accessible and affordable access is essential to provide a modern university education.

Africa has long been the exception with respect to the ability of the Internet to penetrate and support a wide range of activities including business as well as research and education. Distance, absence of competitive international and national telecoms markets, and inadequate financial resources have combined to disadvantage the continent including the research and education activities that already exist, and that could take place in the presence of available and affordable connectivity. Such bandwidth is considered essential to education and research in developed countries.

A number of recently completed studies have provided a reasonably up-to-date picture of research and educational networking in Africa. Funded by IDRC in Canada, the PAREN study (PAREN - Promoting African Research and Education Networking) provides one of the most complete pictures of existing regional national academic networks in Africa and in other developing regions. It concludes that, in Africa, Internet connectivity costs can be up to 100 times higher than those in developed countries. As a result, the total bandwidth access of the average African university is roughly equal to the bandwidth of a single home user (ADSL or cable) in North America or Europe. The graph below displays the price disparities:



Sample size of 26 universities

This kind of price disparity indicates how debilitating it must be to have access, but access that is essentially unaffordable to those institutions which need it most. Such a situation demands international attention and a plan for remediation.

INTERNET ADMINISTRATION/GOVERNANCE AND THE USER

Given the importance of access for development and capacity building, I believe that the best way in which to evaluate the value of any potential change in Internet administration or Internet governance is to predict its effect on the average user. For it is the users of the Internet who will be able to exploit it (in the best sense of the word) and in doing so will contribute to their own country's development as well as their own.

The average user cares a great deal about having affordable access to the Internet. That means that the ISP community needs to be able to offer that accessible Internet, as well as IP addresses to their clientele. The preceding section details some of the many things that national and local governments can do to help ISPs achieve that goal.

Unlike IP addresses, however, typically users does not need to own a domain name in order to do their work. When a domain name is needed, it should always be possible to obtain a domain name of choice from their country code top level domain (ccTLD), whose operation is sanctioned and often controlled by their national government. Generic top level domains (GTLDs) may be interesting, but the GTLD space is unnecessary to meet their domain name needs.

CONCLUSIONS

Three conclusions strike me as paramount. First, for assisting a development-oriented Internet in which the empowerment of users is of the highest priority: (1) access to an available and affordable Internet is the highest priority; (2) private sector empowerment is the engine of growth of the Internet sine qua non; and (3) national and sub-national government policies are by far the most important determinants of he extent to which the private sector is empowered. If the desirability of changes in "governance structure" are measured by their impact on the average user, then the great majority of such issues should be focused upon the national and sub-national levels of government.

Second, not having access to an Internet that is available and affordable works strongly against the ability of the education sector, especially higher education, which is the vehicle for capacity building and in particular, for developing the professional class and retaining it that is so essential for eventually achieving self-sufficiency.

Third, the administrative functions that ICANN exercises have little if anything to do with improving the ability of users to access the Internet and to use it profitably. If anything, ICANN has contributed in a number of ways to the security and stability of the Internet, to the benefit of all users.

Fourth, there do remain significant Internet governance issues at the international level. Cybercrime, spam, and international connectivity costs appear to be at the top of the list. Ameliorating problems in these areas does have some payoff for the average user. The Internet Governance Forum would be wise to concentrate upon those issues that are truly capable of making some progress at the international level, and assisting governments to understand and adopt policies that are applicable at the national level

Chapter 2

Openness

Openness as a Prerequisite for Freedom of the Media

Christian Möller,
Office of the OSCE Representative of the Free Media, Vienna[1]

Openness is – besides security, access and diversity – one of the four main topics of the Internet Governance Forum (IGF). It is the generic term for issues as diverse as open standards or access to content.

Openness also means freedom of expression and freedom of the media. Paragraph 42 of the Tunis Agenda explicitly reaffirms the "commitment to the freedom to seek, receive, impart and use information, in particular, for the creation, accumulation and dissemination of knowledge."

The OSCE Representative on Freedom of the Media has been implementing programmes to raise awareness and to further guarantee media freedom online for years. The Internet is an additional – and in some regions the only – source of media pluralism. The OSCE Representative advocates using the Internet's potential to preserve an open environment instead of restricting the free flow of information by excessive legislation or technical measures.

In addition to three international Amsterdam Internet Conferences from 2002 to 2005, the Office has also published a number of publications on media freedom on the Internet. These include the 'Media Freedom Internet Cookbook' and the recent report 'Governing the Internet – Freedom and Regulation in the OSCE Region'. This report looks at implications of Internet regulation on media freedom in the OSCE region and offers case studies from different parts of the region on how governments, civil society and the telecommunications industry can co-operate in their approaches to Internet Governance.

[1] This article solely reflects the author's personal opinion.

BUILT-IN OPENNESS

As 'code is law' – something of which we have all been aware since Lawrence Lessig's book – the architecture of the Internet is not 'open' per se; it can be created and shaped in any way developers, but also policymakers around the world, would like it to be. It is not enough to demand 'openness' of Internet resources – the guarantee of openness should be built into both Internet regulation as well as technical standards of the Internet. But for this, there is the need for all stakeholders to communicate in an open atmosphere and first to build understanding of other parties' interests.

Policymakers often lack the expertise to deal with the more complex technical side of the Internet. On the other hand, developers have only recently been showing increased interest in the societal impacts of the standards they set.

Currently, it is emerging that Internet regulation by nation states – although often imposed with the best intentions – tends to restrict the free flow of information and open access to content on the Internet. At the same time, technical standards tend to limit openness, including those with legitimate goals like Digital Rights Management (DRM) or proprietary standards.

All actors need to be involved in this discourse and 'openness' should be acknowledged as one of the integral attributes of the Internet that needs to be protected on all levels.

INTERNET GOVERNANCE AND FREEDOM OF EXPRESSION

Increasing attention has been paid to the question of whether the Internet, which has developed outside a classic intergovernmental framework, needs governance at all, and, if so, in what form. Do we need a formal governance structure or will informal means of governance – namely behavioural norms established by the Internet community or by the software code itself – suffice? But Internet governance is not only about technical standards or the Domain Name System. It also has commercial, cultural and social implications, concerning issues like the free flow of information, the fight against intolerance, and freedom of the online media.

Governments do play an important role in Internet governance. Although “governance” is not synonymous with “government”, this does not mean that governments should be excluded. Governments have a function that cannot be filled by other actors, for example in guaranteeing an independent judiciary, protecting human rights and establishing antitrust measures.

On the other hand, there are many fields in which the State should leave governance of the Internet to civil society or the private sector, for example when it comes to the technical functioning, administration, or organization of networks.

‘Openness’ is not only part of the discussions at IGF. The discourse itself also reflects a great deal of the history of the Internet. In the past, electronic communication media – like telephone numbers and radio and television frequencies – were subject to strict regulation by international organizations like the ITU (International Telecommunication Union) and national authorities. By contrast, the Internet started to develop in an academic and then increasingly commercial environment and to a large extent without national interference.

Whereas standards for previous means of communication were set by intergovernmental organizations, for the Internet this is often done by the online community or expert bodies with an open membership. The informal Internet Engineering Task Force (IETF), informal papers – so called Requests for Comments (RFC) – or consensus-building based on the principle of “rough consensus, running code” are all factors that helped to develop uniform standards and the technical advance of the Internet.

In the course of time some of these informal processes coagulated into more institutionalized units. For example, after initial one-man shows such as Jon Postel’s Internet Assigned Numbers Authority (IANA) at the university of South California, ICANN, the Internet Corporation for Assigned Names and Numbers, is today in charge of administering the Domain Name System (DNS).

The success of the Internet and its services like e-mail and the WWW demonstrate the feasibility of governing a global resource in such an open manner. These mechanisms might serve as an example for developing new instruments of policy development in the context of the UN's Internet Governance Forum (IGF), also beyond technical aspects.

OPENNESS OF THE INTERNET GOVERNANCE FORUM

At the price – or the benefit – of not being able to adopt binding decisions, the IGF has managed to be very inclusive. And again, 'openness' is not just a topic for the IGF but also applies to its very composition. The IGF is open to all stakeholders, but unlike other United Nations bodies it cannot agree on final documents or even make recommendations, although some parties increasingly seem to be demanding such documents.

The outcome of this process still remains to be seen, but the form and organization of the IGF definitely represents a new model of policymaking at the international level. Another new instrument formed at the 2006 IGF in Athens is that of 'Dynamic Coalitions'. 'Dynamic Coalitions' are a new form of collaboration between all stakeholders, including governments, civil society, industry and academia. These are endorsed by the IGF but do not constitute formal bodies or institutions. They serve as a platform for state and non-state actors to share their views and contribute to the IGF process.[2]

Similar to the IGF as a whole, these coalitions are open and inclusive, but cannot make any binding decisions. And, in fact, due to their openness any decision would lack democratic legitimacy. On the other hand, maybe there is no need for globally institutionalized Internet governance structures. Maybe more issues could be tackled in a more pragmatic way, by developing minimum standards and agreeing on a rough consensus, for example.

OPENNESS IN INTERNET GOVERNANCE

Applying principles of open discussion and informal proposals – similar to Requests for Comments drafted by expert groups, possibly by different Dynamic Coalitions – may turn out to be

[2] More information on the FOEonline coalition is available at http://foeonline.wordpress.com.

an inclusive approach which really brings together the expertise of all stakeholders under the umbrella of good governance.

Where there is a pressing problem about how to govern the Internet that needs to be addressed on a global scale, proposals for regulation or standards could be provided in a non-binding way. Once adequate solutions are offered, international organizations and governments could adopt them and implement them in a democratically legitimated way.

It would even be possible to implement only those regulation modules that are required. New international treaties could make different parts optional, which parties to the treaty could combine as needed.

This is not a totally new way of reaching international agreement. The Council of Europe's Cybercrime Convention, for example, was drafted in two modules. As rights to freedom of expression differ between countries, it soon became obvious that not all parties could subscribe to a comprehensive content regulatory framework and as a result the convention was split. The actual Cybercrime Convention combines more technical approaches, whereas the Additional Protocol against Racism was ratified only by those countries in which this approach did not contradict freedom of expression regulations.

Even competing strategies by different IGF coalitions could be seen as a marketplace of governance approaches, from which any actor could choose the model which best suits its policy aims. At the same time, this process would guarantee that the developed mechanisms would include both the involvement of experts and different stakeholders as well as democratic legitimation by official decision-making bodies.

These kinds of open modules with open subscription to international agreements, developed by all stakeholders and democratically legitimized by governments, might serve as one possible future role of the IGF and as a new way to design the good governance of the Internet in order to retain the 'openness' of its infrastructure.

Openness, Harmony and Cacophony

Ronald Koven,
European Representative, World Press Freedom Committee (WPFC), Paris

The notion of “openness” for the Information Society seems simple enough. And it is, in principle. In practice is where the complications arise. This shouldn't surprise us. Even the most democratic societies have more problems with openness than they care to admit.

In Sweden, where pioneer freedom of information arrangements date from the 18th Century, people like one former public ombudsman say that the system only works because, in practice, newspaper editors accept unwritten limits on the information they may publish.

In Britain, the well-known “D-Notice” (“D” for ”defense”) system explicitly informs editors of national security information that they voluntarily agree not to publish – even before knowing what the notices will say (presumably on the threat that violations would lead to legislation).

In the United States, whose much vaunted First Amendment to the Constitution is generally seen as the gold standard (or by some in Europe as a major obstacle to curbing “hate speech” internationally), the idea that its plain language was simply what was meant to be enforced was not recognized by the US Supreme Court until it ruled, by a close vote of 5-4 in a 1931 landmark case. In other words, the First Amendment went unenforced from its enactment in 1789 until 1931. In 1972, the distinguished Supreme Court Justice Hugo Black felt compelled to say that the amendment's stipulation that “'Congress shall make no law … abridging the freedom of speech, or of the press' is composed of plain words, easily understood.”

Established democracies continue to navigate the shoals between Islamism and traditional freedom of expression with difficulty. On Sept. 11, 2007, for example, Terry Davis, Secretary General of the Council of Europe, said that a ban by the mayor of Brussels of a march under the banner "Against the Islamisation of Europe" was justifiable because freedom of assembly and free speech rights under the European Convention on Human Rights “should not be regarded as a license to offend.” This seemed to fly in the face of the of European Court of Human Rights key ruling in the Handyside case of 1976 that free speech applies “also to those [ideas] that offend, shock or disturb the State or any sector of the population.” Nevertheless, Secretary General Davis went on to say, “It is very important to remember that the freedom of assembly and expression can be restricted to protect the rights and freedoms of others, including the freedom of thought, conscience and religion. This applies to everyone in Europe including the millions of Europeans of Islamic faith, who were the main target of today's shameful display of bigotry and intolerance.”

So it is understandable that the plain language of Article 19 of the Universal Declaration of Human Rights continues to encounter resistance, both in authoritarian countries and in established democracies - understandable is not, of course, the same as acceptable, effective or desirable.

Article 19 stipulates: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.” It was an arduously won major victory to get the final texts of the World Summits of the Information Society in Geneva and Tunis to recognize Article 19 as a touchstone for future developments.

China in particular has now turned back to its Confucian roots for its strong suggestions that international Internet information policy should be designed to protect society's “harmoniousness.” That would be acceptable if one agreed that democratic societies are modelled on philharmonic orchestras. But free debate cannot dictate when or whether the oboes or cymbals may come into the discussions. China's vision of social harmony would quickly turn into social and political conformity. Political life in a democracy is messy, not “harmonious.” Cacophony has its merits. The democratic faith is that useful truths eventually emerge from such cacophony.

When we start positing that the press has roles or obligations to promote social cohesion, social solidarity, poverty reduction, etc., we might wonder where does that requirement stop? Should journalists be expected to earn degrees in social work?

It is a paradox that the smooth functioning of openness – or "transparency," to use a more fashionable label – requires that some things be closed to public scrutiny. It is an apparent contradiction that the enemies of openness do not fail to exploit. The issues include the protection of journalists' sources and the right to publish comments anonymously. Public scrutiny is limited in those cases for the express purpose of broadening the content of public discourse. And it is the authoritarians who challenge such rights of confidentiality – to choke off debate.

There are moments in public life when confidentiality is needed. Woodrow Wilson's slogan, “Open agreements, openly arrived at,” turned out to be a Utopian dream. It hobbles negotiating processes involving mutual concessions that may only be possible in conditions of confidentiality. That is very different in kind and purpose from the silence that advocates of social harmony would impose when they argue that – more than ever in a world where information and commentaries travel at the speed of the Internet – enforcing secrecy is essential for social peace.

Yet, openness on issues that confront societies may be the only way to move forward. Speaking this spring at a World Press Freedom Committee luncheon in Washington DC, Joergen Ejboel, the publisher of Jyllands-Posten, the Danish newspaper which printed the Mohammed cartoons that led to worldwide demonstrations, was asked what lessons he drew from the episode.

“I think that time will show,” he said, “that the cartoons actually have contributed to a much better dialogue, at least in Scandinavia, because all of a sudden a lot of subjects are debateable. … [U]ntil the cartoon crisis, a lot of subjects … were not even mentionable because a lot of people found that not to say anything and not to do anything would be the safest position."

The demands of extremist Islamists amounted to a call for systematic self-censorship. Despite all its deplorable consequences, the cartoon crisis had a distinct silver lining. As Ejboel noted, it put major issues on the table, opening up salutary debates about how Western societies can adjust to the presence of substantial Moslem minorities while preserving democratic values. Such questions are so sensitive and complex that the first reflex of those in power or in positions of influence may indeed be to avoid public discussion. Ultimately, however, the questions must be openly confronted.

The free debate that is needed if open societies are to remain open is the same both offline and online. Shying away from sensitive issues by formally or informally banning their discussion means that they will burst into the open anyway. Suppressing them increases the probability that their eventual expression will be irrational and violent. And if we suppress views that we deem to be repugnant, how can we measure the extent to which they are held, and, more importantly, how can we counter them in free and open debate?

The fundamental lesson of the cartoon crisis may be that dedication to openness – from the start, as issues arise – is a vital precondition for the establishment of ultimately harmonious societies, where we do not fear the open cacophony of the oboes and the cymbals clashing disharmoniously. Accepting this would be an updated, post-modern recognition of the libertarian view of the need for openness.

The Evolution of Rules for the Internet as a Model for Internet Governance

Peng Hwa Ang,
Nanyang Technology University, Director School of Communications, Singapore

Often, when I tell people that I am working in the area of Internet governance, a common response is: the Internet works best without rules. That, politely speaking, is Internet Scholarship 1.0. One way to imagine how Internet governance might be necessary (or not) for the Internet is to imagine cyberspace as a parallel universe. A few small groups of earthlings land on a lush planet where life as we know it can flourish. The groups can choose to live together or they can live apart. Assuming that it is possible to live peaceably on that planet, what would compel the groups to live together, and thereby subject themselves to some form of government, however loose that form might be? Or, in other words, would there be anything to make those groups come together, sacrifice some liberties, and form some type of government? Well, when the Internet emerged, users felt like aliens in a new place where they could do whatever they want. Governments would have a hard time tracking them down; law enforcement would be difficult if not impossible. It almost seemed as if some version of the US First Amendment on freedom of expression was hardwired into the Internet. Or so it seemed. Looking back now at that utopian view, we know that the internet was never free of regulation and that users were in fact often ready to give up some liberties in exchange for government. Rights to intellectual property, privacy and reputation would only be most effectively dealt with by governments. Self-help, social etiquette and technology could only go so far. Governments have a role to play.

In developing countries, the experience of users on the Internet is not very different from our earthlings on an alien planet. For users and governments of developing countries, the Internet is a new medium for which, there are few readily applicable rules. There is however, a difference compared with the mid-1990s when the Internet exploded into public use in the developed world. Today, there are examples and lessons to learn from.

It is now possible to look back and see that rules Internet regulation underwent three phases of evolution. The first phase was the applying offline rules to the online world. It is the easiest way of quickly regulating cyberspace because offline rules are well understood, at least in their country or origin. This is important because it delineates roles, rights and responsibilities quickly.

Applying offline rules to the online world also comes naturally to the lawyers and judges who have to use the rules; they have been socialised to think that similar facts in similar contexts should be decided in similar ways; the mere appearance of facts or contexts in an online regime should not result in a different result. No one should gain nor lose rights by merely going online.

But having said that, one quickly realizes that the online world is different in important ways from the offline world. Not everything that works in the offline world can be blithely applied to the online world; some things just will not work. And so here is the second evolution of Internet rules.

My favourite example is the issue of liability for third-party content. This somewhat technical term applies to situations where a third party interposes himself between the originator and receiver of information. So for example, if I have a bulletin board, a reader of the board is a second party; anyone who posts messages on my board is a third party. A reviewer of a book on Amazon is a third-party content provider; so is the reviewer of hotels for a hotel booking site.

In the offline world, if I am the owner of the board, I will be liable for any content that appears on it. The rationale is quite simple: I have control over the access of the board. And if I can control access, I can deny access and so I should be liable.

Online, however, the world is different. So the need arises to adapt the offline rules to the online world – the first evolution of online regulations.

The value of online bulletin boards is that they are accessible to anyone. Any third party can provide content. So a hotel booking site is much more valuable if there are guests who can comment on their experience at the particular hotel. This, as the world is discovering, is the social networking power of the Internet manifested as Web 2.0 through sites such as MySpace and FaceBook. The more users there are contributing content, the more valuable the site.

It would be an unbearable burden to impose on the website owner the duty to scan the site for objectionable or even illegal posts. Websites are 24/7 operations; their owners, as long as they are human, need to take fairly lengthy breaks.

Here is where governments have recognized the need to immunize the website owner from liability for posts by third parties. In all the legal regimes I have seen, a law has to be passed for such immunity. (This is a case where a law is needed to remove the penalties of another law; regulation does not always have to be punitive.)

The U.S. and Singapore governments were the first to blaze a trail in this area. In the case of the USA, immunity is total for civil liabilities.[1] In the case of Singapore, immunity is total for both civil and criminal liabilities, but restricted to the "network service provider".[2]

There is, however, still a problem with this. And this is the problem of first-mover disadvantage. There is a genuine dilemma for which there is no easy solution. On the one hand, because the online world is so new to lawmakers and also because technology changes so quickly, lawmakers have actually been reasonably cautious about regulating the Internet. But on the other hand, there are also instances where, quite clearly, regulations will help the Internet. Some have called this positive regulation – rules that help rather than punish users. Presumably, the noti-

[1] S.230 Communications Decency Act, 1996

[2] S.10 Electronic Transactions Act, Chapter 88, Singapore Statutes.

on is that it is all right to pass "positive" rules but not to pass "negative" rules. Such a distinction is unhelpful. Taken to its logical conclusion, the only acceptable colour of traffic lights would be green. In any case, the state of Utah in the USA shows that even legislation intended to facilitate Internet use is susceptible to first-mover disadvantage. In that case, Utah passed the world's first digital signature law.[3] But because the law was so married to a specific technology, it became obsolete when new digital signature technologies emerged. And so comes the third evolution. Probably the best answer to the tensions caused by introducing new rules for the Internet lies in seeking wider consultation, from business and the user community. Or as it is increasingly called, to be 'inclusive' and include all stakeholders such as business and civil society. John Perry Barlow's Declaration of the Independence of Cyberspace was overstated: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[4] He has a partial truth in that governments alone are not sovereign in cyberspace. Nor should they try to be. In the case of the issue of liability of third-party content, wider consultation has refined the rule so that best practice is now to give immunity from liability if the owner of the site acts reasonably after notice is given. This rule was developed after observing that total immunity of the site or board owners means that they often sit on their hands, even when ethics and fair play would say that the objectionable content should be removed. In a number of cases, defamatory statements have been allowed to remain on the site, further injuring those affected. The rule has been refined on a global basis: the Singapore version of 1996 was refined in India, Bermuda, and Vanuatu[5]. Now, it is the Singapore version that needs refining.

[3] Utah Digital Signature Act, 1995.

[4] John Perry Barlow, 1996, A Declaration of the Independence of Cyberspace. Speech at the World Economic Forum, Davos, Switzerland. http://homes.eff.org/~barlow/Declaration-Final.html. Accessed August 30, 2007.

[5] Ang, Peng Hwa. (2005). Ordering Chaos. Thomson: Singapore .

In practice, this means that national governments should ideally consider how offline laws have to be adapted to the online regime – going straight to Evolution 2 first rather than attempting to shoehorn offline rules into the online world. All countries have their own particular laws; it is essential that thought be given to their applicability to the online world.

But such thoughts are not enough. Governments have to learn from international best practice. It is clear that best practice in regulation evolves out of wider consultation. And so business, civil society and other stakeholders should be consulted.

Because developing countries have pioneers, models and best practice to look to, I am optimistic that where governance is an obstacle to development, it can be overcome. The process, however, cannot be rushed. Any meaningful development takes time.

Internet Governance Capacity Building in Latin America: Examination of an Effective Model

Seiiti Arata Jr.[1],
Diplo Foundation, Sao Paulo

INTRODUCTION

This contribution is a personal view of the author, who shares perspectives obtained at DiploFoundation in Internet Governance Capacity Building Programs. The reflections also take into consideration his experience as a former student in distance-learning initiatives for about ten years in different institutions including MIT, Clifford Chance Academy, BarnesAndNoble.com, The Berkman Center for Internet and Society, Universidade de São Paulo, University of Ottawa Law School, WIPO, among many others.

THE IMPORTANCE OF CAPACITY BUILDING TAILORED SPECIFICALLY FOR LATIN AMERICA

Capacity building has been considered a cross-cutting theme in the Internet Governance Forum process. Education is a key element to active involvement, yielding a multiplier effect as participants in capacity-building programs go on to share the knowledge acquired with other members of their community later on. However, the scarcity of Spanish- and Portuguese-language education programs has undermined Latin American participation in international IG processes.

[1] Lawyer and public policy advisor. Member of the Internet Governance Forum Secretariat. Founding member of the Global Internet Governance Academic Network – Giganet. Tutor, Internet Governance Capacity Building Programme, DiploFoundation. Valuable insights were received on earlier drafts from Ginger Paque and Hannah Slavik in the preparation of an article from which this contribution is inspired.

The language barrier, particularly in Latin America, inhibits participation in and even observation of international processes. To leverage Latin American participation, it is important to train activists and negotiators who can help in the process of producing materials in their national languages. The large Francophone presence in the international processes has advanced the translations of documents, lists and events into French, but this rarely occurs with Spanish and even less in Portuguese, which is not an official UN language. It is necessary to emphasize the inclusion of current regional and international activities in the development of new materials specifically designed to insert an active Latin American presence for progress.

Dealing with IG issues requires multidisciplinary knowledge as well as a unique blend of diplomatic and technical skills. These skills are acquired through access to an exchange of practical experiences and information resources, along with the availability of proper educational and technical training. Yet, countries with limited human and financial resources often lack these skilled negotiators. As the global IG debate continues, it becomes even more important to diminish the capacity gap among stakeholders to reach full multi-stakeholderism.

The best way to respond to this is to train each stakeholder group that is to be inserted into IG policy deliberations in a way that enhances regional knowledge sharing to maximize the impact of developing countries in formulating appropriate national and regional policies, as well as participating in international policy developments and processes. Given the importance of cultural and regional interpretations as well as distortions inherent in the translation process, this cannot be done effectively without including local language tools.

Both global and regional capacity-building initiatives are necessary to deal with this scenario. Such initiatives should strengthen the understanding and negotiating capacity of representatives from developing countries. A community of qualified and respected regional researchers shall be created and multiplied, reaching a critical mass from which regional initiatives can emerge.

ONLINE TRAINING SOLUTIONS

Considering that many of the leading institutions providing education and research on Internet governance are currently based in the North, one possible solution to the gap in capacity building for Latin America is the use of online training, with a strong focus on collaborative learning and network-building. Such an approach has been used by DiploFoundation in its Internet Governance Capacity Building Programmes[2]. These programmes involve the delivery of online courses in Internet Governance to regionally-based groups, followed by individual and group research projects aimed at increasing expertise and skills. The programmes have been delivered for the last three years in the English language, while in 2007 Diplo experimented with offering a bilingual Spanish/English regional group based in Latin America.

The remainder of this paper describes several aspects of the IG Capacity Building Programmes considered particularly important from the perspective of the author, who has been both a participant in the programme, and more recently, a tutor. The paper focuses on the online collaboration aspects, including the creation of a bottom-up approach to knowledge building, and motivation of programme participants.

ONLINE COLLABORATION

Ideally, online learning should take advantage of the potential for collaboration offered by ICT tools, leaning towards a social approach to learning. Accordingly, course participants not only learn individually from course materials but also dedicate additional time to interacting with other students and participating in group activities. In fact, students learn faster and more effectively in this way as they are not simply passive receivers of knowledge, but are requested to articulate ideas and express themselves among their peers under tutor coordination.

Diversity. A multi-stakeholder approach is built into the training activities, facilitating the involvement of government officials, civil society representatives, business people, journalists, aca-

[2] http://www.diplomacy.edu/ig

demics, and other actors in modern political international affairs. Under a multi-stakeholder approach, participants are exposed to various professional cultures, approaches, and views on important policy issues. This enriches their training experience and facilitates future communication between the various stakeholders.

Basic texts as starting points. Course discussions start from basic texts prepared by the course team. Together, learners can go well beyond the basic materials provided, by sharing their own knowledge. Especially when the students already have considerable expertise in specific fields which touch Internet governance (such as computer science, political science or international relations, to name just a few), as a group they are able to construct knowledge based on their experience and interaction.

Bottom-up and top-down approaches. The top-down approach is defined in practice by research and peer review by the course development team, updating the basic texts and creating new readings.

These basic texts are available online and are the basis for discussion in forum threads and chat sessions. Most importantly, class interaction takes place right in the basic texts, via a special hypertext tool specially developed to allow the course participants to highlight words or phrases and add comments. Other participants can read these comments and reply back. The bottom-up knowledge building process is constructed as the students interact with each other here.

Modularization. The division of the course syllabus into different disciplines made up of short texts is central to the modularization of the basic content. The hypertext comments added by the students can be considered the smaller units of modularization, a concept drawn up by Yochai Benkler, who has an interesting approach to understanding the mechanics of online collaboration. Modularization, for Benkler, is breaking the project up into little pieces, “each of which could be performed by an individual in a short amount of time”, so that even when his motivation to contribute is small, he will be able to make a minimal effort and still contribute.

The hypertext tool, the modular element upon which discussion is based, is very easy to use and is initiated on top of the basic text. Hypertext entries can be added to specific parts of the basic text or in a thread following the comments made by other participants, creating a vibrant dialogue. Hypertext, as well as the forum discussion, enables the incremental and asynchronous production Benkler refers to and pools “the efforts of different people, with different capabilities, who are available at different times”.

Granularization. The second item recommended by Benkler is granularity of the modules. Following this concept, the size of the modules should remain small so that contributions can be easily made. “This allows the project to capture contributions from large numbers of contributors whose motivation level will not sustain anything more than quite small efforts towards the project,” says Benkler. Hypertext discussions meet the requirement of granularity by allowing for easy addition of short, simple facts, opinions or analysis. To meet the expectations of course participants willing to make more complex and longer contributions, the class forum is the appropriate space for initiating long threads of discussion. In this way a heterogeneous granularity is available in the program, and more significant contributions are taken into account in the evaluation of the participants.

Integration cost. Finally, considering that the foundations phase of the capacity-building program provided by DiploFoundation, in contrast to the research phase, is focused on the learning process rather than presenting a research report or any final product, the quality control and handling of contributions into the finished product (the integration cost) is minimal – the hypertext entries and forum threads are immediately integrated and sorted in chronological order to keep the dialogue consistent.

Expert advisors. Top-down direction and support is offered by tutors together with leading scholars and experts in a wide range of fields, including ICT policy, global governance, Internet protocols, networking, international law, human rights, eCommerce, among others.[3]

[3] http://www.diplomacy.edu/poolbin.asp?IDPool=168

TUTOR-STUDENT AND STUDENT-STUDENT ROLES

Online collaboration is a key component for building the virtual community necessary to produce bottom-up knowledge. Motivational elements must be taken into account in understanding the roles of tutors and students leading to optimal collaboration in the capacity building. High motivation is an important component to be added to the time management, discipline and organization skills one needs to participate in a distance- learning initiative. According to Bruno Frey, motivations can be extrinsic and intrinsic. Extrinsic motivations are external ones, such as monetary prizes or threats of physical or social punishment. Intrinsic motivations are reasons for action that come from within the person, who has clear inner values, long-term goals or just seeks immediate pleasure.

Extrinsic motivations are associated with a reactive mindset. Decision-making is oriented in reaction to external forces. Intrinsic motivations, on the other hand, can be closely associated with a proactive mindset by acting in accordance with inner values and goals. Stephen Covey observes that this is not a black-and-white division, as proactive people are still influenced by external stimuli, whether physical, social or psychological. But their response to the stimuli, conscious or unconscious, is a value-based choice or response. Benkler identifies three groups of rewards: (i) monetary rewards, (ii) intrinsic hedonic rewards experienced from taking the action and (iii) socio-psychological rewards, which are a function of the cultural meaning associated with the act. Without going into detail about each of the modalities, there is one motivational feature that has proven valuable for the Internet Governance Capacity Building Programmes under examination: fellowships.

Fellowships. The practical-experience dimension is a key element for the successful implementation of the programmes. Thanks to the valuable support of different partners, fellowships were granted to successful participants to participate in WGIG meetings, WSIS PrepComs, WSIS Tunis, IG conference in Malta, European Summer School on Internet Governance, internship on the IG Portal of DiploFoundation and fellowships in the WGIG Secretariat and IGF Secretariat in Geneva. Using clear merit-based criteria, fellowships, in a very simplified description, not only have the monetary reward (reimbursement of costs) but, most importantly, make use of the intrinsic hedonic rewards (pleasure of participating in interesting activities) and socio-psychological rewards (status perception and internal satisfaction).

Tutor moderation. In addition to the motivational elements brought up by Benkler, one-on-one support should also be provided for every participant, since collaborative learning does not happen automatically. The tutor has an academic role to play in responding to questions, sharing his expertise and pointing out important references. Most importantly, the tutor plays the role of group moderator, promoting an environment where participants feel free to express their ideas, identifying when expert advisors should be consulted, establishing a model for constructive communication, and supporting participants both individually and as a group.

The objective of good moderation with regard to participant involvement should be to help each individual participate fully, overcoming the various subjective and objective obstacles they may encounter at the beginning of the course. One of the main goals is to create a virtual community in the learning process, one which can sustain the bottom-up dimension.

According to Howard Rheingold's classic definition, the virtual community is the social aggregation that emerges from the Internet when enough people carry on public discussions long enough, with sufficient human feeling, to form webs of personal relationships in cyberspace.

Tutors monitor the daily performance of students and prepare weekly reports of their class activity. Upon noticing a decline in participation, they are able to send private messages to students in order to discern whether they are facing personal difficulties (health, work, family or other) or whether they simply need motivation or additional explanations. The students themselves also play an important role in motivating each other to support and explain their views, and add information according to their professional specializations and regional experiences, to enhance learning in the multidisciplinary classroom.

RESULTS AND DISSEMINATION

The last two IG training and research programs have shown that many former participants have become experts in their own right by pursuing further academic degrees, while others have become active in the various discussions and consultation meetings. For example, some now hold important positions as government advisors on ICT national policy in their local countries and have become part of the Global Knowledge Partnership, IGF Advisory Group, IGF Secretariat, ICANN and UN GAID. So within a year, individuals who were able to build upon their existing knowledge using this program are now able to assist and extend their capabilities to others within their own organizations and home countries. Participants also continue to exchange practical experiences and knowledge through communities of practice established during the course.

CONCLUSIONS

Creating a virtual community in which motivation to collaborate is high and social ties are strong is not a simple task. Here lies one of the greatest challenges for the future of teaching, as predicted by Ray Kurzweil: as information becomes more and more ubiquitous, the primary role of the teacher will be to attend to issues of motivation, psychological well-being and socialization. Capacity-building programs must implement techniques to ensure this role is fulfilled, overcoming the distance implicit in online learning.

Capacity-building programs shall create a local network of Internet governance experts and officials, which will facilitate various policy-related activities as they relate to development, including increased awareness and policy formulation and implementation. Because of language limitations, special care shall be provided to a first wave of participants who will be able to disseminate the knowledge in their own language and amplify the effects of the programs. In this way, the network of alumni becomes an ongoing and dynamic one, promoting the exchange of ideas, best practices and future collaboration.

In Latin America, the approach taken by having both a regionally based group and a bilingual group in which course participants received access to the same English basic materials but were encouraged to express themselves in Spanish has produced great results without the additional cost of translating basic materials into Spanish. This small step has enlarged the Latin American team, which will continue regional developments according to the institutional proposal of building a foundation of expertise and knowledge on Internet governance and policy, in countries with limited financial and human resources.

Diversity Reconsidered in a Global Multi-Stakeholder Environment: Insights from the Online World.

Claudia Padovani & Elena Pavan,
University of Padova & University of Trento

Diversity is a crucial element in development policies and capacity-building strategies. It is central to the very idea of empowering local and trans-local communities, as a core principle that guarantees their needs and aspirations are taken into consideration and effectively addressed. Diversity in the Internet Governance (IG) discourse can be conceived of in terms of content, channels and organizational structures. Broadly concerning communication processes, it is also normally understood in terms of the different voices, issues and cultures that should be heard, addressed and promoted. But one of the peculiar features in the development of IG discourses and practices in recent years, has been the explicit recognition that the sole involvement of governments and intergovernmental organizations in managing global resources of common interest is no longer acceptable or effective: different forms of knowledge, specific competencies and perspectives should contribute to the regulation and management of Internet resources. In other words, a diverse plurality of nongovernmental actors from the private sector, civic organizations and epistemic communities should be included, through appropriate mechanisms, in governance processes.

This understanding has been articulated through the so-called "multistakeholder approach" and formalized by the international community through documents (WSIS, Tunis Agenda 2005[1]) and practices such as the Internet Governance Forum and related processes[2]. This conceptual development, if considered in the light of governance transformations in a globalized context, offers a unique opportunity to reconsider perspectives on development, empowerment and capacity-building, all of which have a crucial stake in the promotion of diversity. Development is also evaluated in terms of cooperation between governments, intergovernmental organizations, private sector and civil society entities, while the necessary knowledge, skills and capabilities to effectively realize such cooperation imply capacity-building strategies that should themselves be diversified and open to the contribution of all stakeholders.

We therefore propose a reading of diversity – as one of the main components of IG alongside openness, access and security – that is founded on a critical understanding of multistakeholderism. As outlined elsewhere, the multistakeholder concept is a highly contested notion: "Different actors hold very different perspectives as to how stakeholders should be conceived, who is to be included and who is excluded and how their interaction should lead to information exchange, deliberation or decision" (Cammaerts & Padovani 2006). It is increasingly evident that stakeholders' participation risks becoming a rhetorical exercise aimed at neutralising criticism through the adoption of an unproblematic consensual understanding of political life. Moreover it is crucial to take into consideration the objective constraints and necessary preconditions to full and effective participation, such as financial and knowledge resources, or the available power base on which actors define their positions in governance processes. Diversity, in this view, also becomes a question of what actors are involved, the representational structures and, finally, the dynamics of power. At the same time, we concentrate our attention on an often overlooked reality: that of

[1] Tunis Agenda for the Information Society (WSIS-05/TUNIS/DOC/6 (Rev.1), par. 62 "We emphasize that any Internet governance approach should be inclusive and responsive…" and par.61 "We are convinced that there is a need to initiate, and reinforce, as appropriate, a transparent, democratic, and multilateral process, with the participation of governments, private sector, civil society and international organizations, in their respective roles…".

[2] http://www.intgovforum.org; http://www.igf2006.org

existing online networks of interaction among those actors who take part in the global IG debate. The offline IG discourse is deploying mainly in a transnational context that is hardly accessible to those who do not have the time, knowledge or financial resources to travel to meetings in Geneva, Tunis, Athens or Rio de Janeiro. At the same time, because of the very nature of Internet resources, virtuality is an inner component of Internet functioning and governance, as well as an important channel through which related debates develop. Moreover, it is often suggested that constraints to participation for actors, operating in different geographical and cultural contexts, may be less dramatic in the online world once appropriate platforms are set up, technical requirements are met and basic skills are provided. Then, it may be possible for everyone to be able to contribute to a plural online conversation. Nevertheless, reality continues to show that even in the online world, diversity remains a major challenge.

While acknowledging the interplay between online and offline interactions, our assumption is that tracing the interlinking among the nodes that collectively make up the IG-related thematic networks on the Web (showing which institutions, documents and organizations are actually engaged in the IG debate) can offer an "alternative" reading of how the discourse is being shaped and framed. We are, therefore, interested in understanding diversity in IG by focusing on "the who, what and where" of the virtual space, as a complementary assessment of offline dynamics (that deserve specific analyses and methodologies).

Here we build on research activities conducted through digital harvesting software[3] and adopt the language and conceptual tools of a network approach to offer reflections for a multistakeholder-oriented assessment of diversity in IG: actors involved, issues debated and representativity in geographical and cultural terms. For each of the three aspects we briefly address a set of questions, and we do this by looking at the composition

[3] We have used the Issue crawler software developed by Govcom.org and accompanying tools. For further information see: www.govcom.org and www.issuecrawler.net. Other visualizations can be retrieved from the Issue Crawler Archive.

and structure of IG issue networks as they can be traced on the Web. Given the space constraints, we here only show one of the maps elaborated through the Issue Crawler software, as an example of the visualizations that stand behind our comments.

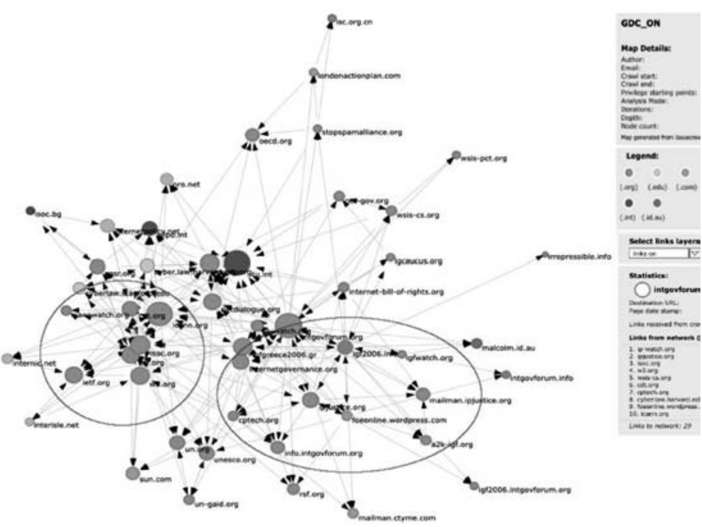


Figure 1: Internet Governance thematic network elaborated through Issue Crawler on March3, 2007 (starting points: Dynamic Coalitions launched around the first IGF meeting; Iteration 2; Crawl depth 2; Analysis Mode: by page).

WHAT "STAKEHOLDER DIVERSITY" EMERGES FROM ONLINE INTERACTIONS?

First we look at the kind of actors involved in the discourse on IG. Is there a meaningful diversity among them, so that we can actually speak of a multistakeholder conversation? Which actors occupy central positions in IG thematic networks and what kind of power relations can be inferred? An initial answer to these questions can be given by looking at the typology of nodes in the networks, identified through their domain extension. Our maps show that ".org" nodes are the prevailing type of actors animating the conversation. This is, according to our investigation, a feature of the IG debate that has not changed over time: there are other kinds of actors as well (identified as .edu, .int, .info, .com or local domains) but in a very small proportion if compared to the .orgs. Nevertheless, this does not imply homogeneity in the field, since the .org extension can refer to a variety of different subjects.

If we take a closer look at these organizations, we find at least three different types of .org actors engaged in the conversation. On the one side, composing a well-connected cluster on the left-hand side of our figure, we find organizations that have traditionally dealt with (and de facto managed) the governance of the Internet in the past decades: ICANN, IANA, IETF and the like. They represent the "traditional" nongovernmental, mainly technical, approach to IG: one that stemming from the historical developments of the Net and related infrastructures has developed "naturally" overtime, with its own logic and very little attention from the side of other actors, including governments (a part, obviously, from US interests to the ICANN). Then we have, though not really articulated into visible clusters of interactions, organizations such as the ITU, WIPO, the UN and UNESCO: international organizations that are supposed to provide guidance on the management of global resources, and represent the traditional logic of intergovernmental decision-making. Finally, the .org category comprises organizations such as IP Justice or Computer Professionals for Social Responsibility (CPSR) which are expressions of civic engagement in the IG discussion (the so-called "civil society"). These organizations often have their own history of advocacy and intervention on information and communication issues, broadly conceived; and yet some of them have become relevant nodes in IG-related networks.

Alongside the above-mentioned technical management cluster, we can see a quite identifiable cluster on the centre-to-right side of the figure: one composed of nodes that relate to the Internet Governance Forum (IGF) conceived as a process[4]. Interestingly the IGF has acted as a catalyst in promoting a diversity of actors that has grown over time: our analyses have shown that the "pre-Athens virtual space" was inhabited mainly by technical and

[4] The official website – www.intgovforum.org- is central in the map both in terms of its positioning in relation to other nodes and for the number of links it receives from the network.

institutional actors[5] while the "post-IGF2006" environment is much more diversified. Organizations from "civil society" have become visible actors in the IG debate. Furthermore the IGF also favoured the emergence of a plurality of related websites (also nodes in our network) that give a better sense of the ongoing process. Looking at this cluster we can say something more about actor plurality. A number of nodes – such as a2k-igf.org or Internet-bill-of-rights.org – link to the "dynamic coalitions": multi-stakeholder issue-driven groups that were launched around the first IGF in Athens and have since become the thematic "homes" of some of the specific issues that compose IG as a policy field.

In terms of relevance in the network, and therefore potential influence on the governance of the Internet, we suggest that interconnected clusters, and central nodes within them, probably play a more relevant role in the debate than individual not-so-strongly connected nodes and actors. These connected clusters don't always seem to have a broad understanding of the overall network and tend to be self-referential; at the same time their interconnectedness often implies a coherent language, a shared logic, history and vision, and therefore a likely stronger capacity to intervene in the transnational conversation.

This potentially more powerful position is partly counterbalanced by the presence of other actors involved in the debate, though peripheral in our maps, such as internetpolicy.net. The greater the distance from core actors in the network, the less likely these nodes are to be of relevance in the conversation. Nevertheless, some of these actors can be considered representative of alternative interests, different values and, possibly, emerging issues. Moreover, some of them may play a bridging role in the network, fostering connections among otherwise non-connected clusters and nodes and therefore contributing to the consolidation of overall thematic networks.

[5] It should also be recalled that these actors were represented in the map as belonging to separated clusters, the IGF playing a connecting role among them. The map is available in the Issue Crawler archive as IntGovForum2006_1.

Two new questions emerge from our investigation, and are left without an immediate answer: what is the role of academia in this virtual conversation, if only the cyberlaw centres at Stanford and Harvard Universities and the Internet Governance Project from Syracuse University appear in the maps? And, even more problematic, what about the absence of the private sector from a debate that clearly touches the strategic interests of business-oriented entities?

WHAT "ISSUE DIVERSITY" EMERGES FROM THE VIRTUAL CONVERSATION ON INTERNET GOVERNANCE?

Are there predominant issues in the IG debate and who promotes them? Can thematic clusters be traced in the Web? Once again, what kind of power relations can be inferred? Thematic networks on the Web do not immediately reveal hierarchies in the status of the issues being discussed; yet some observations can be made on the basis of our understanding of the whole process.

The fact that traditional actors (technical and institutional) and newer actors, especially after the first IGF, co-exist in the virtual space and (at least partly) recognize each other as legitimate parties in the debate, suggests that issue diversity has in fact grown over time. The presence in the thematic networks of the Dynamic Coalitions and of civic organizations such as Consumer Project on Technology (cptech.org) or Reporters sans Frontiers (rsf.org), beside those organizations who have been historically engaged in the governance of the Internet, parallels the widening range of themes included in the umbrella concept of IG. From a prevailing focus on technical matters the discussion has opened up to issues concerning human rights promotion and defence (foeonline.worldpress.org), universal access to knowledge and resources (a2k-igf.org), free software and knowledge production and distribution, and the necessity to foster multistakeholder modes of cooperation among actors (igf2006.info).

Finally, if we assume that central positions in the network to some extent reflect a more powerful status in the field, the relevance of traditional actors indicates the prevalence of issues traditionally connected to IG, such as management of critical resources, security problems and technical standards. At the same time, the necessity of articulating positions on highly contested matters, such as the promotion of freedom of expression or the defence or privacy and security rights, has led newer actors in the field to privilege networking activities among themselves in order to collectively develop shared contributions that could be proposed more effectively in the debate.

Overall, what emerges from IG issue networks on the Web is a quite interesting plurality of themes and positions; while issue priority and the capacity to foster specific views should be assessed through an in-depth analysis of offline interactions.

HOW GLOBAL IS THE "GLOBAL INTERNET GOVERNANCE ENVIRONMENT"?

Given the strategic relevance of Internet resources for societal developments worldwide and, even more important, given the attention focused in the IG discourse on the Internet's potential for narrowing economic and knowledge divides globally, a final key question concerns the level of representation of actors and institutions in the debate, from a geographical, linguistic and cultural point of view. If multistakeholderism is to become a model for decision-finding and decision-making processes in the future, debates and interactions should include not only transnational and supranational actors, but also subjects coming from different cultural contexts as well as local constituencies, which should be given the opportunity to express specific views and needs. Can we actually refer to the current conversation as globally rich and diverse?

The main observation we draw from our analysis is that local domains rarely enter web-based issue networks (the most remarkable exception being Greece -igfgreece2006.gr-), a situation which is justified by the fact that the first IGF was hosted in Athens). Sometimes, a local initiative is included: in the map shown above, for example, we find the national Belgian ISOC chapter or a specific initiative organized in Australia. But in general we see very few national, not to mention local, interventions in the online debate. Slightly more visible is the regional level, which is brought into the conversation through the presence of regional registrars, connected to the technical cluster of traditional managers of Internet resources. When more politically oriented actors from different regions appear to contribute to the debate, this happens through a very institutional approach: for instance, African needs find their way into the discussion through UNECA or UN Habitat.

We therefore underline the very problematic fact that nearly all of the actors in the thematic networks who are contributing to the definition of how Internet resources should be managed in the future come from Northwestern areas of the world. Apart from this less than balanced geographical representation, the dominance of English as the language in which definitions are given, issues are framed and relevant knowledge is produced is a fact. This situation clearly does not contribute to a rich and articulated understanding of globally diverse realities.

CONCLUDING REMARKS

In conclusion, we would like to stress the relevance of understanding diversity in terms of actors and interactions. Actors engaged in discussions on the future of Internet resources and the management of such resources bring their world views, knowledge and expertise to the debate; thereby contributing to defining its directions and outcomes. They also bring in their organizational logic and their understanding of how political processes can be informed by meaningful levels of participation. The plural conversation on IG is one of the most innovative experiments in participatory practices in the contemporary supranational context currently underway. And because this experiment exhibits some shortcomings, it is all the more crucial to underline how the innovative experiment could be better dealt with, to make it in fact “transparent, democratic and multilateral”.

Certainly, the gradual opening of the debate to different kinds of actors, organizations and initiatives that we have witnessed over time, reflects a positive progress and shows that it can take place quite rapidly, especially if opportunities are opened up by “catalyst” events, such as the IGF. This opening has had meaningful consequences in consolidating a broad understanding of IG, one that includes technical, economic, cultural, and public policy issues; a plurality that is now clearly visible in online conversations.

Nevertheless, the limited level of (online) interaction between more traditional and newer actors poses some questions concerning the actual level of reciprocal recognition as relevant parties in a political debate. It also has implications regarding the new and emerging issues to be brought into the discussion. If on the one hand it is highly questionable that an effective multistakeholder approach can develop if actors formally share a stage (WSIS, IGF) but do not enter into a true dialogue, on the other hand it remains to be seen whether the dialogic potential of the "dynamic coalition concept" will be realized, through both offline and online interactions.

Specific attention should also be paid to the absences that characterize the thematic networks we are focusing on. On the one side we believe that strategic innovation in IG, both in terms of content and of process, requires a much greater contribution from the academic community, knowledge networks and scientific world. It is therefore crucial to develop communication channels that connect scholarly associations and research centres, where knowledge that is relevant to the IG challenge is being produced, to the broadening dialogue on the future of this commons.

Secondly, we would draw attention to private-sector entities. These actors seem to be completely excluded from or not engaged in the thematic networks traced on the Web, if elaborated starting from the Athens' dynamic coalitions (which serve as proxies for the broader IG landscape). The lack of adherence of private businesses to these multistakeholder initiatives partly explains the result. But different web-based maps, elaborated on the basis of the outcome of Google queries for "internet governance", show a more marked presence and interest of private sector entities. What is problematic, in the context of the multistakeholder challenge, is not just the limited interest private actors are showing for innovative mechanisms in IG such as the dynamic coalitions. It is the fact that these mechanisms are evolving on the basis of transversally agreed upon principles of transparency and openness. Private-sector entities seem to prefer existing non-publicly accessible ways to conduct their business in the IG context, and are therefore not interested in the democratic potential of multistakeholder practice.

Finally, the dramatic under-representation of the "rest of the world" remains as a open issue that still stands as a huge hindrance to the realization, not just of a diversified conversation among actors, but most of all to the very definition of Internet governance for future generations. In spite of the rhetoric we find in documents and even in the IGF's organizational logic, we are still confronted with a situation that clearly does not favour a culturally rich and diverse composition of the debate. It thus undermines the possibility of contributions from culturally and linguistic diverse contexts. Being highly exposed to Internet developments and facing challenges that are completely different from those of the Western countries, voices from fast-emerging economies such as China, India and Brazil, as well as from the least developing countries, should be offered appropriate mechanisms to make their own perspectives known and develop their own proposals for solution. Such mechanisms would require specific commitments in terms of financial resources, capacity building and openness in politically relevant processes.

These are insights from the online world supported by our understanding of how the IG debate is developing. They are merely a partial glimpse of a complex reality, and yet one that offers an alternative perspective; a glance aimed at developing new research and policy questions, to be addressed in the real world, where concrete interactions take place and actual decisions are made.

The Tele-TASK Internet Bridge between Germany and China

Dirk Cordel,
Hasso Plattner Institute, University of Potsdam

A tele-teaching system as key enabler for successful Internet-based academic coop-eration between Germany and China

The Teleteaching Anywhere Solution Kit (tele-TASK) is a professional and well-proven sys-tem for tele-teaching and e-learning. Thanks to integrated plug-and-play technology, lectures and presentations are easily recorded and transmitted over the Internet. Furthermore, any user can access content produced using tele-TASK on the Internet, live or on demand. From a technical point of view, all you need to virtually participate in conferences, presentations and training courses is a standard browser, and the free RealPlayer plugin.

tele-TASK has already proven its potential in various scenarios. The system is, for example, used for many of the daily lectures at the Hasso Plattner Institute (HPI) in Potsdam, Ger-many. Content produced with tele-TASK lets students and e-learners attend courses from abroad and prepare for exams. As well as the video and voice of the lecturer, his computer desktop is also recorded and transferred synchronously. With more than 8 million hits, the online portal www.tele-task.de, with its high-quality tele-TASK lectures and pres-entations, has become a popular source for e-learning. The system's main component is the tele-TASK cube. All the technical equipment needed to control, record and transfer presentations - such as the encoding computer, microphone re-ceiver, small display, keyboard etc. – is integrated in a small case, which makes tele-TASK a highly mobile system. The presenter merely connects a camera and his computer to this box. The intuitive user interface means anyone can use tele-TASK: there are only three main but-tons to perform the recording (start, pause and stop).

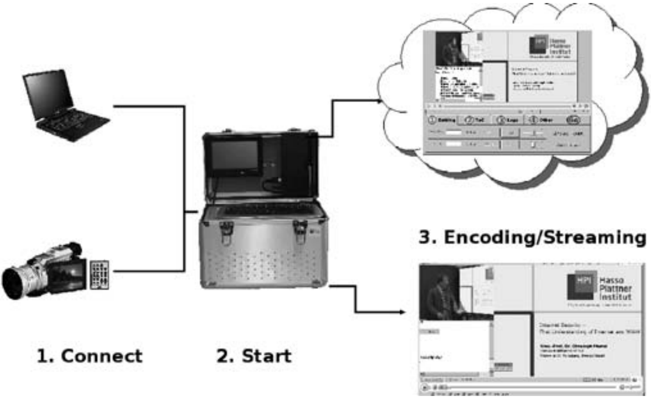


Figure 1: Producing Multimedia Lectures with tele-TASK

At the Hasso Plattner Institute, tele-teaching is already an integral part of lectures. Besides lectures we also record special events like the weekly colloquium, the annual bachelor podium, project presentations, and special events like Germany's first national IT Summit, with Chancellor Angela Merkel in attendance.

tele-TASK is not only used for internal e-learning activities. Via an Internet Bridge, it also en-ables academic cooperation between HPI in Germany and the Beijing University of Technology in China. The Internet Bridge for tele-teaching activities described above officially started in 2002 with the transmission of an e-learning course by Prof. Christoph Meinel, who at the time was working at the University of Trier's Computer Science department. He and his Chi-nese colleague Prof. Yin Boacai at the Beijing University of Technology decided to collabo-rate by offering Trier's lecture course "Internet Security" to computer science students in Beijing via the Internet. This was the first time ever that Chinese students were able to watch a lecture course by a German professor over the Internet.

The enabling technology behind this e-learning course was the tele-TASK system. At that time, its functionality was slightly different to the current system, but it already provided the means to capture, encode and transfer different multimedia input streams live and synchro-nously over the Internet. By making further improvements to tele-TASK and developing better hardware technologies over the following years, we were able to enhance the quality of the lecture videos and also the compactness of the tele-TASK system.

In 2005, another Internet Bridge project was started between HPI and the Beijing University of Technology. Meinel, by now director and professor at the HPI, continued to offer his “In-ternet Security” lecture course to Chinese students at the Beijing University of Technology.

Every year from September to the end of January, about 35 90-minute lectures, two a week, are transmitted to China. The course content is structured into two parts. The first part, “Technological Basics of the Internet,” explains communication in computer networks and Internet technologies, protocols and services. The second part, “Weaknesses and Targets in the Internet” describes popular attack methods and countermeasures to secure computers and networks. Apart from lectures on these topics, each week one HPI exercise sheet is up-loaded to the Beijing University of Technology. At the end of the course, a written exam is prepared (including answers for the Chinese teachers) and sent to the assisting lecturer in Beijing responsible for supervising the exam. Meinel then travels to Beijing. After several formal meetings with Chinese professors, researchers and the executive board, he gives lectures for the Chinese students about “breaking” developments in IT-Security, thereby rounding off the topics discussed via tele-teaching. In addition, there is a presentation about the HPI and its ongoing projects, as some students are interested in coming to Germany to continue their studies with a PhD. Meinel then administers exams to the Chinese students in groups of three. Each exam takes about 30 minutes and students are asked to prove their knowledge in all topics discussed in the tele-TASK lectures and exercise sheets. The end score is a combination of the written and oral tests. If students pass the exam, they receive a certificate signed by HPI and the Beijing University of Technology. To date, over 150 Chi-nese students have successfully taken part in this lecture course from Germany and ob-tained the certificate. Besides the meetings and exams, there are always pleasant, informal meetings between the German professor and the Chinese students where topics like education, culture, and every-day life are discussed, with all participants free to exchange experiences and opinions.

To conclude, Internet-based academic cooperation between HPI and Beijing University of Technology provides great benefits for both partners. Although most of the communication takes place over the Internet, the cooperation is not only virtual; it is still important to meet from time to enhance the cooperative relationship. Secondly, the cooperation is not only an exchange of technological know-how, but also an exchange of experiences and general opinions between different cultures. Tele-teaching with our tele-TASK system has been one of the key factors in achieving this successful and continuous cooperation.

References and Links:
http://www.tele-task.de
http://www.hpi.uni-potsdam.de
http://www.internet-bridge.hpi.uni-potsdam.de/

Chapter 3
Diversity

Cultural Diversity, Multilingualism and UNESCO

Koïchiro Matsuura,
Director-General of UNESCO, Paris

The Internet holds enormous potential for development. By providing an unprecedented volume of resources for information and knowledge, it opens up new opportunities for expression and participation. However, there is also a risk that this potential may not be used to the fullest possible benefit. The broader policy debate on Internet governance is of particular interest to UNESCO, since key elements of its Constitution include a mandate to promote “the free flow of ideas by word and image” and to “maintain, increase and spread knowledge”. This debate is also linked to the principles integral to UNESCO’s concept of “knowledge societies” – freedom of expression, universal access to information, cultural and linguistic diversity and equal access to education – which were echoed in the "Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace", adopted in October 2003 by UNESCO's General Conference.

The Internet is a key factor for developing true knowledge societies, which stress plurality and diversity instead of global uniformity and can contribute to bridging the digital divide and forming inclusive societies. An important component of this concept is multilingualism, which is vital to ensuring cultural diversity and participation in cyberspace of all languages. There is growing concern that hundreds of local languages may be side-stepped, albeit unintentionally, in the radical expansion of Internet communication and information: hence the importance attached to linguistic diversity and local content as part of an Action Line of the WSIS Action Plan for which UNESCO has the responsibility of coordination.

Increasingly, knowledge and information are determinants of wealth creation, social transformation and human development. Since language is the primary vector for communicating knowledge and traditions, the opportunity to use one's native language on global information networks will determine the extent to which one can participate in the emerging knowledge society. Thousands of languages are absent from the Internet and there are no tools for creating or translating information into these excluded tongues. Huge sections of the world's population are thus prevented from enjoying the benefits of technological progress and obtaining information essential to their well-being and development. Unchecked, this will contribute to a loss of cultural diversity on information networks and to the widening of existing socio-economic inequalities.

Freedom of expression is central to building strong democracies, contributing to good governance and the rule of law, promoting civic participation and encouraging human development and security. The principle of freedom of expression must apply not only to traditional media but also to such new media as the Internet.

Governments resort to many methods to restrict free access to and use of the Internet. Some are financial, such as high taxes or tariffs; others are technical, such as filtering and blocking software on servers; and still others are administrative, such as having to obtain permission from authorities to register websites and the refusal to install international servers. In addition, there may be legislative measures, for instance in the form of confidentiality laws to protect personal data, legislative acts that deal with security, or special laws to block sites that are perceived as providing access to information contrary to certain political, behavioural, or moral standards.

While press freedom and freedom of expression are fundamental human rights, most countries have enacted national civil legislation limiting it in cases such as libel, breach of privacy and pedophilia. These matters may not all be without controversy but, in general, such national legislation commands widespread support.

Another challenge is the connection between the Internet and protection against terrorism. The balance between measures required for fighting terrorism and respect for fundamental rights is very difficult to find. There is a real risk that some security measures may, directly or indirectly, undermine the very principles and rights that terrorism seeks to destroy.

It is dangerous to establish rules for the free flow of information. Not only can this hinder the open exchange of ideas and opinions, it may also force unwanted ideas – for example, hate speech and propaganda – to be expressed exclusively underground, making it difficult to counter them with informed arguments. Furthermore, there is the risk that ideas and opinions which could enhance the open debate on controversial issues will be silenced. The real challenge lies in fully exploiting the potential of new media while not compromising civil rights and liberties, including the right to privacy. All citizens have the right to express their ideas and opinions worldwide and to seek information freely through electronic networks. This is also why UNESCO organized two workshops focusing on how to ensure the openness of the Internet and the free flow of information at the first Internet Governance Forum in Athens in 2006, and why it is preparing another workshop on "Freedom of Expression as a Security Issue" during the second Internet Governance Forum in Rio de Janeiro in November 2007 for the purpose of exploring security and security protection mechanisms as factors that influence freedom of expression on the Internet.

UNESCO also observes that the term "Internet Governance" has not yet been clearly defined. For some, it describes the narrow issue of the management of domain names and infrastructure, which are presently administered by the Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation under Californian law. The prevailing tendency in the current debate, however, is to assign a much broader meaning to this term, comprising not only technical, but also ethical, societal and legal issues. Moreover, the term "Internet governance" is misleading as it is laden with presumptions about governing approaches, which for some may imply governmental involvement.

For UNESCO, an important issue is the interdependence between the smooth functioning and openness of the Internet, and economic and technological stability. This is also why UNESCO has established a threefold strategy for its work in regard to the Internet Governance Forum:

a) UNESCO will contribute to the debate on issues within its fields of competence, particularly the broader "cyberspace" policy issues (legal, societal and ethical), insisting on sound analysis, advocating precise language and depoliticized debate.

b) With its record of successfully promoting collaboration among governments and civil society, UNESCO is ready to participate in discussions and to assist those tasked with the review of Internet governance to develop solutions that fit the diagnosis and are of a lasting nature because they reflect a wider consensus on the issues.

c) UNESCO will continue to safeguard key values such as freedom of expression, cultural and linguistic diversity and openness. It will advocate that existing mechanisms such as ICANN, or any modification of these mechanisms, must be based on the following principles:

   - The inherent openness of the Internet infrastructure must be preserved and should be conducive to the free flow of ideas and knowledge through word and image;
   - Modifications must not result in the global Internet governance system becoming subjected to governmental control, nor should they facilitate or permit censorship;
   - There must be a precise correlation between new mechanisms and the problems they seek to address;
   - Technical innovation must continue to be encouraged;
   - Modifications to ICANN or new mechanisms should not inhibit interoperability, cause instability, nor slow down the continued technical development of the Internet;
   - Any global Internet management system or mechanism must be technically competent, transparent and non-partisan.
   - Whichever mechanism manages the current responsibilities of ICANN, the result should be one that enables greater use

> of the Internet, and thereby greater participation in the modern information world by an increasing number of citizens from diverse linguistic and cultural backgrounds.

At the dawn of the information age, it is vital to understand that the full potential of knowledge societies will never be reached if “the free flow of ideas by word and image” is restrained. Freedom of multilingual expression is not simply a happy by-product of such societies, it is the very fuel that drives their dynamic transformation.

What it Takes to Get the Next Billion Users Online

Guy Sebban,
Secretary General, International Chamber of Commerce
(ICC), Paris

INTRODUCTION

The International Chamber of Commerce is the largest, most representative business organization in the world. Its thousands of member companies in over 130 countries have interests spanning every sector of private enterprise. More than 2000 experts drawn from ICC's member companies feed their knowledge and experience into crafting the ICC stance on specific business issues. Access to infrastructure, and in turn to the Internet, is a top-priority issue for business around the world.

ICC created Business Action to Support the Information Society (BASIS) , in mid-2006 to serve as the voice of business in the global dialogue on the information society, following the two World Summits on the Information Society (WSIS) held in Geneva (2003) and Tunis (2005). BASIS participates in UN-linked forums set up to continue the dialogue, such as the Internet Governance Forum (IGF), the Global Alliance for ICT and Development (GAID), and the WSIS follow-up and implementation processes. BASIS builds on the activities and network of the Coordinating Committee of Business Interlocutors (CCBI), which ICC formed to coordinate the participation of world business in WSIS preparations and events. This chapter highlights what it takes to get the next billion users online from the perspective of our business experts, and what governments and other stakeholders can do to facilitate access.

FUNDAMENTAL BUILDING BLOCKS FOR ACCESS

Business believes that access to the Internet ? as well as to the information and communications technologies and infrastructure that allow this ? starts with creating the right conditions to make it possible. We often refer to this as the "appropriate enabling environment", which is difficult or at least challenging to achieve in its complexity, but vital for development.

Internet connectivity starts with the enabling environment ? one cannot make all the advantages of the Internet available without addressing the policy, legal and regulatory frameworks that enable investment in infrastructures to support access. Some of the elements that need to be addressed are:

- Telecoms liberalization
- Creation of an independent regulator
- Development and implementation of the rule of law
- Introduction of pro-competitive legal, policy and regulatory frameworks—resulting in choice regarding quality and cost of services
- Creation of independent courts
- Fostering entrepreneurship and innovation

We must all acknowledge that there are sometimes even more basic conditions that need to be put in place, such as healthcare, and electricity, but for the purposes of this chapter, we will move beyond the basic infrastructure issues. Many of the elements above are self-explanatory, while others are not. Fostering entrepreneurship is a multifaceted objective. What is meant by this and how do we get there? Entrepreneurs are nurtured by having a solid basic education, and skills training. Many businesses are major contributors to training and skills development both for their employees and the initiatives they are involved in, through partnerships with governments and other stakeholders, or independently. Entrepreneurs also need a place to grow that is free of unnecessary obstacles, such as excessive bureaucracy and, administrative burdens. Putting programs in place that help entrepreneurs provides many benefits to individuals and increases the number of available jobs in a country. This in turn benefits the government and the country. Creating incentives regarding taxes and social charges can help new businesses get started and create more jobs. Another way to encourage entrepreneurship is to provide greater access to capital to start or expand a business. Governments and others can help make that possible by creating incentives and developing programs that provide startup funding and teach entrepreneurs how to raise capital.

WHAT BENEFITS CAN TELECOM LIBERALIZATION BRING?

Business has long said that a major step for countries and economies seeking to improve access to the Internet is liberalization of the telecommunications sector. Some of the benefits that result from telecom liberalization include:

- Lower prices, particularly on long distance/international calls
- New and innovative services with better reliability and greater capacity, enabling overall economic growth
- Foreign direct investment (FDI) in the telecoms sector, accompanying spending in the local economy and transfer of technology, skills and business methods
- An increase in FDI as a whole – improved facilities and infrastructure attract FDI and liberalization commitments send a positive signal to potential investors
- Increased user access and the opportunity to deploy more affordable universal access.

Licenses are one of the keys to success in the liberalization process. They provide the basic certainty and legal security investors and lenders need to invest the huge amounts of money necessary to install or to upgrade telecoms infrastructure. Licensing should be technologically neutral to prevent market distortions, to avoid being rapidly outdated, and to foster innovation. For telecoms liberalization to lead to a fully competitive telecoms market, market entry should be subject to as few barriers and restrictions as possible. The success and growth of the Internet in any given country depend directly on the available network of fixed and mobile connections. Where telephone penetration is high, the growth of the Internet has been nothing short of explosive. In countries with low penetration, universal access achieved through liberalization should be the top priority to spread the benefits of the Internet throughout the country. Mobile access has also been successful as a means to enable electronic communications in rural and remote areas.

WHAT ELSE HELPS TO ATTRACT INVESTMENT SO THE NECESSARY INFRASTRUCTURES ARE BUILT?

As mentioned above, fostering entrepreneurship, liberalizing telecommunications sectors, and implementing other elements such as pro-competitive legal, policy and regulatory frameworks, are part of the 'recipe' for attracting investment in infrastructures.

When local and foreign businesses assess an investment environment, they look for a certain level of security for their investments. A key consideration for a sector to attract investment is making sure that laws and regulations are clearly defined. Some of the recommended steps in that reform process include:

1. Making an inventory of existing legal instruments affecting the sector: treaties, bilateral and multilateral trade agreements, telecoms laws, decrees, ministerial orders, licenses, tenders and contracts (such as for specific services with network operators, Internet Service Providers (ISPs), or equipment manufacturers and vendors)
2. Creating a strategy for reform of the sector
3. Ensuring that the team in charge of reform remains loyal to the primary purpose of the reform, which in most cases will be to provide both consumer and business users with more varied, efficient and less costly communications services.

The removal of any international trade barriers to investment is another way to help attract investment. Taking steps to achieve the following conditions can help countries remove obstacles to investment:

- Market access and national treatment commitments for all service sectors without restrictions
- Reduction or elimination of foreign ownership restrictions
- Adherence to the Reference Paper commitments for basic telecoms services only
- Compliance with the GATS Annex on Telecoms for access to and use of public telecoms networks for the provision of value-added services, including Internet services and other sectors for which countries have made commitments.

CONCLUSION

ICC BASIS believes that the Internet Governance Forum (IGF) offers an important opportunity to discuss issues related to access to infrastructure, and access to information and knowledge. In addition, the IGF gives all stakeholders a chance to discuss their experiences, views, and concerns. Discussions about access should raise awareness about the responsibility of governments for ensuring an enabling environment to improve access, and the importance of involving business and other stakeholders in making this environment a reality at the national level.

ICC BASIS members believe that it is essential to establish the necessary enabling environment to promote access to infrastructure and the Internet. This calls for a real focus on the legal, policy, and regulatory conditions that enable private sector investment and innovation, promote competition and foster entrepreneurship. Sharing different perspectives and information on case studies regarding economies that have created successful enabling environments, contrasted with examples of challenges and approaches that were not successful, is an example of the sort of dialogue the IGF has successfully facilitated.

All stakeholders involved in the global discussions on the information society have a common goal: to bring the benefits of the Internet to more people around the world, and to welcome more people into the discussions on Internet governance issues at all levels – national, regional and international.

Business believes that access to the infrastructure facilitates access to education, information, and knowledge, and that all of these elements are important for development.

The Internet for Social Development, Openness and Diversity: The Case of Russia

Michael Yakushev,
Board Member of the Russian CCTLD .RU Coordination Center, Microsoft Russia, Moscow

Openness has been one of the characteristic features of the Internet. Without being open to any potential user and new technological application, the Internet would have never become such a universal, affordable and comprehensive tool for intercommunication.

The notion of 'openness' is closely related to notions of access and freedom. No one would argue today that access to information and services is not a key tool for individual success and freedom and a main criterion for social progress. Of course important questions remain as to what other tools are required for success, and limitations on individual freedom are needed to protect the legitimate interests of wider society as well as national and international security.

Fortunately, these questions can be resolved without compromising openness. Various aspects can be interpreted differently depending on context. For some people 'open the Internet' means 'information that cannot be found anywhere else', for others it means the ability to open for everyone, to open up their creative potential and publicize their own skills '.

Openness becomes a real factor in economic growth and technological opportunity. By being open to its citizens, a government is more trusted and can carry out economic reforms more easily. The opposite is also true – if politicians are unable or unwilling to be clear and honest about their intentions and actions, they will probably not be reelected - or will do their best to change the political system to avoid new elections.

The former Soviet Union is a good example of this. As a politically closed society, it showed very low levels of openness. Gorbachev's policy of 'glasnost' ('openness' in Russian) finally buried the political system of the USSR and the state itself. The main cause was the inability of such a political system to adapt itself and become truly open. It could only disappear. Perhaps the fact that it collapsed at the same time as the Internet emerged is no coincidence...

Internet technology facilitates political openness and access to information without dramatic consequences. Internet openness does not require excessive investment in infrastructure, and it can distribute much more information to far more people than offline means of communication. Technological innovation has changed the perception of the Internet as a 'computer network'. Internet information can now be obtained not only from computers, but also from devices like cell phones and interactive TV-sets. This will make the Internet even more widespread.

As already mentioned, the openness of the Internet offers additional opportunities for self-development and improvement of 'human capital'. More information can be accessed by anyone at a lower cost. This is even more important for less developed countries. But as with any relatively new technological invention, the Internet creates new threats and raises new concerns. Openness becomes an efficient tool not only for students, researchers, voters or local residents searching for information they need; it can also be a tool for terrorists looking for sensitive information or new recruits.

The Internet also opens up new 'dimensions', new interpretations for 'old' notions such as anonymity. Can anonymity be compatible with the concept of an open Internet? Do Internet surfers have a right to be anonymous? Such questions may seem theoretical, but in fact have significant practical implications. First of all, the online legal relationship is closely linked with that of the offline world. No one can limit anything online which is fully lawful offline – and even if such limitations were introduced, they would hardly be enforceable in practice.

So, upon further examination anonymity is always relative: absolute anonymity never exists. A person can be unknown to the vast majority, but to live a normal life such a person has to have legal relationships with different people or entities to whom he reveals his identity in order to enjoy his civil rights. The same applies to the right to be anonymous online. In principle anonymity should be protected as a component of privacy. But, of course, there are different situations where an Internet user may be asked to identify himself – and there should be legal and technical mechanisms in place to enforce such a demand. Similar treatment is necessary in dealing with attempts to use Internet openness for illegal purposes.

Another consequence of openness is diversity. This is also a multifold notion that cannot just be limited to multiculturalism or the problem of internationalized domain names. Internet technologies offer brilliant opportunities to reflect the diversity of today's world. The more we learn about each other, the easier it is to find a common language based on common values implemented in different cultural traditions. And this is not only true for intercultural dialogue between different nations. Diversity can also be helpful for bridging the digital divide within countries, between social groups and between different age groups.

It is a well-known fact that in countries like Germany, France, Russia or China, Internet users prefer to visit web pages in their local language (rather than English-language sites). Such countries have enough resources to produce and protect local Net content. This trend is also evident in other non English-speaking countries, but promoting and protecting diversity sometimes requires the assistance of government, local business, and ethnic communities.

It is interesting that a broader concept of diversity becomes a substantial cultural (and even political) problem for multi-ethnic countries, where the protection of diversity raises the issue of protection of identity. One of the most famous cases is the Catalan movement, which even managed to register its own top-level domain. But there can be collisions on a lesser scale. For example, as a native Russian, I was surprised to learn from Wikipedia that a different form of the Russian language, used mostly in Siberia (so-called Siberian Govor), is recognized as a separate language, similar to but different from standard Russian. This was posted in Wikipedia, a reputable Internet resource. I am not sure what this is - a joke? A separatist movement? Or a linguistic discovery? Different people will have different answers – but it is a real example of diversity and a real pleasure to learn something new and interesting.

The proposal for internationalized domain names is often seen as a best-practice case for the concept of Internet diversity. But even here we find plenty of politically motivated issues. For example, do ethnic minorities have the right to a top-level domain in their country of residence if their language is not official in their country (e.g. Russians in Latvia or Estonia)? If so, who should administer such domains? And if not, what of the principle of diversity?

Overall, such issues – as well as countering illegal usage of Internet technologies etc. – are subject to some regulation, which is usually referred to as 'Internet Governance'. It is important that Internet Governance be based on a multi-stakeholder approach, with equal participation by national (and perhaps regional) government, business and professional associations, civil society, NGOs and non-commercial organizations. It is good news that such a broad approach has gained universal recognition and is being implemented by international forums such as IGF and WSIS. Internet Governance itself should be ruled by principles of openness and diversity – only then can it be genuinely efficient.

An Analysis of Various Models for Wireless Cities

Kaili Kan,
School of Economics & Management, University for Post & Telecommunications, Beijing

INTRODUCTION

Over the last two years, “Wireless Cities” have been mushrooming in the world, especially in the Asia-Pacific region. By the end of 2005, it was reported that over 40 cities in the world were covered by wireless broadband. Only a year later, hundreds of municipalities had reportedly built or were in the process of building wireless cities. Early examples of wireless cities include Taipei, while last year Singapore announced its plan to provide free wireless broadband access nationwide, and recent developments include Hong Kong, Mexico and many others. Unlike previous developments in the telecommunication sector by telecommunication operators (telcos), the recent wave of wireless cities is mostly initiated and driven by municipal governments. Treating this as the “fifth utility” for the city, their goals are to provide an infrastructure for social and economic development, and to provide an affordable service (preferably free-of-charge) to all their citizens in order to narrow the digital divide. As profitability is not even considered, profit-oriented telecommunication corporations, especially incumbent ones, are merely playing a subordinate role, or are being left out of the picture completely. Furthermore, one of the suspected reasons for telcos’ lack of enthusiasm is that, once the area is covered by free-of-charge wireless broadband with VoIP and all kinds of services running over it, their life-supporting stream of revenue will quickly dry up.

ANALYSIS OF CURRENT WIRELESS CITY MODELS

Currently, there are four basic models for funding, building, owning and running wireless cities [1-12]:

- By municipal government agencies directly;
- By private for-profit corporations;
- By a government-contracted private corporation; and
- By commune-like sharing mechanisms based on “grass roots” users.

Looking closely at each of these models from a government’s perspective, we can see that they all have their respective advantages and disadvantages.

Wireless city by government agencies

This model obviously provides the most direct control for implementing the government’s social goals. However, it also has its disadvantage of not providing a market mechanism to attract participation from either user groups or industry. Thus, not only it is subject to rigid government planning procedures which cannot respond quickly to consumer demands, it also places significant burdens on the government agency financially, operationally, legally and sometimes politically.

For example, because providing wireless broadband access has become a commitment of the government to all of its citizens, it is hard to answer the question of why the access quality of one apartment is not as good as that of its next-door neighbor. In addition, in the event that the wireless network’s utilization does not meet initial expectations, the government could be blamed for wasting taxpayers’ money.

Wireless city by private industry

This model’s pros and cons are the opposite to those of the above-described first model. On the one hand, it takes full advantage of market incentives and relieves the government of its commitment and all burdens. However, on the other hand, the for-profit motivation of private corporations obviously deviates from the social goals of the government.

For example, wherever there is no potential for profitability, private corporations are most likely to entirely abandon the goal of building a wireless city. On the opposite end of the spectrum, where an attractive profit potential exists, the availability of bandwidth becomes an issue, leading to the forbidding task of frequency allocation among a large number of competing applicants. Furthermore, since achieving social goals is the underlying reason for the government, it will be obliged to regulate the market, which includes licensing operators, levying tariffs on service, providing universal service, etc. As past experience has shown, each of these on its own is a Herculean task.

Wireless city by a government-contracted private entity

To some extent this model bypasses the problem of frequency allocation and provides a more assured method for achieving government goals. However, no matter what procedure is used to select the private entity, this model creates a market monopoly that is mandated to serve social goals against its own interest of maximizing profitability. Thus, as the century-long case of the U.S. DOJ and FCC vs. AT&T has already shown, the government is left with the impossible task of regulating a monster monopoly and forcing it to serve public interests.

Wireless city by "grass roots" user groups

In this model, "grass-root" users form a "commune" by resource sharing mechanisms. It best takes advantage of the Internet's very nature of "Of the people, by the people, for the people". As the network is built by users themselves, any location that has a demand for access will likely have an access point (AP) built by the people at that location who need it, use it and shared by others, thus automatically and dynamically responding to demands. Furthermore, as the network is built by all members, it naturally becomes free-of-charge among all of its contributors. Therefore, once this sharing mechanism is established, there is no need for the government to invest in, build, own or operate anything for achieving its social goals.

However, this model has one vital weakness, which is how to get it started and reach a "critical mass". Obviously, when the number of shared APs is small, it provides little incentive for others to join the sharing mechanism and thus expand the coverage over the entire area.

THE MODEL OF “LED BY THE GOVERNMENT, BUILT BY THE PEOPLE”

After analyzing the pros and cons of current models for wireless cities, we realize that none of them are perfect. Therefore, as the Beijing municipal government actively plans “Wireless Beijing”, a new model is being devised. Characterized as “led by the government, built by the people”, this model seeks to combine all the advantages of current models while avoiding all their disadvantages. It is composed of the following parts:

Role of the government

It was estimated that the Beijing municipal government needs around 2,000 to 3,000 wireless APs for its own usage, including traffic control, police surveillance, emergency handling, etc., which would cover all the main streets and public areas of Beijing. This wireless coverage is to be built anyway and requires no more than USD $2-3 million, easily allocated within the government’s regular budget. However, the 54 Mbps bandwidth of 802.11g is far beyond the need for daily usage by government agencies, and this surplus bandwidth can be made available to the public.

By doing so, without spending more than it needs for its own usage, the government lays the foundation of “Wireless Beijing Commune”, a publicly shared wireless broadband network.

Role of social entities

Beijing has a large number of universities, schools, government agencies, hospitals, corporate headquarters, etc. Many of these already have Wi-Fi coverage for internal use. Thus, the Beijing government will encourage these entities to open their surplus capacity to other members of the Wireless Beijing Commune. By doing so, these entities become members of the Commune themselves, and will be entitled to free Internet access at thousands of government’s access points as well as all those of other members.

For example, currently BUPT already has its campus covered by Wi-Fi access points, but these can only be used by its own personnel, which is a waste of bandwidth, and only on campus, which limits it usefulness. Upon joining the Beijing Wireless Commune, BUPT's students and staff will enjoy free Internet access throughout the city via access points of the government and other members, while government officials and personnel of other member entities will be able to freely use access points whenever they happen to visit the BUPT campus.

Therefore, by adopting this sharing mechanism and at absolutely no additional cost, the benefit of providing Wi-Fi coverage at these entities' own premises is substantially magnified, and thus provides a strong incentive for all these entities to join the Commune and share their access points. If hundreds of entities like BUPT join, the initial thousands of access points by the government could easily expand to tens of thousands.

Role of individuals

For individuals who have broadband access at their homes or offices, a similar mechanism will be applied. That is, any individual who makes his/her access points available to other Commune members will become a member of the Commune. As members of the Commune, these individuals will be entitled to free Internet access at access points of the entire Wireless Beijing Commune throughout the city.

Once they have access to the Internet, they will enjoy all the services available, including free VoIP phone calls provided by Skype and the like. In effect, after joining the Commune, their monthly telecommunication bill will be shrunk to the single monthly-flat expense of broadband access at their own home or office, eliminating most, if not all, phone bills, mobile charges, etc. This tremendous saving not only will attract hundreds of thousands to join the Commune's sharing mechanism, but will also motivate people to buy wired-broadband access in order to setup access points if they did not have one before.

Non-members of Wireless Beijing Commune

For visitors to Beijing, free access can be provided for a limited period of time upon their arrival. For people who do not have or cannot afford an access point to join the Commune, free access to the Internet will also be provided but at a lower speed and priority, and maybe only at non-peak hours of the day. The difference in speed, priority, time and duration will be applied at the early stage of the Wireless Beijing Commune in order to encourage capable entities and individuals to make their contribution of access points. However, as the network reaches its full coverage and capacity, these limitations could be gradually reduced and eventually eliminated.

Role of telecommunication operators

Obviously, all access points need connections to the Internet backbone. As members of the Beijing Wireless Commune, including the municipal government, are responsible for setting up their own access points for sharing, they will be responsible for providing these connections as well. However, as there are multiple telecom operators as well as cable TV operators who have plenty of optical cables underground, they will be competing against each other for selling their bandwidth and connection. By taking full advantage of this competition, the highest quality and lowest cost of wired connection to Internet backbones can be ensured.

CONCLUSION

Comparing the model of "Wireless Beijing Commune" with current models, it can be seen that it effectively combines the advantages of all four of the current models, while avoiding their disadvantages. Specifically, it

- fully achieves the social goals of the government,
- minimizes the financial, operational, legal and political risk and burdens of the government,
- takes full advantage of public participation,
- realizes complete city coverage while costing each party no more than for its own usage,
- most dynamically respond to demand,
- takes full advantage of market competition and further stimulates it.

Therefore, this model is most likely to bring rapid expansion of the municipal wireless broadband coverage in Beijing, estimated to reach 100,000 shared access points in three to five years.

It is also expected that this model will become the mainstream model for wireless cities throughout China and many other places in the world.

Furthermore, this model introduces the municipal government as a new “heavyweight” player in the telecommunication sector, which often plays a leading role. It will transform current telecommunication operators into “hollow pipes”, providing little else but optical bandwidth and wired access underground. Therefore, rapid growth of wireless cities according to this model will likely bring fundamental impacts to the entire telecommunication sector.

That Small Part of the Web Once Called Television and Radio

Jean Réveillon[1],
Director-General of the European Broadcasting Union
(EBU)[2], Geneva

When experts talk about 'the Web', they usually do not include broadcasting. The debate at the two World Summits on the Information Society in 2003 and 2005 mainly focused on extending the telecom network, costs of accessing it, problems with the software used to connect to the Internet, and so on. Broadcasting's contribution to the future of the Internet was treated as a marginal topic, tolerated mostly because the UN Secretary-General at the time, Kofi Annan, insisted that it should be included.So what is a paper by the Director-General of the European Broadcasting Union, the largest association of public service broadcasters in the world, doing in this book, in which most of the contributors are prominent experts and institutions specialized in the Internet or with a background in telecoms? I can provide some simple answers to this question, the ones we and our members have identified over the past few years, since the digitization process started in broadcasting at turn of the new century.

A TECHNICAL ANSWER

According to European Union forecasts, 93 percent of UK households will be connected to a digital network by 2009[3]. However, at the end of 2005 only 16 percent of them were connected via telecom lines ("broadband")[4]. The rest were connected (and nobody can predict for how long) via broadcasting

[1] With Giacomo Mazzone, the EBU interface with the IGF

[2] Member of WBU – World Broadcasting Unions

[3] SOURCE: Datamonitor research for EC, 2005

[4] SOURCE: ITU Digital Life book, 2006

tools i.e. satellite, terrestrial, or cable TV. This means that, even in the richer countries, broadcasting will remain for many years to come the access portal to the digital world, with the same tools and habits as today.

A SOCIAL ANSWER

In developing countries the situation is even more complicated, because Internet penetration still remains very poor while TV and, more than any other media, radio are present in virtually every home. We call this the 'world digital divide' and our members are committed to fighting it throughout the world. But this phenomenon is already causing a barrier within the populations of the rich countries where digitization is progressing very fast. We call it the 'inner digital divide', where citizens are divided between those who have access to the digital world, and those who do not.

In this latter social group you not only find the poorer sectors of the population (those that cannot afford a cable or broadband subscription – at least 20 percent of the population according to some estimates) but also the elderly and those with poor computer skills (who do not feel at ease with computers). Altogether those excluded from the digital revolution represent half of the population of the richer countries. By 2012 –when analogue TV will finally be switched off in most of the EC, and certainly in the UK, the only interface to the information society for 50 percent of the population will be digital TV and radio. In developing countries, that percentage will be higher and will remain so for longer.

A MARKET ANSWER

As soon as any medium goes digital, its main marketplace also tends to become the digital world, and especially the Internet.

This has happened with letters (replaced by SMS messaging and e-mails). It is happening with music (with online sales and peer-to-peer gradually replacing CD sales); the same will happen soon for newspapers and one day also for movies and broadcasting. The arrival on the market of Joost and Babelgum is a sign that this day is closer than people may think.

So broadcasters are preparing themselves for a revolution in which the traditional flow of programmes (the ‘river’ model: somebody at the source decides the stream, content and the speed) will be gradually replaced by the simultaneous availability of as many programmes as users want (the ‘lake’ model: many sources will make all programmes always available to all users, anywhere and via any means)[5].

In this new world, many of the current foundations of the broadcasting economy will be rocked and overturned:

1. The mass audience will disappear, except for some ‘live’ events. This will erode the funding model based on quantitative advertising.
2. There will be greater pressure on broadcasters’ and publishers’ resources as the quantity to be delivered increases, and the quality tends to decrease as a result.
3. The independence of the media economy from other economic interests and from governments will be under threat, with possible repercussions for freedom of expression, the concentration of sources, and ultimately information reliability.

These three considerations have convinced the EBU, together with the six other existing broadcasting unions around the world (ABU in Asia-Pacific, NABA in North America, ASBU in Arab-speaking countries, CBU, AIB-IAR and OTI in Central and South America), to take an active part in the debate of the Internet Governance Forum under the auspices of the United Nations.

Future governance of the Internet (whatever it will be, whenever it will come into force, whoever will be asked to do it) will require:

- new rules to be established, before broadcasting is integrated into the Internet, to ensure at least the same level of protection that current national (and international) broadcasting legislation grants to citizens;

[5] As defined by Christian Nissen in Public service broadcasting in the new online territory

- a new contract to be written between citizens and public service broadcasting to continue the mission to 'inform, educate and entertain' even in the new digital world;
- guidelines for globalizing the media, to be introduced as soon as possible, to protect and preserve cultural diversity, promote intercultural dialogue and social cohesion, and expand freedom of expression and respect of human rights as universal, common and shared values.

BROADCASTERS' CONTRIBUTION TO THE IGF

Having said this, broadcasters (and the unions representing their employees) can make a huge contribution to the current debate at the IGF.

On access, for instance.

- As digitization (at least in many countries of the world) will occur via digital TV networks rather than through the Internet, there is a need to prepare citizens for the new information society, which uses broadcasting as an interface. Both media literacy and Internet literacy must be included in the PSB mission globally and must be considered as national priorities when broadcasting licenses are assigned or renewed or spectrums are re-allocated;
- Peer-to-peer technologies must be implemented to drastically reduce the cost of distributing content of common interest to many, without paying the current 'one-to-one' connection costs. This will allow us to recreate a simulcasting environment on the Web and use major events that only broadcasters know how to handle (Olympics, Eurovision Song Contest, Live Aid) to bring more and more citizens into the digital world;
- In developing countries, where only radio can reach 100 percent of the population, new communication and interactivity tools must be built around the radio broadcasting model (and its possible interaction with mobile phones) to facilitate the introduction of the digital era;
- Broadcasting is one of the most effective tools in fighting the digital divide between developed and developing countries, and even more importantly, within countries between older

and less skilled people and the Internet generation and affluent families. In doing so, public service media will provide access for marginalized and vulnerable groups of society, including older people and the disabled.

ON DIVERSITY

If you look at the top ten most visited websites in each country, you will usually find the usual suspects (search engines, etc.). But if you exclude international sites, the top positions will always be electronic and print media websites . This means that the best and most successful sources of ‘identitarian’ cultural products on the Internet are national broadcasters and newspapers or magazines.

These media (especially in public service) are there specifically to:

- Publish and protect locally developed content, including content that is not commercially viable. EBU members’ schedules currently contain an average of over 70 percent content that is produced in-house[6]. And even the other programmes are mostly made by national producers, with only a small percentage coming from the world market.
- Enhance the role of audiovisual communication in promoting local content: local and regional channels and programming are an essential part of the public service offer. In Europe alone there are 378 regional TV channels (and a lot more radio stations) in 38 countries[7]. But most of them do not yet have the money to make their content available on the Internet.
- Develop multi-lingual content, including content in indigenous and minority languages: regional and local channels include all channels for ethnic and language minorities, which are exclusively produced in Europe with public funding by the public service sector.
- Advance the role of the Internet in reducing illiteracy and providing accessible content for people with disabilities: in the

[6] SOURCE: EBU Guides vol. 3 : EBU Members ' TV programming, 2006

[7] SOURCE CIRCOM Regional website : www.circom-regional.org

UK a new Royal Charter asks the BBC to subtitle, dub or provide audio description for 100 percent of its programmes before 2009. Other governments have made similar requests of their national broadcasters. This will soon make an enormous amount of content available to disabled people, which in future could be made easily accessible on the Internet.

The public service media will never give up the above missions, because their raison d'être is precisely the production of material reflecting the cultural identity of a country, language, region, or community. So the best way to ensure cultural diversity even in the future Internet world is to encourage traditional broadcasters (which have a special relationship with their audience) to place their content and know-how on the Internet as soon as possible. In countries where this is not yet allowed, and this unfortunately includes some EU countries, barriers should be immediately removed.

ON OPENNESS

- Freedom of expression and the role of government to protect it.
- Privacy and freedom of expression.

Public service media have always been strongly committed to achieving both these targets. In addition, nation states, the European Union and Council of Europe require pluralism, impartiality and support for freedom of expression from all broadcasting stations in Europe[8], even if these principles are not necessarily implemented everywhere to the same degree. The level of information and respect for others' opinions , are usually ofa high standard. However, such standards are unfortunately not yet established and accepted throughout the Internet world.

This is an issue of great concern to all broadcasters and journalists that work for public service channels all globally. Recent

[8] See all documents and recommendations of the Council of Europe on the duties of public service broadcasting in the digital era on their website: http://www.coe.int/T/F/Droits%5Fde%5Fl%27Homme/Media/

examples have shown us that a very high standard is required of journalists working in traditional media (e.g. the Gilligan case in the UK and its consequences for the BBC), whereas bloggers and producers of user-generated content can disregard rules of impartiality and the quest for truth. This is not a moral judgement, but simply an acknowledgment of a problem we all have to face and that public service broadcasters want to help analyze and resolve.

The Internet Governance Forum debate aims to find ways for ‘citizen journalism’ and those producing user-generated content to adopt the fairly high standards of the traditional media as a common standard. This battle is crucial to the future of the Internet. For that reason, EBU/WBU together with the Council of Europe, the International Federation of Journalists and the civil society body Panos Org which specializes in media, will organize a workshop at IGF 2007 under the heading Quality and the Internet: Using and Trusting Internet Web Content, to discuss user-generated content and citizen journalism, their reliability, and the protection to be extended to Internet journalists under the existing laws (the right to protect sources, application or not of defamation and rectification laws, etc.).

ON SECURITY

As the new European Union Directive on Audiovisual Media Services states, the protection of minors and the respect of privacy should be two pillars of every broadcaster's policy. A large number of measures and recommendations have been drawn up in many forums by public and private broadcasters over the years. As a result, this protection in the broadcasting world (at least in Europe) is quite high and such measures could be adopted as a standard for other media, including the Internet.

Most of the results can be obtained via self-regulation, and the association of the various players in the media field plays an essential role in the enforcement of these rules. National control authorities are also strongly involved in monitoring their correct implementation.

The experience gained from years of discussion about the boundaries between the public interest, the public and private spheres in broadcasting and printed media can represent a very useful tool in future regulation of the Internet and of the information published or accessible through it.

CONCLUSIONS

Public service obligations such as:

- serving the individual citizen
- sustaining and defending national culture and cultural diversity
- fostering the democratic processes
- enhancing social, political and cultural cohesion
- serving as a civic ‘market place of modern society’[9]

can find new and more poignant application in the new Internet world.

To facilitate this, existing national rules need to be amended to include the new platforms (and especially the Internet) in the public service remit throughout the world.

To make this possible, new rules need to be introduced at a supranational level and for more than the existing world regions (as we know in Europe today). How (mainly through self-regulation of the various players?), when, and with which tools are questions to be answered by the Forum. Public service broadcasters are eager to join in the debate and in implementing any decisions that may be taken. The world’s broadcasters, conscious that they are currently the only ones able to reach the entire global population, are prepared to contribute to constructing the information society of tomorrow.

Together with the Internet community, we are here to build bridges that will bring the citizens of the whole world to a new environment, where the protections they are granted today in the analogue world (in terms of privacy, reliability, security, access, tolerance, etc.) will not be decreased or weakened but, if possible, increased and be made even stronger.

References:
www.ebu.ch
www.worldbroadcastingunions.org

[9] As defined by Christian Nissen, op cit.

Deploying Internationalized Domain Names (IDNs)

David Maher, Ram Mohan & Philipp Grabensee,
Afilias Limited

The success of the Internet is largely dependent on its interoperability: users know that, when they type a domain name, they will get consistent results, no matter what client they are using. The world's Internet population crossed one billion users in 2005 (Computer Industry Almanac 2006). North America and Europe lead the world in the spread of information and communication technologies (ICTs), followed closely by Asia. According to Internet World Stats 2006, 69 percent of the North American population, 38 percent of the European population, and about 10 percent of the Asia Pacific population access the Internet, with China, Japan and South Korea having comparatively high Internet penetration in Asia. IDNs are a vehicle of inclusion for communities worldwide, and are a requirement for true closing of the digital divide. This paper is based on the belief that further development of IDNs should be global in scope and should be applicable to all peoples and all languages. Of the estimated 6,800 languages spoken in the world today (UNESCO 2004), none except those languages that can be represented by plain 7-bit ASCII encoding are actually available as domain names. Most Internet domain name addresses encoded in plain ASCII are in the English language. As the world's Internet population expands, such an insular approach does not serve the world's population.

Generic Top Level Domains (gTLDs) and many country code Top Level Domains (ccTLDs) have become globally recognized brands as a result of the availability and dependable accessibility of the Internet, powered by global standards and common resolution. Users have an expectation of ubiquitous yet coherent worldwide resolution of gTLDs and have grown accustomed to consistency in registration and resolution processes. Regardless of the continent, computer or application from which a user accesses a TLD, users expect and deserve a similar, consistent and coherent experience at the level in the DNS where actual resolution, propagation and delegation of domains occur.

Currently Web access requires typing a Web address (also called domain name or URL) in English. For populations who do not understand English, this is one significant hurdle in accessing online content. Web addresses, which are the key to entering the multilingual World Wide Web, should also be in local languages. ICANN is responsible for the global coordination of Web addresses[1], and it has recently introduced Internationalized Domain Names (IDN) through the reports RFC 3454, 3490, 3491, and 3492, collectively called the IDN Standards (ICANN 2006). IDN would allow Web addresses in local languages. However, due to the seven-bit ASCII based domain name system, Unicode cannot be used and multilingual IDNs are converted to ASCII Compatible Encoding (ACE) before the address is resolved. Still being debated is how to enable top level domains (TLDs) in local languages and who will control them (Butt 2006, Huston 2006). Due to this continuing controversy, independent systems have also been developed, for example by the Chinese Internet Network Information Centre (CNNIC). ICANN and IDNs are bound to play a critical role in making the multilingual Internet accessible. The launch of domain names in local languages requires the development of a robust dispute resolution policy that considers additions for IDNs and that has the ability to handle disputes for domain names in either ASCII or the native language representation evenly and equally. Moreover, because variants of one name may conflict with other names, a clear policy has to be developed to resolve such conflicts in a manner that is consistent as well as conformant to local laws.

[1] Administered through the support of IANA and Regional Registries (RIRs), e.g. APNIC for Asia Pacific.

EXCERPTED FROM THE PIR PRINCIPLES ON IDNs

Users have arrived at the reasonable conclusion that the operator of a globally resolving TLD registry can be trusted to deal with significant operational issues as they arrive in the domain; it is reasonable for them to expect the same comparable level and quality of service in all scripts that represent the same domain label worldwide.

If the implementation of IDNs is managed in such a way as to result in brand fragmentation, this will inevitably diminish public trust in all gTLDs and ccTLDs. We believe that this factor must be considered in order to avoid exposing registrants to the dangers flowing from a devaluation of the trust that has been built up in the DNS and the global single-root system.

Further, registrars and other distributors of gTLD and ccTLD registrations have implemented automated and standards-compliant systems that result in rapid and accurate domain name transactions. Should a gTLD or ccTLD be managed by different operators for each IDN representation, registrars and other distributors will have to build systems that connect to each of these separate entities for what is essentially the same string (albeit in different languages). This raises the prospect of confusion in terms of the identity of individual registries and the ability of users to understand with whom they are dealing when service questions arise.

In addition, there is a strong possibility of difficulties in dealing with problems that need to be addressed in a variety of representations and in an accountable manner.

1. Protect DNS Security and Stability

   As the Internet becomes ubiquitous, nothing is more critical than ensuring the protection of the security and stability of the DNS.

   The selection of registry operators to manage the gTLDs was made with explicit evaluation of the capability of the operator to handle DNS security and stability issues in an expert manner. With respect to the country code top level domains (the ccTLDs), ICANN and its IANA function regularly review the security and stability of requested changes by ccTLD operators prior to making such changes in the root – a necessary safety precaution whose value has been proven time and again. In addition, there are industry expectations as to the operator's achievement of service levels, the operator's ability to scale to accommodate significant growth of the TLD, and the operator's ability to handle attacks that threaten to compromise the security or the stability of the TLD.

The existing registry operators are in a unique position to respond swiftly and appropriately to numerous security and stability issues because of their investment in systems, structures, processes and people who have gained expertise in resolving problems. Should the management of registries for the same domain in various IDN representations be entrusted to different organizations, then concerted and uniform response to security and stability threats could be so difficult as to be almost impossible.

2. Minimize Regulatory Burdens

The appointment of new registry operators for existing gTLDs or ccTLDs in other IDN representations risks subjecting them to parochial regulatory restrictions, and a likelihood of slowing the natural expansion of the DNS required to accommodate the multilingual interests of the peoples of the world.

One of the secrets of the Internet's success has been its growth and expansion generally free of undue regulatory burdens imposed by governmental and intergovernmental authority. It should be a primary goal of policy development for IDNs to recognize that multiple jurisdictions asserting regulatory authority over the same TLD in different IDN representations would hinder and not help the expansion and utility of domain name system.

In addition, a single regulatory jurisdiction offers other advantages, some of which are enumerated below:

a: Simplification of contact by law enforcement authorities

b: Single source of information for users,

c: Uniformity and established relationships with users.

The Internet is a crucial engine for economic growth and free speech. The Internet remains open to innovation and progress due to the existence of a system free of conflicting regulatory burdens.

3. Foster a Balanced Approach to Intellectual Property Protection and Dispute Resolution

   The uniform application of guidelines providing a consistent process for Intellectual Property protection and dispute resolution is necessary for all users of the Internet.

   Intellectual property challenges have always been present in the DNS and are likely to become even more complex in IDN representations of domain names. The Uniform Dispute Resolution Policy adopted by ICANN for the resolution of domain name - trademark disputes should be extended and modified as necessary to cover IDNs.

   Uniformity is an essential element of this policy. The adoption of different dispute resolution procedures for the same TLD in different IDN representations would seriously compromise public trust in trademarks and brand names and inevitably lead to consumer confusion. All users of the Internet are entitled to the benefits of a balanced and uniform approach to the protection of intellectual property.

4. Maintain Consistency with Proven Internet Guiding Principles

   The IAB (Internet Architecture Board) has provided significant relevant guidance for the DNS in the following RFCs from May of 2000:

   RFC 2825: A Tangled Web: Issues of I18N, Domain Names, and the other Internet Protocols; and

   RFC2826: IAB Technical Comment on the Unique DNS Root.

   In RFC 2825, two statements provide useful guidance:

   1) "…solutions must not cause users to become more isolated from their global neighbors even if they appear to solve a local problem."
   2) "One aspect of the challenge is to decide how to represent the names users want in the DNS in a way that is clear,

> technically feasible and ensures that a name always means the same thing." [emphasis added]

One of the significant challenges of implementing IDNs is to avoid fragmenting the Internet and isolating users. A key means of avoiding this problem is to allow all manifestations of a given top level domain to be managed by a single entity. This simple solution will also address the second issue: ensure that each TLD name always means the same thing.

In RFC 2826, the IAB wisely observed that: "Effective communications between two parties requires two essential preconditions:

- The existence of a common symbol set, and
- The existence of a common semantic interpretation of these symbols. [emphasis added]

Failure to meet the first of these conditions implies a failure to communicate at all, while failure to meet the second implies that the meaning of the communication is lost."

Further, the IAB says: "Names are then constant symbols, whose interpretation does not specifically require knowledge of the context of any individual party."

Most, if not all, existing TLDs have achieved a "common semantic interpretation" with the result that most Internet users are accustomed to a consistent interpretation, or meaning, of a TLD on the Internet.

Importantly, RFC 2826 goes on to say:

"Since the DNS is hierarchically structured into domains, the uniqueness requirement for DNS names in their entirety implies that each of the names (sub-domains) defined within a domain has a unique meaning (i.e., set of DNS records) within that domain. This is as true for the root domain as for any other DNS domain. The requirement for uniqueness within a domain further implies that there be some mechanism to prevent name conflicts within a domain. In DNS this is accomplished by assigning a single owner or maintainer to every domain, including the root domain, who is responsible for ensuring that each sub-domain of the domain has the proper records associated with it. This is a technical requirement, not a policy choice." [emphasis added]

> Insofar as .ORG in different scripts is considered the "same domain," RFC 2826 appears to require that it be managed by a "single owner or maintainer." To the extent that .ORG in different scripts is considered a "different domain," ICANN should establish an equitable and transparent process for evaluating both the value of a new domain as well as its prospective management.
>
> Another well accepted principle, the "Principle of Least Astonishment" also dictates that TLD's be managed in the most consistent manner possible so as to lead to the least confusion. Under the IAB principles outlined above, a "common owner or maintainer" is the likely best solution for this issue as well.

SUMMARY

Because community expectations for IDNs are high, it is crucial to introduce a technology that is compatible and interoperable with IDNA, but that will also address the needs of as many users as possible in the short term, even if all of their applications are not fully IDNA-aware and Unicode display and input capable. Few current Internet users have applications that are IDNA aware. Unless those users are accommodated in some way, there will be almost no adoption of IDNA-compatible IDNs. Despite the belief of some members of the IETF community that users will be happy using the ASCII-compatible form of IDNA names, experience has already started to demonstrate that users are unhappy about that approach and hence IDNs that can only be accessed through "punycode" are nearly worthless to the registrants except as protective registrations. Without some better transition strategy, there will be very little incentive for application programmers to add IDNA capabilities to their applications. IDNs are therefore subject to a "chicken and egg" problem, which presents a barrier to their adoption. If no broad strategy is forthcoming to help most users of IDNs, the likely result will be a patchwork of technologies that attempt to make IDNs work in some way for some subset of the Internet population. To forestall all of that, providers must work quickly to accommodate as many users as possible in a way that promotes interoperability throughout the standards.

Digital Opportunity, Digital Divide

Sarbuland Khan,
Executive Coordinator, Global Alliance for Information and Communication Technologies for Development (GAID),
New York

DIGITAL OPPORTUNITY, DIGITAL DIVIDE[1]

At the beginning of the twenty-first century, we are firmly entrenched in the twin ages of globalization and digitalization. We saw extraordinary technological innovation during the 1990s, including cheaper, more powerful computers; the explosion of the Internet and proliferation of broadband; and the tipping point of mobile telephony.

Despite progress in the diffusion of information and communication technologies (ICT) and innovations in technology and services, gaps in access to ICT remain large. Inequality persists both among and within countries. The International Telecommunication Union (ITU) estimates that some 800,000 villages – representing around one billion people worldwide – still lack connection to any kind of information and communication technology. More than half of those villages are in Africa. Other stunning statistics from the 2004 ICT World Telecommunication Indicators Database illustrate the gaping chasm between the technological haves and have-nots:

- There are roughly the same total number of Internet users (429 million) in the G8 countries -- home to just 14 percent of the

[1] This section draws upon the research and conclusions included in Information and Communications for Development 2006: Global Trends and Policies, World Bank: Washington D.C., 2006, as well as contributions by Tadao Takahashi (Brazil), member of the Bureau of the United Nations Information and Communication Technologies Task Force, and ITU statistics available on the World Summit on the Information Society website (http://www.itu.int/wsis/tunis/newsroom/stats/)

world's population -- as in the rest of the world combined (444 million Internet users).

- Less than 3 out of every 100 Africans use the Internet, compared with an average of 1 out of every 2 inhabitants of the G8 countries.
- The entire African continent – with more than 50 countries – has fewer Internet users than France alone.
- Denmark has more than twice the international Internet bandwidth than the whole of Latin American and the Caribbean combined.
- In 2004, there were still 30 countries with an Internet penetration of less than 1 percent.
- Africa has an average of 3 fixed telephone lines per 100 people.
- Of Africa's 26 million fixed lines, over 75 percent are found in just 6 of the 55 African nations.
- In 2004, Africa accounted for 13 percent of the world's population, but for only 3.7 percent of all fixed and mobile subscribers worldwide.
- The 14 percent of the world's population living in the G8 countries account for 34 percent of the world's total mobile users.

While these numbers demonstrate the present depth of the digital divide, over the past 25 years there has been a positive movement to connect the previously unconnected. In particular, there has been a significant increase in the number of individuals with access to telephones, with developing countries accounting for more than 60 percent of the world's telephone lines in 2005 – most of the growth coming from mobile telephones, which now outnumber fixed ones. Even poor households have been able to benefit from telephone access through prepaid services and calling cards.

ITU statistics show that in 2004 Africa had close to 100 million total telephone subscribers, 76 million of which were mobile subscribers. Africa's mobile cellular growth rate has been the highest of any region over the past five years, averaging close to 60 percent year on year. The continent has the highest ratio of mobile to total telephone subscribers of any world region.

Furthermore, estimates indicate that worldwide Internet use more than quadrupled between 2000 and 2005. A significant proportion of this increase can be credited to new wireless technology and associated business models, which have increased competition and accelerated the development of broadband infrastructure in rich and poor countries alike and have helped, in particular, to begin to connect the urban poor and rural communities with affordable yet commercially viable services.

ICT-FOR-DEVELOPMENT AND POLICYMAKERS[2]

Due to the successful advocacy of the World Summit on the Information Society (WSIS) process and the information and communication technology for development (ICTD) community, it is increasingly accepted that when applied strategically, ICT has the potential to increase growth in businesses of any size and in countries at any stage of development, thereby creating new sources of income and employment for the poor. ICT can reduce poverty by making a country's economy more efficient and globally competitive. In addition to reducing income inequality, such technology has the potential to improve health and education services, enhance social inclusion and promote more efficient, accountable, democratic government, especially when combined with freedom of information and expression.

This distinctive role in supporting sustainable poverty reduction is increasingly being recognized by the world's policymakers. A consensus is forming that it is crucial that ICT should move closer to the mainstream of development economics and policies, nationally, regionally and globally. However, movement in this respect has been slow.

Effective policymaking to redress the disparities is, in many cases, hampered by the limited availability of current data for most developing countries. Many governments lack adequate tools to monitor, evaluate and guide investments in ICT and connectivity in underserved areas. While the need for measurable, comparable indicators to track progress and benchmark

[2] This section draws upon the research and conclusions included in Information and Communications for Development 2006: Global Trends and Policies, World Bank: Washington D.C., 2006.

performance in building an information society has been recognized, agreement remains to be reached on which data should be compiled and benchmarked internationally and which organizations should be responsible for various indicators, such as on access, quality, affordability, efficiency and sustainability.

Among the biggest challenges to the integration and diffusion of ICT facing developing countries are insufficient policy and implementation capacity; opposition from vested interests; and persistent obstacles to the adoption of ICT, such as slow, unreliable and expensive telecommunication services, limited incentives to change business models and operating structures, lack of trust and legal impediments.

It is understood that governments have primary responsibility for the welfare of their citizens and must provide an enabling economic, political and social environment and, in particular, design and implement e-strategies to guide national development. Other stakeholders, however, have distinct responsibilities of equal importance to ensure that the benefits of ICT reach all women, men and children. As is reiterated throughout the WSIS documents, only through the international cooperation of governments and the partnership of all stakeholders will it be possible to succeed in our challenge of harnessing the potential of ICT as a tool, at the service of development, to promote the use of information and knowledge to achieve the internationally agreed development goals and objectives, including the Millennium Development Goals (MDGs), as well as to address the national and local development priorities, thereby further improving the socio-economic development of all human beings.

OVERCOMING THE GOVERNANCE DEFICIT THROUGH COLLABORATION

We are, then, in the midst of an age of paradox: the wealth generated with the integration of the world economy (largely thanks to new technologies, for instances, in ICT and transportation) is concentrated among few. The rest do not have access to that very same economy and technologies. And few of those "have-nots" will see a change in circumstance in the short to medium term without a significant shift in trajectory.

What is the reason for this significant inequality? There is a governance deficit at all levels. This is the result of the traditional approach to governance with players adhering to strict roles with limited cooperation: government creating and enforcing laws, private sector pursuing profit for shareholders, and civil society taking a peripheral role in influencing both government and business through the efforts of concerned citizens.

However, our new economy cannot be managed equitably without a grand collaboration of stakeholders. Networks of networks are needed to respond to the challenges and opportunities of an integrated world economy, make the benefits truly universal and have the risks shared by all. We need new models for such grand collaboration to manage the challenges of globalization in the digital age to universalize access and participation so that the interests of all stakeholders – not just a privileged few – are protected.

In an effort to trigger the necessary shift to more equitably share the benefits of globalization among the world's peoples, the United Nations responded through a series of conferences and summits held during the 1990s, including the International Conference on Financing for Development (Monterrey, Mexico) and the 2000 Millennium Summit (New York City, USA).

THE WORLD SUMMIT ON THE INFORMATION SOCIETY: AN INNOVATION

In 1998 at the ITU Minneapolis Plenipotentiary Conference, Resolution 73 proposed holding a World Summit on the Information Society with the aspiration of sharing the benefits of the IT revolution with all. ICTD programs had already begun to proliferate through various parts of the United Nations, and a strong ICTD community was developing among civil society. At the substantive session of the Economic and Social Council (ECOSOC) in 2000, a Ministerial Declaration on ICT and development[3] was released. In 2001, the G8 Digital Opportunity

[3] Development and international cooperation in the twenty-first century: the role of information technology in the context of a knowledge-based global economy, E/2000/L.9

Task Force (DOTForce) and the United Nations Information and Communication Technologies Task Force, were launched as multi-stakeholder platforms for advancing digital development in the developing countries.

Following extensive preparatory activities, the first phase of the WSIS was held in Geneva in 2003, attended by more than 11,000 participants from governments, the private sector and civil society. In the intervening two years, tremendous energy and resources went into the pursuit of advancing the WSIS agenda with the intention of demonstrating progress by the time the second phase would be held in Tunis in November 2005. The Tunis meeting drew more than 19,000 participants.

The WSIS was an innovation on a number of fronts. Its format – split into two phases, two years apart, the first hosted by a developed country, Geneva, and the second, a developing country, Tunisia – was an obvious deviation from past practice. The result was that the process delivered a novel framework within which to discuss complex issues and reach agreement in sensitive areas. Although it was an intergovernmental summit like the others, it enjoyed unprecedented participation of the private sector, non-governmental organizations and to a lesser extent, academia, media and foundations.

Moreover, it was truly a global process. Large numbers of regional and thematic events of all sizes and with diverse organizers were held before and during the Summits. Preparatory Committee meetings engaged all stakeholders – not just governments -- in the planning of the Summit structure and drafting of the outcome documents. Meanwhile, online interactive forums had proliferated to provide channels for discussion across a spectrum of topics prior to, between and following the two phases. Thousands of actors engaged in initiatives, capacity-building, research and other activities as contributions to the Summit. The result of all this was tremendous sustained focus on the subject, innovations in applications, and historic collaboration over the period of the Summit process.

Four outcome documents emerged from the two phases: the Geneva Declaration of Principles[4], the Geneva Plan of

Action[5], the Tunis Commitment[6], and the Tunis Agenda for the Information Society[7]. The Geneva phase had sought to develop a shared vision of an inclusive, people-centered, development oriented Information Society; the Tunis phase aimed to turn that vision into action.

The WSIS can claim some significant achievements: it shifted the discussion from a technology focus to a development focus; it demonstrated the power of bringing all key actors – government, business, civil society, academia, the technical community, and intergovernmental organizations – together around one table to address challenges collaboratively; and it created a new dynamic in which innovation and technology are now viewed as key levers to reaching the internationally agreed development goals.

The WSIS process helped sensitize the larger development community, which began to see ICT as a cross-cutting issue and of its potential as a strategic tool for the achievement of internationally agreed development objectives in a range of fields, including health, sustainable development and empowerment of women. The role of information and communication technologies and development was recognized in the Millennium Declaration (para. 20[8]) and in the 2005 World Summit Outcome Document (para. 60(g)[9]). While there is growing recognition of the importance of ICT at the policy level, the link between ICTD and the achievement of the United Nations development agenda needs to be operationalized in development practice and programs.

There is a tremendous opportunity for this to happen in the implementation and follow-up phase, during which United Nations entities are responsible for overseeing the 11 action

[4] WSIS-03/GENEVA/DOC/0004

[5] WSIS-03/GENEVA/DOC/0005

[6] WSIS-05/TUNIS/DOC/7

[7] WSIS-05/TUNIS/DOC/6 (rev. 1)

[8] 20. We also resolve: …To ensure that the benefits of new technologies, especially information and communication technologies, in conformity with recommendations contained in the ECOSOC 2000 Ministerial Declaration, are available to all.

lines[10] and specific targets. At the United Nations headquarters, the Secretary-General, the General Assembly, the ECOSOC, and its Commission on Science and Technology for Development have each been given specific responsibilities to follow-up.

However, in line with the multi-stakeholder make-up of the entire WSIS process, the Tunis Agenda placed a very strong emphasis on the need for all actors to play a role in the implementation and follow-up. Among the many references to multi-stakeholder cooperation, paragraph 80 states:

We encourage the development of multi-stakeholder processes at the national, regional and international levels to discuss and collaborate on the expansion and diffusion of the Internet as a means to support development efforts to achieve internationally agreed development goals and objectives, including the Millennium Development Goals.

All actors – governments, private sector and civil society – are expected to collaborate on the basis of their strengths and available resources to implement the outcomes of the Summit. All have a joint duty to maintain the momentum generated by the WSIS and to strive to have ICTD activities converge with the mainstream UN development agenda so that the international community can meet its commitments to the world's needy and marginalized within the 2015 time horizon.

[9] 60. We recognize that science and technology, including information and communication technology, are vital for the achievement of the development goals and that international support can help developing countries to benefit from technological advancements and enhance their productive capacity. We therefore commit ourselves to:

(g)Building a people-centered and inclusive information society so as to enhance digital opportunities for all people in order to help bridge the digital divide, putting the potential of information and communication technologies at the service of development and addressing new challenges of the information society by implementing the outcomes of the Geneva phase of the World Summit on the Information Society and ensuring the success of the second phase of the Summit, to be held in Tunis in November 2005; in this regard, we welcome the establishment of the Digital Solidarity Fund and encourage voluntary contributions to its financing.

[10] see: www.itu.int/wsis/implementation/index.html

GLOBAL ALLIANCE FOR ICT AND DEVELOPMENT

As one element of the United Nation system's contribution to the multi-stakeholder follow-up, on 28 March 2006, Kofi Annan approved an initiative called the Global Alliance for Information and Communication Technologies and Development (GAID). The Alliance was launched at an inaugural meeting held in Kuala Lumpur on 19-20 June 2006 with over 500 participants from all regions and stakeholder groups. It operates under the patronage of the Secretary-General and reports to the Economic and Social Council, which has been mandated to oversee the WSIS follow-up in the context of the implementation of and follow-up to the outcomes of major United Nations conferences and summits.

At the request of the Secretary-General, during the course of more than a year the United Nations ICT Task Force had undertaken consultations during meetings in Berlin, Geneva, France, Dublin, Shanghai and Tunis to establish the foundation for the new Alliance. Furthermore, regional consultations were held by some of the nodes of the Task Force, and online input was solicited through the Task Force website. In this way, GAID's principles and modalities were debated at length, taking into consideration the perspectives of many stakeholder groups.

GAID's mission is to contribute to transforming the spirit and vision of WSIS into action and promoting the use of ICT for the achievement of the internationally agreed development goals, including the Millennium Development Goals. It does so by providing an inclusive, multi-stakeholder global forum and platform for cross-sectoral policy dialogue and by enabling and catalyzing multi-stakeholder partnerships for action under the GAID umbrella. The Alliance provides multi-stakeholder input to intergovernmental bodies, including Economic and Social Council and the Commission for Science and Technology for Development.

It is structured as a decentralized network, open to participation of all stakeholders, including governments, business, civil society, academia and international organizations.

The Alliance aims to expand the circle of participants in policy and partnership debate beyond the traditional set of stakeholders, by actively engaging constituencies that currently are not adequately involved, explicitly: non-governmental participants from developing countries, media, academia, youth, and women’s groups. In building on existing initiatives and institutions and promoting synergy among them, the Alliance attempts to make extensive use of the latest web-based collaborative technologies thus minimizing the need for physical meetings.

The Inaugural meeting of the Alliance in Kuala Lumpur in June 2006 agreed that the Alliance will initially focus on the use of ICT in promoting the following four broad areas: 1) Education, 2) Health, 3) Entrepreneurship, and 4) Governance (enhancing citizens' participation and promoting accountability, transparency and efficiency in governance processes).

Activity within those areas, or those of a horizontal cross-cutting nature, take place predominantly via a limited number of flagship partnership initiatives and thematic Communities of Expertise. In addition, the regional networks and stakeholder networks may launch specific activities, while keeping the above focus areas in mind.

Over the course of the first year, GAID and its networking mechanisms undertook advocacy activities to keep ICTD high on the political agenda, organize or support thematic and/or regional meetings, training sessions and other events, including an annual Global Forum, with a view to contributing to global policy dialogue and building human capacity. Furthermore, GAID collaborates with other suitable entities sharing similar goals, including organizations engaged in the implementation of WSIS Action Lines, the United Nations Group on the Information Society (UNGIS) and the Partnership on Measuring ICT for Development, with a view to enhancing synergy of existing activities and to facilitating creation of new partnerships.

GAID presents an opportunity to build on past experiences and initiatives, including the DOT Force and UN ICT Task Force, and to engage wider participation from all stakeholder groups, across a number of sectors, from developing and developed countries, reaching out to marginalized groups, and inviting participation of policy-makers and practitioners alike.

ACHIEVING THE DEVELOPMENT GOALS -- TOGETHER

After the World Summit on the Information Society, a new stage of activity in Information Communication Technologies for Development is beginning. Indeed, there is discernible movement towards a convergence with so-called mainstream development, as it becomes evident that many of the internationally agreed development goals will not be met without a massive scaling-up of efforts. With its multiplier effects, ICT holds much untapped potential that can be leveraged. However, computer and telephone networks alone are not sufficient to attain the MDGs by 2015; that will require the deployment of human networks as well. The Global Alliance on ICT and Development can play catalytic role in ensuring that the international community – governments, civil society, intergovernmental organizations, private sector and others working together – can fully realize the potential of leveraging ICT for development to the benefit of all humanity, not just a privileged few.

It is not a challenge that governments can overcome alone; the private sector and civil society bring unique assets to the table. Intergovernmental organizations, such as the United Nations, catalyse innovation, both by providing forums and frameworks within which these parties can work together to achieve common visions and by synthesizing best practices and lessons learned, using the knowledge of the larger system.

GAID aims to do its share to maintain the momentum generated within the ICT for development community and broaden efforts through advocacy and partnership creation to raise awareness, educate, build capacity and generate sustainable full-scale action not only to ensure that all the world's people have access to a telephone or the Internet, but also to ensure that they, and succeeding generations, live healthier, better, more fulfilling lives.

Theme	Lead organization(s)	Partners
Better Connectivity with Broadband to Africa As a key enabler of the four priority areas, this initiative will support African efforts to accelerate the roll-out of communication infrastructure and increase broadband access. Economic growth in Africa will depend upon widespread access to ICT which in turn provides access to local, national, regional and global markets. Therefore, national and regional backbones, cross-border links, and rural connectivity need to be vastly expanded, in parallel with the deployment of applications to take advantage of connectivity for productive use.	ITU, World Bank	European Commission, the African Development Bank, the E-Africa Commission/ NEPAD, bilateral and multilateral donor organizations, telecommunications operators associations, and representatives of users and civil society
telecentre.org Building on the existing telecentre.org program, this GAID initiative will promote a more inclusive digital world by helping telecentres become stronger, more sustainable and more numerous. The aim is to move beyond simply providing access to also include elearning, training, skills development, local content generation, financial services, e-government and others services relevant to the local community. Partners will work in four areas: 1) building telecentre networks; 2) developing content and services; 3) documenting knowledge and learning; and 4) convening events for telecentre leaders.	IDRC (Canada)	Microsoft, SDC, GKP, Inter-American Development Bank, network and knowledge-sharing partners at the national and international levels

Theme	**Lead organization(s)**	**Partners**
Cyber Development Corps The initiative promotes capacity building through South-South cooperation and will establish a global outreach program based on the spirit of volunteerism to help lesser-developed nations and communities benefit from global ICTs, infrastructure and resources; and help enhance their national development plans towards becoming equal participants in the global information-knowledge society.	Ministry of Science, Technology and Innovation (Malaysia)	UNDP, UNCSTD, telecentre.org, Philippines Resources for Sustainable Development, Inc., Islamic Development Bank, Digital Opportunity Trust, Microsoft Malaysia

FLAGSHIP ADVOCACY INITIATIVES

Theme	**Lead organization(s)**	**Partners**
Global Initiative for Inclusive Information and Communications Technologies This initiative will (1) promote ICT solutions for people with disabilities and related best policy practices among governments in the context of the new UN Convention on the Rights of People with Disabilities and expanded member states legislations and regulations, and (2) accelerate the development by industry and civil society of the scientific, industrial, standardization and economic conditions to make such solutions affordable worldwide.	Wireless Internet Institute and World Times, Inc.	United Nations Department for Economic and Social Affairs (UN/DESA), UN Enable, IBM, UNITAR, Air France, NIIT, Georgia Institute of Technology and additional private sector participants

Theme	**Lead organization(s)**	**Partners**
Free Access for all Schools to the Internet Schools are particularly fertile grounds to foster the development of a new generation in the global knowledge society. Efforts to connect societies and people to the Internet are in the making; however, no systematic effort has been undertaken to connect all schools to the Internet. GAID will provide the umbrella for the campaign to mobilize support for this initiative and help find innovative financial solutions to avoid the cost burden for schools.	Swiss Development Agency	ITU

COMMUNITIES OF EXPERTISE

Community of Expertise	**Lead organization(s)**
Governance cluster	
E-governance for Development	DPADM, UN/DESA
E-services for Development	Observatory for Cultural and Audiovisual Communication
Information and Communication Technologies for Peace	ICT4Peace Foundation
Entrepreneurship cluster	
ICT Policy and Finance for Social, Community and Public Entrepreneurship	Association for Progressive Communications (APC)
Expanding Financial Services to the Un/Under-banked	Intel Corporation
Enterprises' Competitiveness through the use of ICTs	ILO, ICC, UNCTAD

Community of Expertise	Lead organization(s)
Education cluster	
ICT Competencies for Teachers	UNESCO
Enhancing Access to and Application of Scientific Data in Developing Countries	Chinese Academy of Science
Beyond Distance Research	Leicester University
ICT for Education	Talal Abu Ghazaleh Companies
ICT Integration and Pedagogical Engineering	WITFOR Education Commission
Health	
ICT for Country Health Strategies	WHO
Rural development	
E-agriculture	FAO
Gender cluster	
Gender, Development and Information Society Policies	IT for Change
International Taskforce on Women and ICT	Centre for Women and Information Technology
Youth	
Youth Social Technopreneurship	Philippine Resources for Sustainable Development
Local content	
e-Content and Creativity – World Summit Award and Network	International Centre for New Media

Chapter 4

Security

The Need for a Global Framework in Response to Growing Challenges in Cybersecurity

Dr. Hamadoun I. Touré,
Secretary-General of the International Telecommunication Union (ITU), Geneva

We are engaged in a fierce battle – a battle for the future integrity of the Internet. From its origins as a private, secure defense research network, the Internet has grown to transform modern life as we know it. The total number of Internet users surpassed one billion in 2006 and continues to grow at an astounding rate, nearly trebling from 390 million Internet users in 2000 to reach 1.13 billion Internet users by the end of 2006. And yet, the very growth and future potential of the Internet are in danger from growing threats and cyberattacks. By some estimates, spam now accounts for 90 per cent of all e-mail traffic and has reached such critical volumes that experts are warning that spam and other related threats could paralyze the Internet. Unless there is progress in building confidence and security in the use of ICTs, users' diminishing trust in the Internet will limit its growth and transforming potential. Perhaps, we should not be celebrating the unrivalled growth of the Internet – perhaps our true concern is whether the Internet's potential for growth is being undermined by cyberthreats.

Threats in cyberspace deserve increased attention for several reasons. The Internet began as a closed network with a limited number of trusted users, which meant that user authentication was originally not an issue. In today's open Internet, where anyone with access to an Internet café can log on, online identity (and online anonymity) is a key issue. The growth of the

Internet has opened up many more opportunities for criminals to exploit online vulnerabilities and to commit cybercrimes and attack countries' critical infrastructure. Furthermore, the constant evolution in protocols means that the protocols and algorithms used to secure Internet transactions are successively compromised and replaced, in the constant tug-of-war of human ingenuity. We have reached a point where no sooner is a new device or technology introduced than hacker websites spring up to exchange ideas and approaches seeking to compromise the new technology. Hacking is increasingly a "criminal profession", with more and more attacks being carried out by criminals with a profit motive. Toolkits and applications for phishing, spam, malware, scareware and snoopware can today be acquired relatively easily from underground sites or even purchased legally, lowering the financial and intellectual entry barriers to acquiring tools which facilitate unauthorized access to information and communication systems in a bid to manipulate or destroy them. The evolution of telecom networks towards Next-Generation Networks (NGN) may make networks more vulnerable, through the decentralization of intelligence to the edges of the network. All these trends mean that we have now reached a critical stage in the development of the Internet, a stage where its future growth and potential are in jeopardy.

Defining "cybersecurity" and the threats to security is no easy task, given the different interpretations of the broad concepts of "cyber" and "security" and the different terms in use for these concepts in different countries. In order to reach a common understanding on what cybersecurity and cybercrime mean to member states, ITU established a Council Working Group in 2006 to study definitions and terminology relating to building confidence and security in the use of ICTs.

Viruses, spyware, phishing, identity theft, zero-day exploits, Denial of Service (DoS) attacks, zombie botnets, and other attacks and vulnerabilities are now commonplace. From being considered as annoying nuisances, spam and cyberthreats have evolved into something more menacing, with the ability to wreak havoc on our networks, as well as the data and information transmissions they carry. Cyberattacks can now occur anywhere and at any time, and can cause massive damage in a short space of time. The almost completely global availability of the Internet means that a hacker operating from a country anywhere in the world can use computers to attack government sites of any other country. Another trend widely observed is that hackers are moving from a central command-and-control model to a peer-to-peer model with a distributed command structure for controlling botnets (or networks of compromised computers) across different countries. Countries can no longer close their borders to cyberattacks. These attacks are very difficult to guard against, whilst the legal framework fails to keep pace with technological developments. Cyberthreats have become an international problem, requiring a coordinated international response. Many countries have adopted or are working on legislation to combat cybercrime and other misuses of information technology. These laws are drawn up so as to be enforceable in well-defined national or regional geographical boundaries. Other countries are setting up agencies to oversee the protection of their critical infrastructures by monitoring cyberattacks and coordinating emergency responses. Others again have launched awareness campaigns to raise user awareness and are working with the private sector on technical solutions. However, such national and regional initiatives cannot cope with an increasingly global problem. Cybercriminals cannot be easily extradited from the country where the cybercrime was instigated to the country where it was committed unless legal frameworks are interoperable. This is far from the case today. To deal with such an international problem, an international framework is needed for countries to respond in a coordinated way.

At the World Summit on the Information Society (WSIS), world leaders and governments appointed the ITU as the sole focal point and facilitator of Action Line C5 on “Building confidence and security in the use of ICTs”. ITU has a long involvement in security issues and has already achieved notable successes in the field of security standards for ICT networks; one of the most important security standards in use today is X.509, a recommendation developed by the ITU Telecommunication Standardization Sector (ITU-T) for electronic authentication over public networks and the definitive reference for designing applications in Public Key Infrastructure (PKI). The elements defined within X.509 are widely used in everything from securing connections between a browser and web server to providing the digital signatures that enable electronic transactions to take place. Standardization and standards institutes build user confidence by establishing clear standards and guidelines for risk management, as well as ensuring that these standards are met (e.g. in norms, trading standards and quality certification). With its long experience of work in telecommunication standards, ITU is ideally positioned to work on security standards and both the ITU-T and ITU Radiocommunication (ITU-R) sectors have carried out significant work in security architecture, encryption and authentication and information security management systems.

The ITU Telecommunication Development (ITU-D) sector is working to develop national cybersecurity capacities through a focused programme of technical assistance and workshops for developing countries. ITU-D is developing a Report on Best Practices for a National Approach to Cybersecurity. This report suggests guidelines for governments to formulate national strategies for cybersecurity and Critical Information Infrastructure Protection (CIIP). It identifies key elements including:

- developing a national cybersecurity strategy
- establishing national government-industry collaboration
- creating a national incident management capability
- deterring cybercrime, and
- promoting a national culture of cybersecurity.

ITU-D has also developed several toolkits to help countries assess their national cybersecurity readiness, as well as a framework for establishing watch, warning and incident response capabilities. These issues are being explored through a series of workshops in different countries.

Addressing today’s challenges of cybersecurity goes far beyond work in standards and national capacity-building, however – a comprehensive approach and coordinated response mechanism is needed for dealing with cyberattacks at regional and international levels. Because attacks on isolated countries can cause damage far beyond national boundaries, an international framework is needed. This is the need that ITU proposes to fulfill with its pioneering new initiative, the Global Cybersecurity Agenda (GCA). Alongside partners from governments, industry, relevant regional/international organizations, research institutes, academic institutions and individual experts, ITU has established a global framework for dialogue and international cooperation aimed at proposing strategies for solutions to build confidence and security in the use of ICTs.

The Global Cybersecurity Agenda will unite existing initiatives and partners with the objective of proposing global strategies to address today's challenges in the fight against cybercrime and to maintain cyberpeace. The ultimate aim of the Global Cybersecurity Agenda is to make significant progress on the agreed goals in the fight against cybercrime through a coordinated international framework. It is based on international cooperation, and strives to engage all relevant stakeholders in a concerted effort to build security and confidence in the information society.

The Global Cybersecurity Agenda is based upon five strategic pillars:

1. Legal Framework
2. Technical Measures
3. Organizational Structures
4. Capacity Building
5. International Cooperation

The legal framework, technical measures and organizational structures need to be undertaken at national and regional levels, but also harmonized at the international level. The last two pillars, capacity-building and international cooperation, cut across all areas. Through the GCA, ITU will fully engage its member states and all the world's players in its activities. It will collaborate closely with its partners to identify current challenges, consider emerging and future threats, and propose global strategies to meet the goals of the agenda.

In order to assist ITU's Secretary-General in developing strategic proposals to member states, a High-Level Experts Group (HLEG) has been established to propose strategies in all five work areas or pillars. The HLEG unites experts from governments, industry, relevant regional and international organizations, research institutes, academic institutions and individual experts from around the world, designated by the ITU Secretary-General.

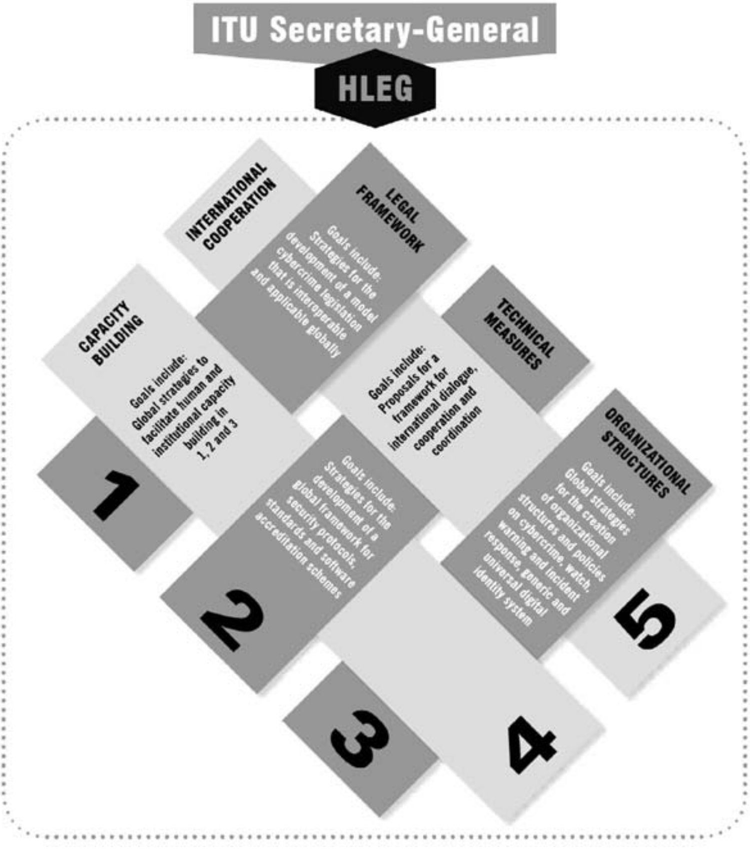
This HLEG will propose strategies for the seven main goals on the Global Cybersecurity Agenda:

1. Develop model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures
2. Create appropriate national and regional organizational structures and policies on cybercrime
3. Develop globally accepted minimum security criteria and accreditation schemes for software applications and systems
4. Develop strategies for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives
5. Develop strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries
6. Develop a global strategy to facilitate human and institutional capacity building to enhance knowledge and know-how across sectors and in all the above-mentioned areas
7. Draw up a framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

Through its 191 member states and more than 700 sector members and associates, ITU is uniquely placed to seek consensus on a framework for worldwide cooperation in cybersecurity. ITU is a pre-eminent forum where diverse views on cybersecurity and cybercrime can be discussed, with the goal of arriving at a common understanding amongst all concerned parties as to how these issues can best be addressed at the international level. Such an international framework is sorely needed at a time of growing uncertainty in the size, scale and scope of cyberthreats. Only by establishing an international framework promoting cybersecurity can we hope to have any prospect of cyberpeace.

GLOBAL CYBERSECURITY AGENDA

A FIVE-PART PLATFORM



ITU Secretary-General

HLEG

INTERNATIONAL COOPERATION

LEGAL FRAMEWORK

Goals include: Strategies for the development of a model cybercrime legislation that is interoperable and applicable globally

CAPACITY BUILDING

Goals include: Global strategies to facilitate human and institutional capacity building in 1, 2 and 3

TECHNICAL MEASURES

Goals include: Proposals for a framework for international dialogue, cooperation and coordination

Goals include: Strategies for the development of a global framework for security protocols, standards and software accreditation schemes

ORGANIZATIONAL STRUCTURES

Goals include: Global strategies for the creation of organizational structures and policies on cybercrime, watch, warning and incident response, generic and universal digital identity system

The Future of the Internet Economy

Pier Carlo Padoan,
Deputy Secretary-General, Organisation of Economic
Co-operation and Development (OECD)[1], Paris

The Future of the Internet Economy will be the subject of the first OECD Ministerial meeting ever hosted in Asia. Taking place in June 2008 in Seoul, Korea, it will examine the implications of the rapid growth in use and reliance on the Internet for our economies and societies. Ministers from OECD as well as many non-member countries, together with all other stakeholders, will strive to articulate a collective vision of a desirable future economy and society supported by the Internet.

Realising this vision will, more than ever, require action by all stakeholders and cross-border co-operation, which is at the heart of the OECD's mission. That is why we, and our member countries, view co-operation with the Internet Governance Forum (IGF) as an increasingly important element of our work. This article previews the forthcoming OECD Ministerial meeting and our contributions to IGFs from Athens to New Delhi.

A DECADE OF CHANGE: OTTAWA TO SEOUL

In 1998, as the Internet was first emerging as new force in shaping our economies and societies, the OECD convened a Ministerial Conference on E-Commerce in Ottawa, Canada. This established the strategic direction of policies in areas such as privacy, security, taxation and consumer protection, that have been instrumental in nurturing online activity and helping to make it part of our daily lives. The Ottawa Ministerial was prominent in recognising that, in order to be effective, policies surrounding the Internet required co-operation across all stakeholders. In gathe-

[1] The views in this article are those of the author and may or may not reflect those of OECD member countries.

ring leaders from government, business, organised labour and civil society, and in achieving a large measure of consensus on the best way forward, this meeting laid the foundation for a decade of policies which have proven remarkably successful. That being said a great deal of "Internet time" has passed since the Ottawa Ministerial. Back then, Google was a one-month-old company operating in a garage with just three employees. Other fledgling ventures, such as Amazon and eBay, have gone on to become successful mainstream companies, and new services, such as iTunes or Skype, are used by millions of people around the world. The network's infrastructure has also fundamentally transformed since Ottawa. Dial-up Internet access has given way to always-on broadband technology. Increasingly, Internet access is routinely undertaken via all manner of wireless devices. In the future, the network of networks will continue to evolve reaching further into our daily lives and into other infrastructures upon which we rely. Microchips and sensors, for example, will process all manner of information from what is in our shopping baskets to water quality in our reservoirs and all this information will be tied together by the Internet. The poster child application of the Internet – the World Wide Web – has also been transformed over the past decade. Levels of user participation and publication are historically unprecedented from blogs, podcasts and wikis through to services such as Flickr, and YouTube. Social networking sites such as Bebo, Facebook and MySpace represent another rapidly developing frontier of communication. The creativity and innovation being fostered in these domains is impressive but so too are the daunting challenges for privacy in an Internet-centric world. The rapid evolution of the Internet has vastly raised the capabilities of those with malicious or fraudulent intent. Today's Internet is a venue for increasingly severe and sophisticated attacks on consumers, business and online government. This demands greater co-operation between all stakeholders, and action across policy domains from education to law enforcement. The task of managing and protecting our online identities and personal information is one of the most pressing issues facing policymakers. Doing so in a global Internet economy is even more challenging.

AN INFRASTRUCTURE CRITICAL FOR OUR ECONOMIES AND DAILY LIVES

As a starting point, the OECD Ministerial meeting will assume that the Internet now fundamentally underpins all our economies and societies. Our reliance on the Internet for commercial and social activity is increasing, along with its growing role in delivery of key services, such as health and education. New forms of usage have also emerged with important economic and social implications and effects on innovation, growth, employment, knowledge creation as well as challenges to privacy and security. Today, it is difficult to think of a policy domain that is not affected by the Internet. Some are readily discernable, such as the need for regulatory reform for communication networks or the many considerations surrounding digital content. Whereas separate and distinct networks (data, video, telephony) once provided critical communication functions these infrastructures are now converging towards the Internet. These changes cut across and challenge legal and regulatory frameworks applicable to telecommunication and broadcasting. They are disruptive for existing business models in areas such as content production but create enormous opportunities for innovation and growth. More broadly, the Internet and the constellation of information technologies it connects are viewed as essential ingredients in addressing some of the world's most pressing policy issues: sustainable and increasing economic growth, aging societies, environmental management, energy efficiency, the eradication of poverty and so forth. The implications for economic and social activities are far-reaching and profound, including for the next several billion users. Hence expectations toward the Internet have increased dramatically since 1998.

At such a point, policies need to be carefully crafted and coordinated across policy domains, borders and various stakeholder communities that will guide the future of the Internet economy. Moreover, with the emergence of new players in global markets, such as India and China, policy discussions need to draw out the principles necessary to address opportunities and challenges at international level. Building on the core competencies of the OECD the Ministerial will develop stronger linkages to the global Internet economy and the policies necessary for an enabling environment. Three themes will be addressed:

FUELLING CREATIVITY

The Internet has greatly expanded our capacity to create, compute, communicate, co-ordinate, and innovate, toppling barriers that constrained so many economic and social activities in the past. It has led to increased productivity, lowered costs and raised living standards in ways difficult to imagine just a few years ago. This creative activity is generating new software and hardware products, sensor technologies, new ways of organising global business, employment creation, and the development of digital content across the economy and in research, government, health and education. The theme of Fuelling Creativity will consider:

- How to enable innovation and encourage new co-operative models for growth and employment.
- Enabling maximum access to public sector information and content and its re-use by the private sector.
- The value of e-science in innovation policy and in the OECD's innovation strategy.

BUILDING CONFIDENCE

As it becomes a key conduit for economic and social activity, the Internet also attracts fraud and malicious practices that are increasing in size and sophistication and threaten consumer and user confidence. As no single entity working alone can ensure a trusted online environment, there is a need to work collectively – across borders, engaging all stakeholders – to formulate effective practices and policies to prevent an erosion of confidence. The theme of Building Confidence will consider:

- Policies to ensure the security of critical information infrastructure and combat malicious software.
- Multi-stakeholder, cross-border co-operation for privacy, security and consumer protection.
- Policies to empower consumers online, ensure fair mobile commerce transactions and combat identity theft.
- Policies for digital identity and its management.

BENEFITING FROM CONVERGENCE

Through technological development and regulatory reform, network platforms for data, voice and video that were previously separate are converging to a single platform based on the Internet protocol. This is resulting in a range of new services, a re-evaluation of business models and changing levels of competition in formerly distinct markets. Policy is caught up in this change and must adapt to the new environment. The Internet's capabilities are expected to be further transformed as it embraces new technologies such as wireless access and sensor networks. The theme of Benefiting from Convergence will consider:

- Overarching principles needed for convergence and the transition to the next generation of high-speed networks.
- Guidance to help consumers navigate the transition towards a converged network that offers bundled and tailored services while stimulating competition.
- Policies for opportunities and challenges offered by evolving RFID and sensor networks.

THE OECD MINISTERIAL AND THE IGF

In 2005, the second phase of the World Summit on the Information Society (WSIS) addressed steps to establish the foundations for an Information Society. The creation of the Internet Governance Forum, as a part of the Tunis Agenda, was one of the principal outcomes of the WSIS. The OECD welcomed this initiative and in 2006 assisted in the preparation for the inaugural IGF as well as participating in the Athens event itself.

The issue chosen for an IGF workshop was the OECD's then recently finalised Anti-Spam Toolkit. This topic was selected not only because it represented an immediate and practical concern for Internet users and policy makers but because it was an outcome of multi-stakeholder engagement. The OECD's Anti-Spam Task Force brought together representatives from government, business, the technical community and civil society.

The Athens IGF workshop also proved an ideal opportunity for a group of stakeholders to launch the StopSpamAlliance. This joint international effort was initiated by APEC, the EU's

Contact Network of Spam Authorities (CNSA), ITU, the London Action Plan, OECD and the Seoul-Melbourne Anti-Spam group. Since that time four associate partners have joined the StopSpamAlliance: the Asia-Pacific Telecommunity (APT), the Messaging Anti-Abuse Working Group (MAAWG), the Internet Society (ISOC), and the Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE).

The objective of the StopSpamAlliance is to help co-ordinate international action against spam and related threats more effectively by gathering information and resources, and improving information sharing among participating entities.

In line with the WSIS Tunis Agenda – asking members to "deal effectively with the significant and growing problem posed by spam" and calling upon all stakeholders to adopt a multi-pronged approach to counter it – the StopSpamAlliance pages link to initiatives in the field of anti-spam legislation and enforcement activities, consumer and business education, best practices, and international co-operation. The website is at: www.stopspamalliance.org

Moving forward, the 2007 IGF in Rio de Janeiro, represents an opportunity to take stock of a wide spectrum of views in the lead-up to the Seoul Ministerial. The OECD will again present work it has undertaken relevant to one of the IGF's main themes with a view to its dissemination to the global Internet community. This time the OECD is organising an open forum on its work on malware which will be finalised prior to the Seoul Ministerial.

Looking beyond Rio, the 2008 IGF in New Delhi represents a perfect opportunity to present the outcomes of our own Ministerial Meeting on the Future of the Internet Economy, and we look forward to ongoing co-operation between the OECD and the IGF. We view this as part of the OECD's standing commitment to provide useful solutions to problems posed by the governance of globalisation, and to be instrumental in enabling economies and societies to benefit from the large opportunities it presents through closer economic interdependence.

Security of the Domain Name System

Steve Crocker & David Piscitello,
ICANN's Security and Stability Advisory Committee (SSAC),
Los Angeles

The Domain Name System is arguably the most critical of all Internet applications. Simply put, if DNS isn't available, users are unable to resolve host names to IP addresses and so cannot connect to Internet servers. The DNS is a remarkable distributed database system. It has adapted admirably to the demands of nearly a billion Internet users. However, having name resolution in the critical path of the majority of application transactions means it is essential the information is reliable.

The DNS infrastructure (the local, country and top-level domains, plus root name server systems and the communications paths that serve them) is a prime target for attackers who now regularly attempt to disrupt name service by launching distributed denial of service (DDoS) attacks. It is also a powerful tool for attackers, who also regularly exploit the DNS for impersonation-based attacks such as phishing and pharming for e-criminal activities such as identity theft, fraud, e-money laundering, and child pornography. Authentication, confidentiality, and integrity protection would make it difficult for attackers to exploit the DNS for pharming and identity theft purposes, but these security measures weren't among the original DNS design objectives and protocol. For some time, the Internet community has been developing and deploying measures to make the DNS secure. Let's look at why these are important and how they can mitigate several types of attacks.

DNS THREAT VECTORS

The threat vectors used to exploit the DNS fall into two categories: information origin impersonation and unauthorized alteration or substitution of false DNS information. In the context of DNS, impersonation can take several forms. By impersonating a DNS client, an attacker can falsely register his computer and dynamically update false resource records at a DNS server. The attacker can also impersonate thousands of DNS clients and use this army of clients to flood DNS servers with queries (see [SAC008]). By impersonating a DNS server, an attacker can answer DNS queries and direct clients to phishing and identity theft websites. Attackers who impersonate DNS servers are also able to transfer bogus zone data to an unsuspecting DNS server.

Impersonations are themselves formidable attacks, but the maliciously altered or "poisoned" DNS resource records and zone data which attackers inject into the DNS enables additional, equally malicious attacks. Altered DNS cache data, subverted zone data, and DNS data intercepted and modified by an attakker during a man-in-the-middle (MITM) attack are common attack tools for phishers and pharmers.

To improve DNS security, we must define methods to detect and thwart impersonation. We must also be able to detect when DNS information has been altered without authorization by a party other than the authoritative source of DNS information. Two sets of DNS security standards satisfy these security requirements: Transaction Authentication for DNS and DNS Security.

TRANSACTION SIGNATURES (TSIG)

Peer or mutual authentication is used by many Internet security protocols as a means of verifying communicating endpoints before exchanging data. For example, in IP Security (IPsec), two security gateways (e.g., Internet firewalls) use a protocol called the Internet Key Exchange (IKE, [RFC2409]) to perform peer authentication. A common implementation of IKE allows each server to verify its identity by securely transmitting a secret that only the two servers share. A similar shared-secret based authentication method – the Secret Key Transaction Authentication for DNS [RFC2845] – is available for DNS.

The Transaction Signatures (TSIG) protocol defined in RFC 2845 allows any pair of name servers (A and B) to authenticate each other each time they perform a DNS message exchange. TSIG provides what is often referred to as (message) integrity protection, as follows. DNS server A sends a message to DNS server B. The DNS message can be a query, response, dynamic DNS update or zone transfer, and is encoded according to normal DNS protocol conventions, with one important addition: an encrypted hash of the DNS message is added to the message in a special resource record, the Transaction Signature (TSIG RR). DNS server A adds a timestamp to additionally protect the query from a replay attack.

When DNS server B receives the query, it decrypts the hash and compares this value against a hash value it computes over the message it received. If the values are equal, the message is authentic.

Specifically, DNS server B knows that only DNS server A could have created the hash value attached to this DNS message and that this message is an exact copy of that composed by A and has not been altered in transit.

TSIG can be used to protect a variety of DNS message transactions, ranging from a single dynamic DNS update by a client host to a transfer of the DNS resource records for an entire domain (commonly referred to as a "zone transfer"). Of these, the greatest benefits may be gained by authenticating zone transfers. In a 2006 survey, Infoblox and The Measurement Factory discovered that nearly one in three "allow zone transfers to arbitrary queries, enabling duplication of an entire segment of an organization's DNS data from one DNS server to another, and leaving them easy targets for denial of service [and impersonation-based] attacks."

Name server administrators must maintain a unique key for each pair of name servers that will protect DNS message exchanges using transaction signatures. TSIG uses timestamps to protect DNS transactions from replay attacks. Name server administrators must maintain synchronized and accurate network time on DNS servers that use TSIG. Managing network time and a modest number of shared secret keys is a small price to pay for the ability to thwart DNS message alteration and name server impersonation in strategic locations within your network.

Managing shared secrets does not scale well, and this influences where TSIG can be optimally deployed. Clearly, not every organization can use TSIG to authenticate transactions with root name servers; however any organization could use TSIG to authenticate peers at “fan in” point in a network, where one or a handful of name servers processes DNS queries for a very large number of clients. Examples of such deployments include dynamic DNS updates from approved DNS clients, DNS exchanges between the clients and referral name servers an organization operates internally; and zone transfers between an organization's name servers and those operated by preferred ISPs.

TSIG provides per-transaction integrity protection and thus mitigates the threats of name server impersonation and DNS message alteration. In the DNS security world, this is sometimes called “channel” security. TSIG does not, however, provide the means to verify whether the DNS information conveyed in that transaction wasn’t maliciously altered prior to transmission. Like any other data, DNS data is vulnerable to corruption and unauthorized modification. For example, a successfully executed DNS cache poisoning attack will result in the corruption of DNS information that a name server records in its local cache.

Similarly, a successfully executed “privilege escalation” attack can provide an attacker with full administrative control over an authoritative name server. Acting as administrator, the attacke can modify individual name records or entire zones in that server’s master file. The attacker could also impersonate a name server and return “non existent name” to any or all queries for this domain. Such attacks are sometimes called “betrayal” attacks because a trusted source provides false DNS information.

DNS SECURITY

To mitigate threats against DNS data at rest, an authority that administers a domain’s name data must provide one or more forms of data object security. File system and drive level encryption software (Microsoft Encrypted File System) are popular examples of data object security. These security software systems provide three services: data origin authentication, data confidentiality and data integrity protection.

In the context of the DNS, only the first and last are relevant. Data origin authentication confirms that the name server claiming to be the authoritative source for a domain's zone data is really the authoritative server and not an impostor. Data integrity protection provides the recipient with a guarantee that the DNS data it receives is accurate and authentic copies of the domain's authoritative zone data. Since the purpose of DNS is to share domain name information, providing data confidentiality is less relevant and currently not accommodated.

Future DNS Security extensions will protect zone files during transfer. Some organizations do incorporate, in their zones, data that should not be disclosed publicly. These organizations typically "split" DNS into public and private zones and carefully restrict transfer of the latter.

DNS Security ([RFC4033], [RFC4034], [RFC4035]) provides data origin authentication and zone data integrity protection using public key cryptography as follows: a DNS administrator creates a public/private key pair for zone data of a domain over which he claims authority (e.g., example.com). He then stores the private key of this pair in a secure manner and publishes the public key in a new resource record type (DNSKEY) in example.com's zone file. Publishing the public key allows any name server to acquire example.com's decryption key and thus decrypt any zone data that example.com's DNS administrator has encrypted using example.com's corresponding private key.

Example.com's DNS administrator then computes a message digest over example.com's zone data using a strong hash algorithm (typically SHA1 or SHA256), and encrypts the message digest using example.com's private key. The DNS administrator adds this digital signature to example.com's zone file in another new resource record type, Signature (RRSIG). The RRSIG is then included in all DNS response messages.

To determine whether the data is authentic,

- use example.com's public key found in the DNSKEY resourcerecord,

- decrypt the hash value recorded in the RRSIG record using the message digest algorithm indicated in the RRSIG record
- compute the hash of the example.com's zone, and
- compare the hash value in the zone data in question against the locally computed hash value.

If the values are identical, the zone data are accurate and authentic copies of example.com’s zone data. This protection can be applied to any resource record set of a zone's data. Since public key cryptography is used, any DNS client or server that receives zone data purported to be from example.com from any name server can determine if the data are authentic in this manner.

A domain’s zone signing key is a critical element of the DNSSEC’s data object security. To determine whether the signing keys themselves are authentic, each zone administrator arranges to have the domain name parent authority sign his zone’s public key, and makes this signature available in a Delegation Signer Resource Record (DS RR). Name servers that implement DNSSEC validate signatures by tracing the chain of signed public keys back to a trusted root of the authoritative security domain. For example, the 2nd level label “example” is registered under .COM, so the administrator would arrange to have VeriSign sign its public key with VeriSign’s private key. COM is a top level domain, thus VeriSign would have the public key it uses to sign .com signed by IANA (Internet Assigned Numbers Authority), which administers the authoritative root (“dot” or “.”).

DNSSEC’s data object security measures complement rather than duplicate TSIG’s channel security measures. Thus, an organization seeking to adopt a strong security policy should consider having its resolvers and name servers validate zone data whenever the RRSIG and DNSKEY records are available, use the DS to validate signing keys, and use TSIG to ensure integrity of communications with whatever set of name servers it chooses to trust.

GOVERNANCE ASPECTS OF DNS SECURITY

The full value of DNSSEC will be achieved when every zone is signed and every resolver checks the signatures on DNS queries. It will take quite a while before DNSSEC is fully deployed, but there will be considerable value well before then if the top level domains are signed: Once this happens, each community will be able to move forward with deployment and use of DNSSEC within its own applications. For example, governments can sign their zones and thereby protect their citizens from being lured to bogus sites, as can industries such as the financial services and health care sectors, universities and major business groups, which can each implement DNSSEC and begin to include it within their own best practices.

From an Internet governance perspective, DNSSEC is an important tool for protecting the integrity of the Internet infrastructure, and should certainly be on the agenda. Each country should set a date for the deployment of DNSSEC within its own ccTLD and government zones and also encourage its adoption by the business community.

At time of writing, Sweden, Bulgaria, Puerto Rico and Brazil have signed their top level domains, and work is underway in several other countries.

In the United States, DNSSEC is now included in the government's requirements for its high-value network sites, and work is underway for its top level domains to be signed. See [DNSSEC June 2007] and [FISMA].

The top level domains all reside in the root, and work is also underway to sign the root. Some consider the signing of the root to be a political issue because it involves the creation of a key to be used by everyone to resolve DNSSEC entries. All that is really required is for the process of creating and managing the root key to be rigorously neutral and properly managed so as to ensure the integrity and accuracy of the entries in the root zone.

Good resources for tracking the deployment of DNSSEC and getting help in deploying it are maintained at the website [Deployment] and at the sites listed in the Additional Information section following the citations.

CITATIONS

- [DNSSEC June 2007] http://www.dnssec-deployment.org/
- news/dnssecthismonth/200706-dnssecthismonth/
- [FISMA] http://www.dnssec-deployment.org/news/FISMA.htm
- [RFC2409] The Internet Key Exchange (IKE)
- [RFC2845] Secret Key Transaction Authentication for DNS (TSIG)
- [RFC4003] DNS Security Introduction and Requirements
- [RFC4034] Resource Records for the DNS Security Extensions
- [RFC4045] Protocol Modifications for the DNS Security Extensions
- [SAC008]: DNS Distributed Denial of Service (DDoS) Attacks (31 March 2006) [PDF]
- http://www.icann.org/committees/security/ssac-documents.htm
- [Deployment] http://www.dnssec-deployment.org

ADDITIONAL INFORMATION

- DNSSEC – DNS Security Extensions. Web site that provides excellent and important background information for a general and technically literate audience on the history and development of the protocol, and useful tools. http://www.dnssec.org/
- M. Gieben, DNSSEC, The Internet Protocol Journal, 7 [2] (June 2004). Verified January 20, 2005. Offers a useful introduction to the protocol. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-2/dnssec.html

Protecting Children on the Net

John Carr,
Children's Charities' Coalition on Internet Safety, London,
United Kingdom

The Internet is an astonishing technical achievement. In the industrialised world it has already transformed many aspects of modern life, and it continues to spearhead further dramatic changes. In other parts of the world the Internet and related technologies promise a great deal. Potentially, they will allow many different societies to leapfrog expensive and lengthy stages of economic development.

For children and young people in particular the Internet is becoming phenomenally important. It is reshaping the way in which they learn at school, and it is also reshaping higher and further education, professional education as well as on-going or lifetime education, for example for those who might want or need to retrain for a new career later in life.

When linked with other digital technologies, the Internet allows a degree of personalization of education and training which was unimaginable only twenty years ago. We can foresee a time when every child and young person will have their own education programme, tailored to their own specific aptitudes, interests and needs.

Every child will also be able to have their own "digital vault". This could not only store their entire educational history, essentially forever if that's what they want, but in addition it could be expanded to contain a record of many or all key elements of their life outside of and after school. Future biographers will have to learn to work in very different ways from their predecessors.

Of course it is not only what is happening within the world of education and learning that is driving larger and larger numbers of children and young people towards the Internet. Cyberspace is cool. The Internet is where your friends hang out, where you keep up with the activities and output of your favourite musicians or sports team, or discover new musicians and new teams.

Whereas the older generations might regard the Internet in a very instrumental way – a place to go to do specific things such as buy books or an airline ticket – children and young people, the new generation of digital natives, increasingly simply see it, along with their mobile phones, as an obvious and completely integrated extension of their everyday lives. Indeed. as convergence takes an even greater hold, the distinction between the different hardware or access devices is fast dissolving. More and more children and young people live in and feel fully part of a 24/7/365 connected world.

Many national governments are now completely convinced of the value of being online, both in educational and broader social and economic terms. The whole drift of public policy across huge swathes of the world is to encourage ever lower broadband prices and ever greater levels of take-up and use of the Internet. But in the UK the government is going yet further and intervening even more directly as far as children and young people are concerned.

At the moment around 11 percent of UK households with children and young people of school age do not have any kind of Internet access within the family home. It is now accepted that this means the children in those homes are increasingly at an educational and social disadvantage, and the household itself is at an economic disadvantage.

The reasons why these households have no Internet access are many and varied. Some relate to economic considerations e.g. the cost of the connectivity, or the cost of the hardware and software. But often money is not a significant part of the explanation.

Significant cultural or religious factors may be at play in some households. Others may have children with physical disabilities where conventional hardware will simply be no use to them. Specific adaptations may be needed. Refugee and itinerant families can sometimes present special challenges. In some families, fear or anxiety about a range of risks and dangers associated with the Internet can act as a barrier to take up. Such fears or anxieties may exist in their own right, or otherwise be particularly important where a child has certain kinds of learning difficulties or is vulnerable for any one of a number of reasons which may be permanent or temporary in nature.

However, overwhelmingly, whether or not a particular family has Internet connectivity in the house appears to be linked to the level of educational attainment of the head of household[1]. The level of educational attainment of the head of household ties in very strongly with their perception of whether or not the Internet has, or could have, any value or relevance to themselves or other family members.

Through the "Home Access" initiative UK Government policy is now to focus very specifically on the 11 percent of families who still do not have any kind of Internet access in their home. The aim is to reduce that number to zero, with a more ambitious longer-term target being to ensure that, in every family and household, every child or young person of school age has a "satisfactory" level of access to the Internet[2]. If you are a family with four children, and all those children need to do their homework in the evening or at the weekend, having only a single computer with Internet access may be of little practical value. It might even lead to increased family tensions or difficulties.

We have noted that concerns about the risks and dangers associated with children's and young people's use of the Internet act as a barrier to some families' take-up and use of the Internet. In the context of its Home Access initiative, the UK Government therefore accepts it has a very direct and specific responsibility for the online safety of the children and young people who will obtain Internet access through the programme, but this simply reflects a wider acceptance of the Government's responsibility for online safety for all children and young people.

[1] Future Foundation report for BT (insert precise reference)

[2] The author is chair of the UK Government working party which is focussing on the safety standards which are to be attached to the Home Access initiative.

The Internet is increasingly recognised as being a public space but there remains a widespread feeling that there are still too few protections for children and young people within it. A major unintended and unforeseen consequence of the growth of the Internet as a mass consumer product has been the emergence of categories of risk which hitherto were either completely unknown or were much more limited in their scope. For some children the Internet has become an additional medium through which they can be bullied, harassed, threatened and made to feel unsafe.

In relation to children and young people, many of the risks or dangers they are exposed to, even in the real world, are anyway often poorly understood by parents, teachers and others with a responsibility for supporting children through the different stages of their development into adulthood. But even when the risks are understood at a general level in a real-world context, there is often a very limited appreciation of what practical steps could be taken to reduce or minimise them in the online world.

Many children and young people are completely fearless when it comes to using the new technologies. They believe themselves to be Masters of the Universe, completely invincible. But many often lack an appreciation of just how badly things can go wrong if they take what seems to them to be a few innocent and trusting steps.

It was ever thus. The job of a child is to push at the boundaries, to see how far they can go on their journey to becoming an adult. The job of parents and teachers is to teach children and young people about the risks and dangers that are out there and how to avoid them, or how to deal with them should they nonetheless encounter them en route This applies just as much to a child's use of the new technologies, as it does to a child's use of a bicycle. Just as parents try to control a child's intake of sweets or try to curb the amount or type of TV programmes their children watch, so nowadays parents need to know what lies behind a computer screen, where the computer can take their children and what could happen to them when they get there.

The problem, of course, is that while most parents know about bicycles, sweets and TV, because they learnt about them from their own parents and have themselves been consumers of them, there is no equivalent generation to pass on any distilled wisdom or experience about online risks and dangers. Today's parents are really the first generation being faced with this challenge. It is the younger generation who frequently know more about the technology and feel more confident about using it. But does this mean that today's children will definitely be the Internet-savvy parents of tomorrow? No doubt many of them will be, but it would be quite wrong to assume blandly that all of them will be. That depends on what they learn today.

Without doubt this lack of awareness, often of some fairly basic aspects of children's and young people's use of the technology on the part of parents, is rooted in the fact that many of today's parents and teachers left school before the Internet became what it now is. Parents and teachers have not had the same opportunity to gain a similar level of familiarity with the technology as their children. This more limited knowledge means parents and teachers may struggle to help their children understand or deal with the risks that the new technologies present.

It is all very well for a teacher or a parent to utter wise words about different risks or dangers to children, but unless these words are located in the specific context of the child's everyday experience it is too easy for them to be dismissed or sidelined as being empty platitudes. We urgently need to find better ways to help parents and teachers to get up to speed. Even if they never quite match the technical knowledge or chutzpah of the younger generation there has to be a much greater degree of proximity than we have achieved so far.

For example, in a survey conducted for NCH[3] earlier this year, ICM[4] interviewed a thousand children aged 11-16 and roughly the same number of their parents[5]. One third of children surveyed said they regularly used blogs, yet only 1 percent of their parents knew that they did. In fact two-thirds of parents did not

[3] Formerly National Children's Homes, the UK's largest independent child welfare organization

[4] A major polling company

[5] See http://www.nch.org.uk/information/index.php?i=77&r=469, supported by Tesco Mobile

know what a blog was. Similarly, 79 percent of children said they used Instant Messaging regularly, yet only one third of parents understood what Instant Messaging was.

There are two principal security threats to children and young people posed by the Internet. Firstly it can facilitate their exposure either to egregiously age-inappropriate content which they may find disturbing or distressing. Secondly it can also expose them to predatory individuals who mean to harm or exploit them.

Addressing the security threats to children and young people is not only vital in its own right, from a child protection standpoint, but it is also important because of the impact any well-publicised failures have on the general level of public trust and confidence in the Internet. A medium that is so frequently associated with stories about child pornography, paedophiles and scams of various kinds perpetrated against youngsters is one that many will choose to avoid.

A startling illustration of this enduring lack of public confidence in the Internet was supplied in a MORI[6] poll carried out for "The Sun"[7] in January 2006[8]. Entitled "Britain Today" it showed that, given a very wide range of choices, two of the top five "worries" of adult Britons concerned children and the Internet. Whatever view one might take about the empirical basis for such a level of concern,[9] there is no denying, firstly, that it is grounded in real events that have happened to real children and, secondly, that these concerns persist.

If we all had greater certainty about who was transacting with whom, rather as, typically, we still do in the real world, a great many other problems which continue to plague the Internet

[6] A major polling company

[7] The UK's largest, daily tabloid newspaper

[8] See http://www.mori.com/polls/2006/s060117.shtml

[9] Official figures are not always very helpful in allowing anyone to make judgements about the scale of the problem, much less to make comparisons with pre-internet days, but two reports which, inter alia, present some of the data to do with child sex abuse on the internet and child pornography have been submitted separately to the Select Committee. These are "Child Abuse, child pornography and the Internet" (2004), and "Out of Sight, Out of Mind" (2006), both published by NCH.

would also be very likely to diminish. People are far more likely to behave badly or inappropriately online if they believe there is little or no possibility of them being identified and held to account for their actions. This applies as much to posting child pornography, and to grooming children in Internet chat rooms, as it does to engaging in phishing or spamming.

There is no “silver bullet”, no one single measure which will solve all of the problems facing children and young people on the Internet. We need to put together a combination of educational and awareness measures which reach out not just to children and young people but, crucially, also to their parents and others who have analogous responsibilities e.g. teachers. But we do also have to go as far as we can with technical measures and in that connection the issue of being able to know who we are actually dealing with, and their age, is very important, particularly in the context of child protection.

A number of online service providers and businesses had started insisting on using credit cards or other forms of banking cards as a means of identifying who an individual was, and whether or not they met certain age criteria, before they were allowed to engage in a particular action e.g. join a web service or buy a particular product or service. However in some countries e.g. the UK, the banks issue plastic cards to children as young as 11 and this creates additional complications.

More recently, however, we have started to see the emergence of so-called “pre-paid” banking cards which utilise, for example, the Visa and Mastercard logos. They are being marketed as providing access to exactly the same online and offline locations that conventional Visa and Mastercard credit cards offer. Yet these pre-paid cards can be obtained for cash, over the counter in a corner shop. These cards can be obtained in a way that renders them, effectively, untraceable and shoots a great hole through any notion that credit cards or banking cards can any longer, on their own, be accepted as a proof of age or identity.

Traditionally, where age-restricted goods or services were being sold, it was always possible to carry out a visual check. The vendor had to use their judgement to determine whether or not the person standing in front of them wanting to buy something met the stipulated age minimum. If they could not provide proof of their age, and the vendor had any doubts about it, they would simply refuse to sell them the goods or provide the service. Since a reliable visual check of a person's age is, for practical purposes, impossible on the Internet, children and young people have been able to obtain access to age-restricted goods or services or gain access to places on the Internet in circumstances which they would not have obtained in the real world e.g. they have been able to gamble, buy knives, alcohol or tobacco, join adult chat rooms or sites, or buy adult videos. In addition, children and young people have also been the victims of frauds which may well not have succeeded or even been attempted if the target audience was limited to adults.

Greater certainty about individuals' online identity has to be at the centre of any new strategy that aims to keep children safe online or which aims to ensure that the real-world laws which apply to age-restricted goods and services can also be applied in the virtual world. National Governments could be the agencies to lead on the introduction of schemes of this nature, and within many countries it is possible that their existing system of national identity cards could be adopted for that purpose. However not all countries have national identity schemes and even those that do may feel reluctant to pursue such a course of action, for any number of perfectly valid reasons. That being so it will fall to the private sector, perhaps with the banks and schools playing a particularly important part, to come up with an age and identity verification system that will start to build the wider public's confidence in the Internet as a safe place for children and young people, and themselves, to work, learn and play.

What do the Words "Internet Security" Mean?

Avri Doria,
Lulea Technology University, Sweden

BACKGROUND

Internet security is frequently discussed, but if you ask someone what they mean by it, you may get many different and sometimes contradictory answers. Security has become an overloaded term used by many in various differing ways. While I am not a protocol security expert, the first and still most common reference in my work in the Internet industry had to do with the security of the network itself and was specifically related to security aspects of protocols. A longstanding practice among those writing protocols as candidates for standards status in the Internet Engineering Task Force (IETF) is to require a security considerations section in every specification. This technical requirement is still my first assumption on hearing the word security used in Internet context. It is not, however, the primary association among others involved in the issues of Internet governance.

As the Internet grew, the instance of threats against the stability of the network began to grow and the need for concerted effort to combat these threats to the stability of the network itself prompted the introduction of Computer Emergence Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs).

Meanwhile, as interest in the Internet as a means of doing business grew, the next concerns for security had to do with securing transactions, so that customers would be able to trust the Internet enough to do business. The security concerns extended further into the protection of the customer's data and while this was not an important concern for businesses themselves, it became a concern for consumer protection agencies.

Once governments started to pay attention to the Internet and began to describe it as a national resource linked with national security, security concerns started extending to concerns about cyber-crime and the assumption of cyber-terrorism. As with any technology, its potential for weaponization eventually became apparent as well as the political advantage to be gained by accusing others of using the Internet in acts of cyber-aggression. However valid the initial claims of cyber-terrorism and cyber-warfare were, these topics are now regarded as issues of Internet security.

At the same time that businesses and governments began to get involved in making policy regarding Internet security, citizens and users began to express concerns for the privacy of their data and their civil rights of freedom from surveillance.

Finally some have extended the notion of Internet security to protecting children from viewing inappropriate material and have included the need to protect children from child pornography and people, especially women, from the use of the Internet for exploitation and modern slavery.

These and perhaps other meanings are all included in the words "Internet security". This paper will look briefly at Internet security in various senses and at the relationship between these disparate meanings. The paper will also explore the question of whether the overloading of the term "Internet security" has reached the point were one can no longer discuss the issue intelligibly without first defining the context of the discussion.

SECURITY IN THE SENSE OF PROTOCOL SECURITY

For the development of protocols, the Internet Engineering Task Force (IETF) requires that every protocol specification include a security considerations section that discusses the security risks that might be incurred by use of the protocol and discusses ways to remedy those risks.

"Most people speak of security as if it were a single monolithic property of a protocol or system. However, upon reflection one realizes that this is clearly not true. Rather, security is a series of related but somewhat independent properties. Not all of these properties are required for every application. We can loosely divide security goals into those related to protecting communications [...] and those relating to protecting systems [...] . Since communications are carried out by systems and access to systems is through communications channels, these goals obviously interlock, but they can also be independently provided."[1]

The guideline goes on to break down the requirement for protecting communications to include:

- Confidentiality: "means that your data is kept secret from unintended listeners"[2]
- Data integrity: "make sure that the data we receive is the same data that the sender has sent"[3]
- Peer authentication: "we know that one of the endpoints in the communication is the one we intended"[4]
- Non-repudiation: this is the ability for someone who received authenticated data with data integrity to prove that fact to a third party.

The RFC goes on to depict a model that demonstrates both the threats and possible solutions. While it is clear that in many cases the tools provided by protocol designers are necessary in order to provide the types of Internet security discussed in this paper, they are by no means sufficient for dealing with the wider scope of Internet security concerns.

SECURITY IN THE SENSE OF PROTECTING THE NETWORK

System security is concerned with protecting the machines themselves and the network infrastructure. In most cases this involves preventing unauthorized usage and preventing others from interfering with authorized usage, for example the oft-cited distributed denial of service attacks (DDOS) where a network of unsuspecting machines is used without authorization to prevent authorized usage of some other target resource.

[1] Guidelines for Writing RFC Text on Security Guidelines; RFC 3552, Jul 2003, page 3

[2] ibid page 4

[3] ibid

[4] ibid

In terms of operational security the realization is that no matter what protocol writers and system implementers do to protect their protocols and systems, the miscreant hackers[5] would find a way around the protection. In this fight, various groups formed to provide immediate defense after attacks were reported. The efficiency of the CERT and CSIRTs in this 'arms race' has been impressive; with every new virus or DDOS attack, it is often a matter of hours before a protection has been developed, although deploying them to the Internet users themselves can take longer. Again while it is clear that this is necessary in providing Internet security, it is not sufficient, even in combination with the protocol level, for solving the issues contained in the broader definition of Internet security.

SECURITY IN THE SENSE OF MAKING IT SAFE TO DO BUSINESS

The business community has been very concerned about the trust users of the Internet can have in their online transactions. If due to the prevalence of phishing[6] attacks bank customers lose money and cannot trust their bank's web site, it costs the bank money. If a customer cannot trust that their confidential financial information, e.g. their credit card numbers or their financial value, is safe and will not be misused, they will not give businesses the information that the latter collect in order to fine-tune their product offerings and maximize their profits. It is important to realize that these days the profits many businesses generate from the information they collect from their customers can be as great as the profits they make from their products. If people, other than those businesses, gain illegitimate access to this information, the illusion of safety the customers feel in freely giving their private information to companies is lost, and with it the immense profits these business get from buying and selling information about their customers.

[5] It is important to realize that not all hackers are bad. Originally hackers were just brilliant people who could sit down and write a system from a tabla rasa. Unfortunately some of these bright people are also miscreants.

[6] The fraudulent process of collecting private information by pretending to be someone that the customer would usually trust, like their bank.

In this case security is served by procedures and toolkits, such as those put out by the Organisation for Economic Co-operation and Development (OECD) for helping business assess their risk and then design and manage security systems. Businesses also rely on law enforcement agencies, both public and private, and on the policies of groups such as the Internet Corporation for Assigned Names and Numbers (ICANN) to give them the means they feel they need to fight potential crime. In ICANN, the battle against phishing and other security threats is the ostensible reason that businesses insist on the requirements for full public access to all registrant data such as phone numbers and addresses, despite the fact that this access causes security problems for the individual registrants. In the judgment of businesses this is justified because the threat to the market, e.g. the well being of the banking or recording industry, is greater and more important then the privacy threat to individuals. This is the tip of a conundrum caused by mixing many different requirements for security; society ends up with a tussle[7] between those who want to protect their markets and profits and those who want to protect their privacy. Arguably both are security priorities but a question is pending as to which predominates in a just society. Businesses rely on the technical and operational security solutions described above. They also rely on governments and other policymaking bodies to enable them to gain the information they need and to give public and private law enforcement the tools they need in order to provide the level of security they feel is required.

SECURITY IN THE SENSE OF A STATE'S SOVEREIGN INTERESTS

While governments showed very little interest in the Internet when it was first created, as it grew they decided that it was an

[7] Tussle was introduced in the Internet context by Clark, Sollins, Wroclawski and Braden in a 2002 paper titled "Tussle in Cyberspace: Defining Tomorrow's Internet". their basic premise is "... one important reality that surrounds the Internet today: different stakeholders that are part of the Internet have interests that may be adverse to each other, and these parties vie to favor their particular interests."

issue of national interest. As such, it quickly became a matter of sovereignty and thus a concern for the national security apparata.

It started out with fighting cyber-crime at the behest of business interests. With the worldwide concern, whether fully justified or not, about the Internet being used for cyber-terrorism, the national security interests in some countries have been able to rationalize almost any action in the name of security. The final straw in the creation of a national priority for major security control of the Internet has come with the fear and uncertainty bred by the juxtaposition of children's interests and the fact of pornography on the Internet. Among many national leaders, the issues of terrorism and pornography, especially in relation to children, provide sufficient reason to warrant the suspension of all rights and liberties on the Internet.

Governments have taken the security threat to the Internet one step further than with the weaponization of the Internet, and accusations of acts of cyber-war, or at least accusations of the potential and intention for acts of cyber-war. Cyber-war can be defined as any use of the Internet to disrupt another country's activities, be it the economic, cultural, governmental or military process. War and it cousin terrorism, are of course the biggest security threats to all people. And when one speaks of cyber-war, one is talking about the governments that sit in august intergovernmental bodies such as the United Nations and not of the 'rogues' who dispute the legitimacy of these governments – their actions are called cyber-terrorism.

In many cases the technological tools provided by protocol implementers and the operational tools provided by CERTs and CSIRTs might be enough to protect vital national Internet resources from attack. However, government often considered it necessary to stop potential threats and this often involves the process of determining what a person might be thinking or who they might be talking to. This has led to the development of other Internet security tools that frequently threaten the security of citizens and other users.

SECURITY IN THE SENSE OF THE UNIVERSAL DECLARATION OF HUMAN RIGHTS

Human rights are defined in the Universal Declaration of Human Rights[8] (UDHR), the International Covenant on Civil and Political Rights[9], and the International Covenant on Economic, Social and Cultural Rights[10]. Taken collectively, these agreements, as well as other international conventions, can be understood to define the civil, political, economic, cultural and social rights of all the world's people, regardless of nationality, status, identity or other factors. Anything that threatens these rights can be defined as an appropriate issue for Internet security as it threatens the security of every one of the world's people.

In the context of the Internet, the primary right involves Article 19 of the UDHR which was affirmed in paragraph 4 of the WSIS Declaration of Principles[11] issued in Geneva in 2003:

"We reaffirm, as an essential foundation of the Information Society, and as outlined in Article 19 of the Universal Declaration of Human Rights, that everyone has the right to freedom of opinion and expression; that this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers."

Of course that is offset by paragraph 5 of the same principles:

"We further reaffirm our commitment to the provisions of Article 29 of the Universal Declaration of Human Rights, that everyone has duties to the community in which alone the free and full development of their personality is possible, and that, in the exercise of their rights and freedoms, everyone shall be

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

[9] http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

[10] http://www.unhchr.ch/html/menu3/b/a_cescr.htm

[11] http://www.itu.int/wsis/docs/geneva/official/dop.html

subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations. In this way, we shall promote an Information Society where human dignity is respected."

The juxtaposition of these paragraphs, as well as their referents in the UDHR, articles 19 and 29, are two components in one of the major tussles in the security issue. In the quest for national security on the Internet, governments have engaged in many practices that threaten the security of individuals on the internet, for example surveillance, monitoring communications, censorship of writing, imprisonment and torture when self-censorship due to fear of repression was not sufficient. It can be argued that government pursuit of security is frequently in direct contravention to individual security.

While many of the tools provided by protocol technologists, e.g. encryption for confidentiality, might work to protect users, governments have often used their power of legislation to make the use of such tools illegal. In addition, industry has often complied with government requests, sometime with due process and sometimes without or with only a semblance of due process, to circumvent individuals' privacy and right of free expression. It is rather clear that governments' self-proclaimed needs for security are often the cause of the threat to the fundamental security rights of individuals. This particular tussle shows no signs of a quick resolution and is a key policy problem for Internet governance.

DISCUSSION

As this discussion of the definitions hints, there is a major tussle inherent in the definition of "Internet security" once we move beyond the simple technical discussion of confidentiality, authentication and non-repudiation. It does not take long, when discussing business requirements for security, before the security of users' privacy becomes part of the tussle. Likewise a nation's security policies can quickly impinge on the rights of citizens to privacy and freedoms of expression. Even issues such as the creation of domain names are rapidly becoming involved in a tussle when it becomes a matter of protecting the 'moral security' of children or of a sensitive religious population.

This amalgam of definitions can be seen in the program[12] for the Rio de Janeiro meeting of the Internet Governance Forum (IGF). Specifically, the IGF attempts to blend the many meanings of security and thus includes the following under the title of “security”:

- Security threats to countries, companies, and individuals as users of the Internet and to the Internet itself
  - The definition of security threats, international security cooperation, including such issues as cybercrime, cyber-terrorism and cyber-warfare.
  - The relationship between national implementation and international cooperation.
  - Cooperation across national boundaries, taking into account different legal policies on privacy, combating crime and security.
  - The role of all stakeholders in the implementation of security measures, including security in relation to behaviour and uses.
  - Security of internet resources.
- Authentication and identification
  - Authentication and identification and their role in fostering trust online and their relation to the protection of privacy.
- Challenges to privacy in a security environment.
  - Respecting freedom of expression.
  - Privacy and identity.
  - Privacy and development.
- Security issues related to the protection of children.
  - Protecting children from abuse and exploitation in the online environment.

[12] Draft Programme Outline for the Second Meeting of the Internet Governance Forum (IGF) http://www.intgovforum.org/Rio_Meeting/DraftProgramme.24.09.2007.rtf

As a neutral ground, the IGF is a suitable venue for debating this issue, and the diplomatic language used to describe the problem is good in that it includes many facets of the tussle. While it is difficult to predict anything greater than understanding and a continuation of the precarious balance between the various Internet security requirements, there is hope that the various sides will be able to participate as equals in discussions of such a critical Internet issue.

Chapter 5

Critical Internet Resources

Critical Internet Resources – A Private Sector Perspective

Vint Cerf,
Chairman of the Board of Directors of ICANN,
Marina del Rey

The Internet has evolved from its constrained, experimental and highly focused origins to become a vast, global ecosystem embracing stakeholders from all sectors: the public, industry and business, academia, governments and civil society. Its physical manifestation lies in the hands of a remarkable confederation of parties. All of these stakeholders own their portions of the Internet in the form of laptops, desktops, servers, mobiles, routers, wireless subsystems, and other devices. Some players own physical communication resources such as optical fiber, satellite, cable systems and wireless networks and others provide software and network-based applications. Still others provide services that promote and support electronic commerce, social networking, electronic messaging of all kinds, content distribution and delivery, education, and many, many more online applications. It might be argued that the owners of the Internet represent one of the most diverse groupings of entities in the history of telecommunications. One of the key design concepts of the Internet was the notion that anyone who could implement portions of the Internet according to its protocol rules could reasonably connect to the rest of the system and become a part of the global network ecology.

There can be little debate that as remarkable as this array of stakeholders is, it also represents only a portion of the full range of parties interested in one aspect or another of the global Internet. Collaboration, cooperation, and coordination are the order of the day in enabling the Internet and all its myriad applications to actually work for its global user base. The term "critical Internet resource" invites a narrowing of the list of Internet resources to a small subset that seem to deserve the title "critical." In fact, however, the resources that must be present for the Internet to thrive and evolve are diverse and widely spread around the globe.

My colleague, Robert Kahn, has sometimes compared the Internet to the "economy" and asks, "Who is responsible for the successful operation of the economy?" The answer seems to draw in innumerable parties, each with a role to play, cooperating directly or indirectly through various market forces, practices and conventions. As in the economy, people play a critical role in the well-being and evolution of the Internet. Without skilled programmers, engineers, operators, equipment makers, application designers, enlightened governmental policymakers, thoughtful legal practitioners, effective and innovative business leaders, researchers, teachers and knowledgeable users, the Internet would not be the remarkable global engine of innovation and utility that it has become. Any consideration of critical Internet resources must take into account the wide range of people resources that are needed to keep the Internet operating and evolving in productive directions. As we consider the challenge of the Millennium Development Goals, the need for many suitably experienced people has to lie high on our list of critical Internet resources.

The standards that are used in implementing the Internet represent a kind of recipe for its operation. Without them, interoperability and the innovation this invites would be impossible. The maintenance and creation of standards thus lies on the main stream of critical functions without which the Internet could neither function nor evolve. There are many organizations whose focus on digital information handling standards is relevant to the Internet's well-being. Among them are the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronic Engineers (IEEE), the European Telecommunication Standards Institute (ETSI), the International Telecommunication Union Technical standards organization (ITU-T), the World Wide Web Consortium

(WWWC), and many national standards bodies as well as private-sector groups facilitating industry forums and consortia. All of them can be considered critical Internet resources insofar as they contribute to the Internet's stability and to its ability to evolve to meet new requirements and changes in technology and user demands.

The Internet is rooted in digital transmission, storage and processing technology. That fact alone has many consequences, not the least of which is that digitized intellectual property has become more difficult to manage, if one is concerned about controlling access to the property to enforce business models based on the notion of confining access to instances of the digital content to parties prepared to pay for their access. Organizations such as the World Intellectual Property Organization (WIPO) and others drawn from national or provincial settings have the unenviable objective of reifying digital content management within frameworks intended for rather different physical manifestations of intellectual property. Bodies that facilitate the establishment of conventions for managing digital information and protecting the interests of intellectual property holders represent another critical element in the global Internet infrastructure.

This is just a part of a larger framework of legal structures that are intended to facilitate the development of and perhaps subsequent enforcement of policies and practices that make possible electronic commerce in its most general sense. Included in this broad context might be contracts arrived at and signed electronically, conventions for order entry, confirmations, shipping and delivery of goods, online delivery of content and a host of other business practices that enhance the utility of the global Internet for businesses, consumers and governments around the world. Included in this larger legal framework must be conventions and practices for dealing with abusive use of the Internet, in which category one might place spam, fraud, misrepresentation, identify theft, damage to property including software (through the propagation viruses, worms, Trojan horses), a wide range of denial of service attacks, harassment, and distribution of illegal materials (such as child pornography), and so on. To deal with these problems one not only needs laws tailored to the online, global digital environment but also potential inter-governmental agreements and cooperation between the private sector and various levels of law enforcement practitioners. These critical legal resources need to cooperate in substantive ways to protect the interests of citizens, business, academia and government.

The Internet's design was based on the premise that a standard set of technical rules could allow an arbitrary number of networks to be built and operated independently, an arbitrary number of devices to be connected to these networks, owned and operated by a diverse collection of parties, and an arbitrary range of applications to be developed and supported through the interconnected set of networks. In order to achieve this degree of distributed management and operation, certain technical resources had to be coordinated in a more global fashion, and among these are the top-level domain names of the Internet, the allocation of unique Internet addresses and the tracking of protocol parameters necessary to assure the interoperability of independently-produced software and systems.

Coordinated assignment of these resources may also be considered critical to the successful operation of the Internet and to accomplish this task, the Internet Corporation for Assigned Names and Numbers (ICANN) was set up, in part through the action of the U.S. Government. Prior to its creation in 1998, these matters were managed by the Internet Assigned Numbers Authority (IANA) which was operated by a researcher at USC Information Sciences Institute under a contract with the U.S. Government. Even this critical global coordination is actually carried out in a distributed fashion. The assignment of Internet Addresses to users of the Internet (including application service providers) takes place through Internet Service Providers (ISPs) who receive their address allocations through Regional Internet Registries (RIRs). The RIRs coordinate their global policies through the Number Resources Organization (NRO), which in turn delivers proposed global policies to ICANN for ratification by its Board of

Directors. There are five Regional Internet Registries in Europe (RIPE-NCC), Asia/Pacific Rim (APNIC), North America (ARIN), Latin America and the Caribbean (LACNIC) and Africa (AFRINIC).

Among the central issues facing the Internet community in the near term is the runout of available, unique IPv4 address space and the need to put into place the allocation and assignment of the new IPv6 address space. ICANN has addressed this issue in cooperation with the NRO and RIRs. It is anticipated that the last blocks of IPv4 address space will be allocated by ICANN to the RIRs around 2010-2011 and that introduction of the IPv6 address space into the Internet's operation is a critical activity. ICANN has already authorized entry of IPv6 addresses into the root Domain Name zone file (see below) and assignment of IPv6 address space by the RIRs and ISPs.

Domain names are delegated to users by way of registrars and registries, of which there are now hundreds around the world. In addition to generic Top Level Domains (gTLDs) such as .com, .aero, .int, .net and .museum, there are also over two hundred country coded Top Level Domains (ccTLDs) including .de (Germany), .br (Brazil), .ke (Kenya), .cn (China) and .ki (Kiribati). ICANN is responsible for managing the delegation of Top Level Domain names to qualified operators and for establishing and managing the framework of registry and registrar operation. The process is heavily oriented towards a multi-stakeholder, bottom-up process of policy development.

Among the important expansions of Domain Name space is the introduction of non-Latin symbols ("characters" or "glyphs") into Domain Names. Standards have been developed to achieve this objective at all levels in the Domain Name system and tests are underway in the last quarter of 2007 to validate the use of these extended symbols in the "root zone file" which points to the actual Top Level Domain subsystems on the Internet that can translate the domain name into appropriate Internet Protocol (IP) addresses. Successful testing of these new forms of domain names should lead to the introduction of new, non-Latin domain names during 2008.

To these two important Internet resources, one can add the general introduction of new generic Top Level Domains. Meeting the interest in the creation of new TLDs while protecting users against potential confusion and even abuse has been a challenge but multi-stakeholder discussions are expected to produce guidelines for the solicitation of new Top Level Domains in 2008.

Another essential element of the Domain Name System is assurance for users that when they look up domain names in the DNS they are receiving the same information that was placed into the system by the operator of that particular domain name. A system of digital signing of the various zone files including the root zone (which points to all the Top Level Domain Name servers) called DNSSEC is in development and its deployment should be considered relevant to the stability and security of the Domain Name System. Users can request digitally signed responses from the DNS and have confidence that the information has retained its integrity as long as the digital signature on the data can be validated.

It goes without saying that the operators of the Root Zone Servers represent another critical and visible resource for the Internet. Through the advice of the Root Server System Advisory Committee (RSSAC), coordination with the U.S. Department of Commerce, and cooperation with VeriSign's root zone master update system, ICANN coordinates its updating of the Domain Name Root Zone and its propagation to all root servers on the Internet. It is important to recognize that through the use of "anycast" techniques, there are far more root zone servers than the original 13 root zone operations would imply. There are over 100 root zone servers around the world.

By now it should be quite obvious that the Internet's ecosystem is global in scope, complex in its character and utterly dependent on collaboration, cooperation and coordination for its effective operation. Efforts to develop increasingly effective processes for harnessing the power of the Internet to achieve the Millennium Development Goals set out by the World Summit on the Information Society will of necessity need to engage a wide range of Internet stakeholders, to the extent that the Internet is or can be the means to reaching these Goals on a global scale. The multi-stakeholder model of ICANN reflects in many ways the multiple facets of the Internet ecosystem and represents an attempt to fashion an instrument of policy development for a narrowly defined but important part of the general Internet's structure. We shall succeed in evolving the Internet and making its capabilities accessible to the full world's population only by addressing the full range of critical infrastructure needs outlined in this paper and, more generally, in this book.

The New Global Politics of Internet Governance

Milton Mueller,
Syracuse University, New York, Internet Governance Project[1]

I am against using "development" as the compulsory touchstone for Internet governance dialogue. I prefer to talk directly about the politics, economics and policies of global Internet governance. The frame of development diverts our attention, clouds debate and replaces substantive policy dialogue with rhetorical mush. What does "development" mean? Who is against "development?" Is there a party advocating underdevelopment and poverty in the field of Internet governance? At best, the rhetoric of "development" is just a code word for progressive people to indicate that they care about the less wealthy and powerful countries in their policy calculations. That is fine and good. But let's not talk in code; let's talk openly about the way actual Internet policies and institutions distribute power and wealth, and how Internet policies actually affect people. Let's talk about who wins and who loses from specific decisions, and how those decisions are made.

At its worst, the concept of "development" becomes the pervasive ideology of "Developmentalism" that William Easterly (2006) complains about, which channels the concerns we have about poverty into "fattening the international aid bureaucracy" and supporting "the self-appointed priesthood of Development" in the IMF, World Bank and UN agencies.

[1] The Internet Governance Project (IGP) is an alliance of academic researchers with expertise in global governance, Internet policy, and information and communication technology. Its partners publish a variety of timely and readable analyses of current Internet governance issues and participate actively in the Internet Governance Forum, ICANN, and other relevant venues. http://internetgovernance.org

"Like other ideologies, this thinking favors collective goals such as national poverty reduction, national economic growth and the global Millennium Development Goals over the aspirations of individuals. Bureaucrats who write poverty reduction frameworks outrank individuals who actually reduce poverty by, say, starting a business."[2]

To make progress on Internet governance after the World Summit on the Information Society (WSIS), one must break away from routine UN concepts and take a fresh look at the political and economic forces shaping the contours of the Internet. The rise of the Internet altered the international balance of power around the governance of information and communication technology. The recipe for change included three key ingredients:

1) The enhanced role of non-state actors in global governance. The Internet's unplanned emergence as the dominant standard for data communications worldwide, combined with privatized and liberalized telecommunications, conferred de facto control of critical resources and standards upon private Internet companies and the technical community.
2) The "flat," global connectivity of the Internet, which undermined the territorial sovereignty of states in ICT policy. It did not render states powerless, of course, but any government that permits its citizens Internet access exposes itself to globalized markets for information, communication and media services where it is harder and more costly to exercise national regulatory control.
3) Change was caused by the pre-eminence of one sovereign nation, the United States, in establishing a global framework for Internet governance. Because the TCP/IP protocols were first developed and implemented by US Government contractors, the US inherited the centralized levers of control. In that way it gained the ability to exercise a kind of unilateral globalism in the construction of an international Internet governance regime around ICANN.

[2] William Easterly, "The Ideology of Development," Foreign Policy, July/August 2007, p. 32.

WSIS was basically a reaction to the three forces of change described above. At the summit there was a clash between two models of global governance, a traditional one based on agreements among sovereign, territorial states, and a new transnational order based on private contracts among nonstate actors – but dependent on the global hegemony of a single state (the U.S.) for its implementation. Although the situation is still not fully settled, the general outlines of a new equilibrium are evident. Because of WSIS, the gap between the ICANN regime and the old sovereignty-based order has been narrowed; there has been a regression to the mean. Key elements of the non-territorial, multi-stakeholder ICANN regime have survived the challenge and their existence is no longer in peril. At the same time, governments have gained greater authority over ICANN's activities. ICANN's GAC will begin to look more and more like a United Nations for the Internet, and governments' self-proclaimed "sovereign right" to "set public policy" for the Internet has been recognized by all the signatories to the WSIS Tunis Agenda.

Looking forward, political contention over global governance of the Internet will continue in three key areas. One of the most central is the Tunis Agenda's attempt to create a special role for governments in setting "public policy" for the Internet. It is not clear whether this can work. There is no bright line separating decisions that can be classified as "public policy" from those considered "technical management." The claim that states have a "sovereign right" to make policy for the Internet may not be compatible with the non-territorial reach of networked computers and the distributed authority over a network of networks. When do we need global as opposed to national policies for the Internet? When global policies are needed, do nation states fully represent the public interest at the global level? There are dangers in mixed models: ICANN's GAC, for example, gives governmental participants special status but lacks many of the procedural safeguards of traditional intergovernmental arrangements. And we must not overlook the fact that a key to the Internet's success was its ability to devolve policy-making power to individuals and organizations.

Some of the most interesting and strategic issues in Internet governance are related to security. Security is a collective good and security for the Domain Name System (DNS) is an area where adoption and implementation of a global standard makes sense. A newly standardized protocol, DNS Security Extensions (DNSSEC), could make the Internet's infrastructure more secure. In order to implement DNSSEC on a globally compatible basis, however, the procedures for managing the DNS root must be revised. The world would have to agree on a single, authoritative "trust anchor" that would digitally encrypt the root zone file. This change provides both an opportunity and a huge challenge for global governance of the Internet.[3] In revising the root zone management procedures, we can develop a new solution that diminishes the impact of the legacy monopoly held by the U.S. government over the DNS root, and avoid another contentious debate over unilateral U.S. control. Or, we can continue to rely on U.S. government initiatives, such as those promoted by the US Department of Homeland Security[4], thereby strengthening the special powers of the U.S. and generating mistrust among other power centers, such as the European Union and China – possibly leading to a fragmented implementation.

Finally, there are likely to be strong pressures to regulate Internet content at the global level, and equally strong resistance to such efforts. ICANN's attempt to subject proposals for new top-level domain names to standards of "morality and public order" offers a clear example. Many governments and some religious and business interests want ICANN to censor offensive or controversial names at the top level. Civil libertarians and minority viewpoints vehemently oppose such a policy, arguing that ICANN should be a neutral technical coordinator

[3] See Brenden Kuerbis and Milton Mueller, "Securing The Root: A Proposal For Distributing Signing Authority" (May 17, 2007). Internet Governance Project. Paper IGP07-002. Available at http://internetgovernance.org/pdf/SecuringTheRoot.pdf

[4] See Signing the DNS Root Zone: Technical Specification. Prepared for the US Department of Homeland Security, by NIST, Sparta Inc., Shinkuro, Inc. Version 3.0.2, October 2006. http://mail.shinkuro.com:8100/Lists/dnssec-deployment/Message/553-02-B/061031RootSignSpec.pdf

and not a global censor.[5] More broadly, there are growing efforts by governments to reassert borders on the Internet by blocking or filtering content.[6] There are also growing challenges to those efforts, with civil society and business invoking the norms of “network neutrality” and “nondiscriminatory trade” in information goods and services.[7]

Long term, Internet governance will make more progress if we focus on matters of substantive policy such as DNSSEC and content control, rather than on generalities such as “development.”

[5] See the “Keep the Core Neutral” Campaign, http://www.keep-the-core-neutral.org

[6] The OpenNet Initiative is a consortium of scholars at Universities of Toronto, Cambridge, Oxford and Harvard that identify and document Internet filtering and surveillance. See http://opennet.net/

[7] Google has asked the US government to treat censorship of China as a trade barrier. See http://googlepublicpolicy.blogspot.com/2007/06/censorship-as-trade-barrier.html

The Internationalisation of Internet Resource Management: An African Perspective

Adiel A. Akplogan,
AFRINIC

INTRODUCTION

When we talk about Internet resources, there is a need to differentiate between name and number resources. Name resources are managed following a different model than number resources, which this session covers. One key difference is that in many cases names are managed based on purely commercial rules while numbers are still managed based on technical constraints, mainly aggregation for optimization of the routing table size.

In this article, we will spend more time on number resource management and look at its internationalisation from an African perspective.

BACKGROUND TO THE INTERNATIONALISATION OF IP ADDRESS MANAGEMENT

IP addresses are the core resources needed to run the Internet Protocol. They allow all connected equipment to have a unique identifier to ensure unambiguous communication between them. Right from the beginning, there was a need to register assignments of these identifiers to networks and hosts. The registration was first managed manually by John Postel. Originally, address space was then allocated based on fixed, non-flexible boundaries for the host and network part identifiers. The space could only be organised into three classes: class A, with128 possible network identifiers and about 16 million hosts per network, B, with about 16,000 possible network and 65,000 hosts per network and C, with2 million possible network identifiers and only 254 hosts per network[1]. As the Internet grew quickly during the late 1980s, two problems appeared: the rapid depletion of address space due to the non-flexible class divisions and the uncontrolled growth of the Internet routing tables due to routing information that was not aggregated. This is the basic dilemma of address space assignment: conservation versus aggregation. On the one hand, conserving the address space means assigning exactly what is needed to avoid wastage; on the other, easing routing-table pressure means aggregating as many addresses as possible in one routing-table entry. To handle the conservation issue, the predefined class-based management of IP addresses was abandoned and replaced by a supernetting technique called CIDR (Classless Inter Domain Routing) addressing, which mainly allows assignment of IP addresses to networks in a more granular way with a variable length of network size and host count. The complication introduced by these new factors for address space management and the continued growth of the Internet across the world made it increasingly difficult for one person (John Postel at the time) to handle the task. IANA (the Internet Assigned Numbers' Authority) was then set up to take over the job so far done by John on wider amplitude. After a while, it appeared that for certain practical reasons, this central registry model would not scale enough to cater for the globalization of the Internet and the attendant cultural diversity. In 1990, the need for change was clearly recognised by the Internet Architecture Board in their recommendation to the US Federal Networking Council stating that "it is timely to consider further delegation of assignment and registration authority on an international basis" (which inspired the authors of the RFC 1174). This recommendation was followed by some guidelines for a new regional registration system to be set up in RFC 1366, 1466 and later, RFC2050.

The first regional body to be set up based on RFC 1174 was RIPE NCC[2] (Réseaux IP Européens – Network Coordination

[1] RFC 791: ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

[2] More about RIPE NCC can be found at www.ripe.net

Centre) formed in 1992 to serve as the delegated registry for Europe. APNIC[3] (The Asia Pacific Network Information Centre) quickly followed in 1993 to serve Asia and the Pacific, then ARIN[4] (The American Registry for Internet Numbers) to serve North America in 1997. The three RIRs were also serving the needs of other regions as well such as Africa and the Indian Ocean (by RIPE NCC, ARIN and APNIC) and Latin America and the Caribbean (by ARIN). These two regions eventually set up their own delegated registries respectively in 2002 (LACNIC[5] – Latin America and Caribbean Network Information Centre) and 2005 (AFRINIC[6] – The African Network Information Centre).

Today, all the fives region have their own registry with the main advantage of having an organisation close to the needs of the local community.

THE CASE OF AFRICA

So one may ask - why did it take so long for a registry like AfriNIC to be set up (almost eight years after ARIN and 13 years after the first registry)? The simple answer is that the setup of an RIR (Regional Internet Registry) is largely driven by local community needs and the evolution of local Internet infrastructure. The approach followed in all the other regions was "bottom up" and this is meant to be the case everywhere as described in an Internet Coordination Policy document (ICP-2[7]). In the case of Africa, the first initiative to set up a registry was back in 1997 (nearly the same time as ARIN) but, as the IP infrastructure in the Africa region was still very new, it was hard to get a proper consensus and endorsement from the community – mainly because there is no real local IP backbone to which ISPs in Africa are connected. Most have one-to-one connections to upstream providers in either Europe or USA from where they

[3] More about APNIC can be found at www.apnic.net

[4] More about ARIN can be found at www.arin.net

[5] More about LACNIC can be found at www.lacnic.net

[6] More about AFRINIC can be found at www.afrinic.net

[7] ICP-2: Criteria for Establishment of New Regional Internet Registries - http://www.icann.org/icp/icp-2.htm

get their IP addresses. According to Dr. Nii Quaynor, one of the co-authors of the first project paper (in 1997), “the difficulty was simply that Africa did not have adequate access to IP addresses, and building hidden networks with severe numbering constraints made African networks not easily accessible globally. Africa’s knowledge of Internet technology was thus significantly reduced”.

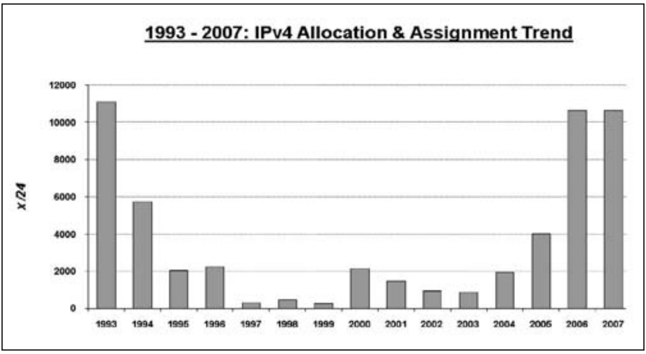
As the network started to grow and more and more providers began running BGP (dynamic routing), peering locally and facing nightmares of renumbering every time they changed providers, the need to have their own allocated IP block arose. A more fundamental requirement was to have a registry close to their needs, based on the regional state of the network and the region’s culture. The new organisation was established in April 2004 and the process to set up an operational registry took another year (obtain endorsement of the local community, comply with the ICP-2 document). AfriNIC became the fifth accredited RIR in April 2005.

WHAT ADVANTAGE HAS AFRINIC BROUGHT TO OPERATORS IN AFRICA?

The internationalisation of IP resource management has certainly brought IP address growth in each region. From the African region’s perspective, the setup of AfrINIC has been very positive. Once the organisation was set up and even before its accreditation, the first thing that was done was to launch a wide awareness program aimed at operators. Its main goal was to correct misconceptions about the availability of IP addresses to be used in the region. In two years (2005-2006), AfriNIC has visited more than 20 countries to conduct training and meetings on how IP addresses are managed and how operators can take advantage of the international structure of the system to get their own resources. The result was very positive, with more and more ISPs becoming members and getting the allocated IP addresses they need for deploying their networks and services. In many cases, we noticed that operators do not even know that they can use their own allocated addresses to connect to the Internet.

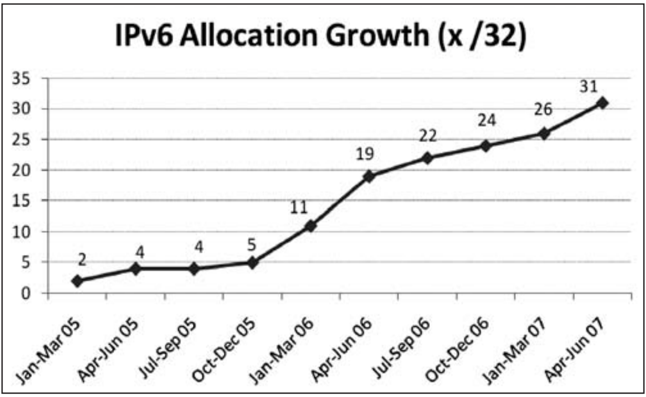
In two years of operation (2005-2007), we have more than doubled the number of existing Local Internet Registries (from 113 in 2005 to about 300 today) and tripled the number of IP addresses allocated each year.

According to the same Dr. Nii, "another meaningful advantage of the existence of AfriNIC as a local registry is the fact that now the local community is visible in the global addressing policy regime, and taking ownership of management of numbers resources by Africans. The process of establishing AfriNIC in itself educated Africans, who acquired skills to operate an RIR serving the Africa region. This capacity-building process has continued with AfNOG (African Network Operators Group), AfTLD (African Top Level Domain Manager association), AfriSPA (African ISP Association) and others who share the same community of operators".



Two important things can be noted from the above graph. First, before 1994, an important number of allocations were made to be used in the region. Most of these allocations were based on class addressing as described above. With the setup of the RIRs and the application of classless addressing, the number of allocations decreased significantly (as expected) up to 2003. Secondly, since 2004 the impact of the accreditation of a regional registry to serve the region again changed the trend of IP resource allocation, with steady growth over the past four years. The proximity of a regional service along with the effort made to educate local operators on the benefits of using their own allocated IP addresses has shown positive results. While the ratio of IP addresses allocated in Africa still sounds very small (approximately 2%, partly due to the state of Internet infrastructure in the region) the evolution in the past year makes us feel that things are changing very quickly and Africa may catch up a bit, mainly with the launch of broadband services in several parts of the continent and the emergence of IP based services for mobile phones and Integrated services. In all the regions, the management of IP addresses based on the local reality has shown that the local community gains many advantages while keeping the Internet stable and the key technical principles (aggregation, registration and conservation) in place for managing this finite resource.

Another positive effect we have observed from having a local registry is the awareness of IPv6.



This new version of the protocol and associated addresses has been under discussion and in experimental/live deployment for a while in several regions. Very few operators in Africa were aware of the need and the importance of getting to know IPv6. When AfriNIC was setup, IPv6 was immediately included in the training and regional meeting plan backed by several measures taken by the board to waive fees for IPv6 allocations. The subsequent growth was not surprising even though we have not yet reached the point where each IPv4 network also operates IPv6-

ready services. With allocations from AfriNIC, it is positive to see that for once, the Africa region is not too far behind other regions in IPv6 adoption.

Despite the positive impact of the setup of a registry to serve Africa's needs in term of IP addresses, it is also important to add that there are still many challenges for an organisation like AfriNIC to efficiently achieve its mission. Management of IP Resources is based on a bottom-up multistakeholder approach as defined in our policy development process. But very few operators and policymakers really participate in the process. Perhaps this is due to the limited resources they have at their disposal to follow and efficiently participate in the discussion and the process in general. Global events like the WSIS and the IGF, in which AfriNIC has been very active in various ways, are examples of a positive environment where a lot has been and is being done to build the capacity of both institutions and individuals in this area. AfriNIC and other similar organisations in the region are working to build capacity that can help increase participation by different stakeholders.

Widening the Internet Address Space: Towards IPv6

Latid Latif,
IPv6 Forum, Luxembourg

BUILDING THE BUSINESS CASE FOR IPV6 ADOPTION

Defining the business case for IPv6 has been a very challenging task. IPv6 stands ready to revitalize the growth and use of networking and the Internet as a platform for commerce, education, entertainment and general information sharing. However, at the end of the day, it is still just communication "plumbing". The market has long looked to IPv6 to deliver the next killer application when in reality IPv6 is just a tool, albeit a critical one, in the development of new applications and network-based services. This reality, combined with the short-term perspective on return-on-investment (ROI) and quarterly earning reports most businesses have had post-dotcom bubble, have created an environment hostile to investment in new technologies including IPv6, most notably in North America and Europe.

Another impediment to IPv6 adoption has been one of the IPv6 community's own making: extolling the virtues of IPv6 primarily from a technical perspective. While IPv6 offers a number of technological advancements, such as a larger address space, auto configuration, a more robust security model for the peer-to-peer environment, and better mobility support, these features – offered in a technology vacuum – have not resonated with big business. Business and government leaders alike are concerned about how to resolve problems, how to generate revenue, and how to build efficiencies and cost savings into their organization. IPv6 certainly has the ability to help deliver these scenarios, but the focus of the story needs to be the solution – not the technology that helped deliver that solution.

GLOBAL MANDATES AND POLICY FOR IPV6 ADOPTION

Over the past six years, IPv6 has enjoyed remarkable success for integration via support from government or industry standards bodies. The reasons for these mandates vary widely from technical to political, but regardless, they have helped cement the concept that IPv6 is simply not a passing technology, but truly the foundation for the next generation Internet. To provide some specific cases, the list below identifies a number of governments or industry bodies that have called for IPv6 usage:

- 3GPP mandated exclusive use of IPv6 for IMS (IP Multimedia Subsystems) on May 10, 2000.
- IMS has been selected by Telecommunications Industry Association (TIA) as the NGN platform.
- In Sep. 2000, the Japanese Prime Minister identified IPv6 as a critical part of the eJapan 2005 initiative. The Japanese government provided tax incentives to companies which integrated IPv6 support.
- The South Korean Government announced its support for IPv6 in Feb 2001.
- The United States Department of Defence mandated the integration of IPv6 in June 2003 to be ready by 2008. The OMB has set the budget and milestones.
- The European Space Agency declared its support to IPv6
- The Japanese ITS project and the European Car2Car consortium recommended exclusive use of IPv6 for its future car2car applications
- The Digital Video Broadcasting (DVB-S) consortium decided to move to IPv6.
- The Chinese government created and financially supports CNGI, an IPv6 backbone network designed to be the core of China's Internet infrastructure.
- CENELEC has opted for IPv6 for the smart home concept.
- GRID has adopted IPv6 in its Globus Toolkit 4

These represent just a few of the numerous examples for major support of IPv6 by government bodies or industry consortiums. In the case of government bodies, aggressive IPv6 adoption curves have pushed industry, particularly those vendors that support or interact with the government, to work toward IPv6 adoption themselves.

IPV6 AS A SOLUTIONS TOOL

Organizations utilize information technology every day to solve business problems (Note: we will use the term "business" in the general sense – applicable to any organization, be it government, non-profit, or corporation). With the adoption of networking technologies to facilitate communications, conduct financial transactions, or exchange information, the IPv4 based system has been quite successful but it has now been pushed to its limit. Ignoring for a moment the issue of potential IPv4 address exhaustion, the limited volume of addresses has short changed technology advancements in areas like anycasting, multicasting, or peer-to-peer exchanges. Most advanced network support features like security and quality of service were afterthoughts – not part of the original design of IP. As a consequence, the standards bodies and industry have provided solutions that extended the capabilities of the network, but also drastically increased its complexity and created additional problems.

Today, organizations are finding it increasingly difficult to deploy new IT solutions that are cost-effective and relatively simple to support. A heavy reliance on Network Address Translation (NAT) hinders network simplicity and becomes prohibitive to the creation and support of additional services. As a simple example, let's examine a Business to Business (B2B) relationship between an organization and its partners.

Company Biz.com has an extranet with 22 different vendors/partners for the purpose of supply chain management. Each company, including Biz.com, must use private addresses to number their internal network (i.e. 10.0.0.0/8). As it turns out, it is quite common for there to be network numbering overlap – e.g. Company Biz.com and 6 of the 22 partners all have nodes using the address 10.1.1.17. This creates a problem that can be remedied by using static NAT mapping to create unique addresses for each device that is accessible to the extranet partners. So 10.1.1.17 becomes 192.168.0.7 externally for Biz.com and an entry is made in the outward facing NAT device. Each partner that also has that address in use creates a similar entry, but with a "unique" address.

Each organization must participate in the process. It requires great coordination, extra equipment, and constant management. Clearly in this case, use of IPv6, with the ability to uniquely identify each node, alleviates the need for this complicated and expensive NAT mapping scheme. And this represents just one of hundreds of ways IPv6 can be used to solve "real world" problems that add value to the organization and have Return On Investment (ROI) models attractive to management.

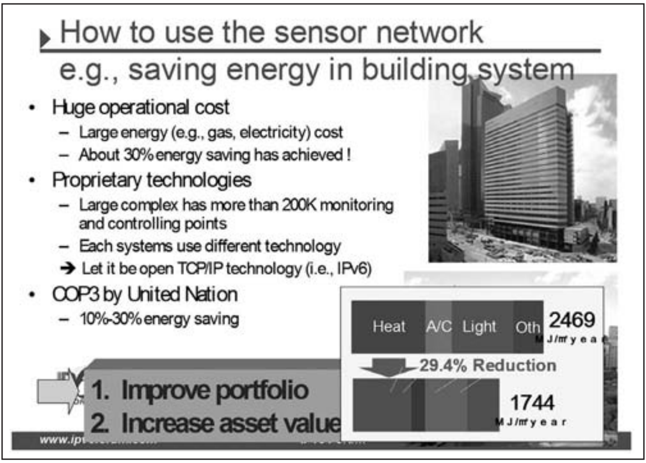
IPv6 has several advantages over its predecessor, including a larger and more diverse address space, built-in extensibility, and the power to support a more robust security paradigm. As such, it serves as a powerful foundation for the creation of new and improved net-centric sets of products and services. Although the last few years will not go down in the annals of history as revolutionary for the Information Age, innovative thought didn't cease – it just moved into simmer mode. The IPv6 Forum, as pundits for the adoption of IPv6, has actively pursued and identified possible ways to leverage IPv6. This list is by no means exhaustive, but it does highlight a number of very promising technologies where IPv6 will be a critical building block:

- Ubiquitous Communications – With increases in the number of mobile phone users, the expansion of Internet-related services through the cellular networks, and an increasing number of connection mediums (UMTS, WiFi, Wimax, UWB, etc), there is a need for a uniform communications protocol that supports mobility and can handle a large number of devices.
- VoIP/Multimedia Services – VoIP has been making excellent progress from a technology adoption perspective. A move from H.323 to SIP has enabled more robust VoIP implementations with a greater level of simplicity and expandability. Additionally, the type of traffic occurring over the network is far more diverse, including data, voice, and video (currently known as triple play, or quad-play with wireless). The ability to access content, be it data, voice, or video on any platform is very attractive to end users, particularly those who are

highly mobile. IPv6, with increased address space, a large multicast space capacity, and an affinity for SIP, serves as a logical platform for the expansion of these services.

- Social Networks – People interact. The form by which they do this has changed drastically over the years – from written letters, to phone calls, to e-mails, to SMS and IM messages. That evolution continues today. The ability to transfer photos, conduct conversations in private Peer to Peer (P2P) environments, display personal information on the Internet, find like-minded communities, or play interactive games requires an Internet that is flexible, supports ad-hoc connections, and can be secured. IPv6, with its auto configuration capabilities and support for IPSec at the IP stack layer will be a critical tool to enable this environment.
- Sensor Networks – Sensor networks are a new concept. They can be found in manufacturing equipment, heavy machinery, security systems, and HVAC (heating, ventilation, and air conditioning) systems.
  - What is new is the concept of integrating all those proprietary systems onto one communications systems.
  - In a post 9/11 world, the use of monitoring systems to detect toxins and radioactivity in water systems, air filtration system, or at airport or shipping terminals around the world has increased substantially.
- Product Tethering/Communities of Interest – Manufacturers would love to have relationships with their product once it leaves the factory. The reality is that most consumer electronic and white goods producers have little, if any, interaction with the end users of their product. In a world where all things can be connected, the opportunity to create new services, be it remote troubleshooting and device management, or providing value-added services – such as automated grocery shopping, are almost endless. Not only could the end users' experience be enhanced, but the manufacturers, or their ISP partners, could create new services not feasible in an IPv4 world.

Yet the need for increased security and monitoring has to be offset against the cost of deploying and managing those systems. IPv6 offers a very stable and flexible platform that supports mobility, ad-hoc networking, and a large number of simple devices. . See the example below for how IPv6-based sensors in a “smart” building can help lower building energy costs.



How to use the sensor network

e.g., saving energy in building system

- Huge operational cost
  - Large energy (e.g., gas, electricity) cost
  - About 30% energy saving has achieved !
- Proprietary technologies
  - Large complex has more than 200K monitoring and controlling points
  - Each systems use different technology
  - ➔ Let it be open TCP/IP technology (i.e., IPv6)
- COP3 by United Nation
  - 10%-30% energy saving

1. Improve portfolio
2. Increase asset value

As stated, these are by no means all the opportunities possible in an IPv6 world. Companies in Asia, Europe, and North American have already begun to look at IPv6 as a platform for creating a competitive advantage. Companies that take the time and effort to understand v6 stand a good chance of leapfrogging their competition and vaulting into the next-generation Internet with a substantial lead.

BUILDING A PLAN FOR IPV6

So the opportunity exists with IPv6 for those willing to consider the protocol as a tool for defining solutions to existing business problems, and a platform for innovation for next generation products and services. How does the IPv6 Forum and industry continue the groundswell for IPv6 integration?

First, the need to understand IPv6, its features, and most importantly, how they map to potential networking problems, still exists. Although the IPv6 Forum and the regional task forces have provided all manner of educational opportunities for industry, there remains a need for a coordinated effort to increase IPv6 awareness at three levels:

- Strategic planning at the corporate level
- Return on Investment (ROI)
- Technical knowledge at a tactical level.

To achieve a measure of success, the IPv6 Community needs to follow this basic strategy:

- Generate an interest in technical solutions at the CEO/CTO level. Stories of the virtues of auto configuration and the power of IPSec EH should be left at the boardroom door. Solutions that fix problems or build competitive advantages are compelling. The fact that IPv6 is the glue that makes the solution work should be last. Once these solutions are “sold”, IPv6 will become part of the long-term strategies of these organizations.
- Create a framework for ROI to justify sound decision-making. The IPv6 Forum is not in the business of defining a specific number, percentage, or time frame for ROI – organizations need to do these themselves. But providing them with the framework for an ROI model will expedite this process.
- Solutions sold at the Cxx level will need competent engineering and architecture to deliver. This requires formalized education and knowledge transfer... The Cxx level needs to understand and support this process.

This approach has achieved great success in the following three cases to name just a few:

- US DOD as a long term strategic planning large-scale organisation
- The Chinese government, which has a 20-year plan to connect its entire industry, institutions and nations favoured by its central planning system.
- 3GPP as a Greenfield standard for next generation wireless with strategic thinking in terms of scale and dimension of the project.

THE BUSINESS INITIATIVE: STRATEGIC PLANNING

The quest for the ultimate business case has been the Achilles heel of IPv6. The business climate has been hostile to investments in new technologies since the Internet and 3G spectrum bubbles and successive disruption from terrorism attacks and war. The focus has been squared to squeezing maximum revenues from the current infrastructure.

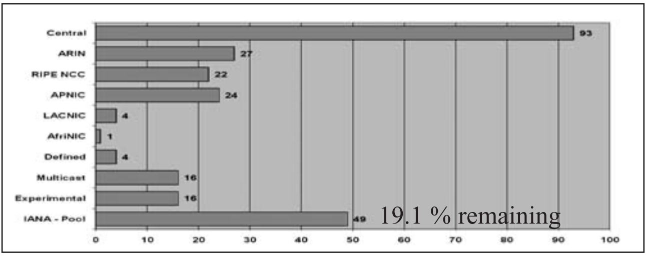
Since IPv6 is viewed primarily as a long-term plumbing exercise, it's quite obvious that even if it offers the best of breed features it does not suffice to justify the investment in the plumbing. Unlike Y2K, there is no 'big bang' date at which IPv4 address space will run out; thus there is no perceived urgency in IPv6 deployment while ISPs can take revenue from IPv4 deployment. The choice between an immediate deployment and a gradual technology refresh is fairly obvious depending on the size of the address space allocated to the region in question.

The address space as the first strategic driver

The new study published in Sep 2005 by Tony Hain @ Cisco demonstrates an alarming trend in the rate of IPv4 address depletion. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html

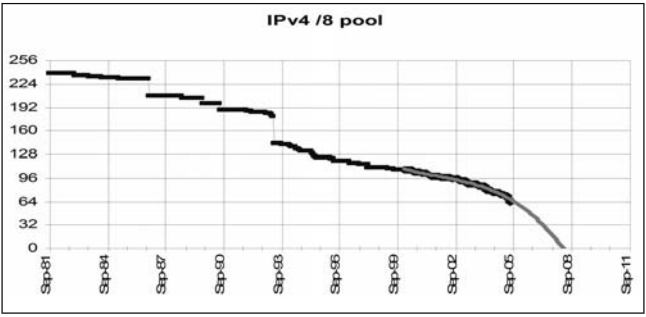
The following chart shows the distribution of all 256 IANA /8 allocation units in IPv4 as of January 16, 2007. The Central registry represents the allocations made prior to the formation of the Regional Internet Registries (RIRs). ARIN (North America) [2], RIPE NCC (Europe) [3], APNIC (Asia/Pacific) [4], LACNIC (Latin America) [5], and AfriNIC (Africa) [6] are the organizations managing registrations for each of their respective regions. RFC 3330 [7] discusses the state of the Defined and Multicast address blocks. The Experimental block (also known as Class E—RFC 1700 [8]) was reserved, and many widely deployed IPv4 stacks considered its use to be a configuration error. The bottom bar shows the remaining useful global IPv4 pool. To be clear, when the IANA pool is exhausted there will still be space in each of the RIR pools, but by current policy [9] that space is expected to be only enough to last each RIR between 12 and 18 months.

Jan. 16, 2007



IANA allocated 25 /8's between Jan. 1, 2004 and Jan. 5, 2006
Typical RIR re-allocation period 9-12 months

The following graph provides the exhaustion perspective, showing the entire address pool from the publication of IP Version 4 (note that data prior to 1995 is accurate as to where it was allocated, but with very coarse granularity as to exactly when). The projection curve is based on the IANA allocations from January 2000 onward.



This study will be reviewed and updated by Tony Hain on a quarterly basis: http://www.tndh.net/~tony/ietf/ipv4-pool-combined-view.pdf

The first independent study on IPv6 by RTI for US DOC
In February 2006, the US Department of Commerce released the first independent study of the fast-forming IPv6 marketplace, as well as a cost-benefit assessment of the transition to IPv6. http://www.ntia.doc.gov/ntiahome/ntiageneral/ipv6. Some of the highlights of this report, which were supported by RTI International's economic impact analysis in the latter half of

2005, should make businesses and government organizations sit up and take notice.

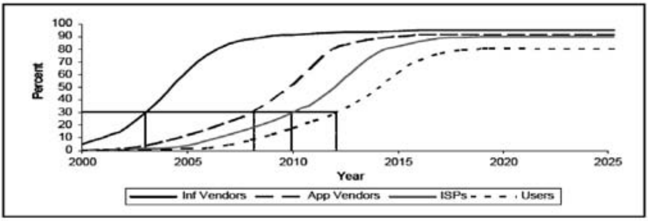
The report presents estimates of the costs and benefits associated with transitioning from Internet Protocol Version 4 (IPv4) to Internet Protocol Version 6 (IPv6). Cost estimates are based on likely development and deployment scenarios provided by stakeholders during interviews conducted by RTI International (RTI). Based on these interviews, RTI estimates the present value of incremental costs associated with IPv6 deployment over a 25-year period to be approximately $25 billion ($2003), primarily reflecting the increased labour costs associated with the transition. Although these cost estimates seem large; they are actually small relative to the overall expected expenditures on IT hardware and software and even smaller relative to the expected value of potential market applications.

Because major applications for IPv6 have yet to emerge, it is more difficult to quantify their potential benefits. Stakeholders participating in this study identified several major categories of IPv6 applications that, in total, are estimated to have potential annual benefits in excess of $10 billion. These categories include Voice over IP (VoIP), remote access products and services, and improved network operating efficiencies.

However, benefits estimates included in this report are more subjective than cost estimates because they are based on Internet applications that are not yet well-defined. In addition, benefit estimates are potentially conservative because they do not reflect future, next-generation applications that may be enabled by IPv6.

Based on interviews with stakeholders, the penetration curves in Figure ES-1 were constructed to represent likely deployment/adoption rates for the four major stakeholder groups. The infrastructure and applications vendors' curves represent the path on which vendor groups will offer IPv6-capable products to customers. For example, based on information provided in interviews, RTI estimates that 30 percent of infrastructure products offered by vendors were IPv6-capable by 2003, and 30 percent of Internet applications offered by vendors are projected to be IPv6-capable by 2008.

Figure ES-1. Penetration Estimates of IPv6 in the United States



The ISP curve represents the share of ISPs’ networks that are expected to be IPv6-enabled. As shown in Figure ES-1, RTI estimates that, on average, 30 percent of ISPs’ networks will be IPv6-enabled by 2010. Similarly, the users curve represents the share of users’ networks (including infrastructure vendors, application vendors, and ISPs’ internal network users) that is projected to be IPv6-enabled. For example, on average, 30 percent of users’ networks are projected to be IPv6-enable by 2012.
The analysis of the report for the US market includes:

- A services market that is approximately $25 billion over the next quarter century.
- A market that generates $10 billion in cost savings EVERY YEAR.
- A market that for every dollar invested returns $10 in cost savings.
- A market that has 8 cents of every dollar going toward the actual infrastructure update, with the other 92 cents being invested in taking advantage of it.
- A market that has important cost savings in 4 key areas:
  - Improved security
  - Increased efficiency
  - Enhancement of existing applications
  - Creation of net-new applications

We see a market that is enabled by creative thinking, solid training, and enlightened delivery mechanisms. This report should act as a sign post to prosperity. Too early to be a road map, but a powerful indicator for forward thinking organizations around the globe.

No longer is IPv6 an 'unfunded mandate' waiting for a multi-billion dollar appropriation from the US Congress or any other government. Now we have the first independent assessment of this new marketplace as a large market, with a ten to one return on investment, which unlocks hidden value within organizations while saving them real dollars in operations.

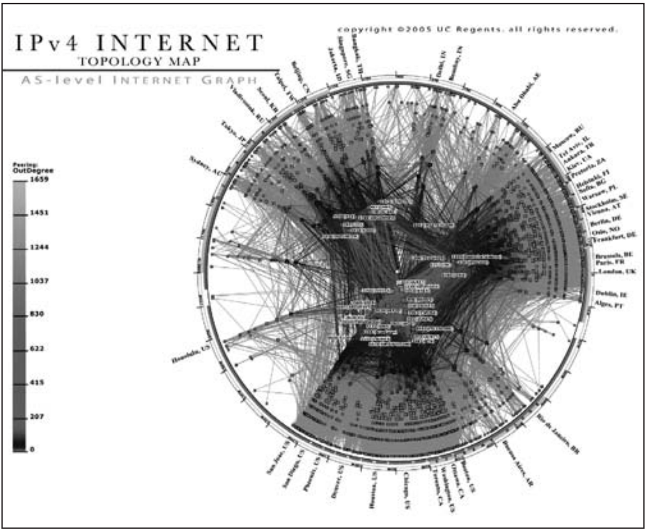
The RTI report has prompted the very senior Washington DC business executive, Jim Garrettson, to organise an IPv6 briefing conference in DC as part of his ExecutiveBiz briefings to Corporate CEOs and Congressmen. Congressman Tom Davis, an advocate of IPv6 has accepted to join. The president of the IPv6 Forum was invited to deliver a keynote on The New, New Internet IPv6: Technology's Next Big Step:
https://www.execbizevents.com/ExecutiveBiz/events/event.php?event_id=17

FIRST CONCLUSIONS AND RECOMMENDATIONS

IPv6 is the place to be. IPv6 is already available to forward-thinking countries and corporations wanting to sustain an advantage over their competitors. Only now have European organizations begun taking steps towards a transition to IPv6. This document describes the features and functions that will keep them competitive globally.

The Deployment of IPv6 worldwide: The world upside down!

The following chart shows that IPv4 connections are highly meshed around a very dense core with MCI/UUNET (now Verizon) at its centre. The US has by far the highest density of networks.

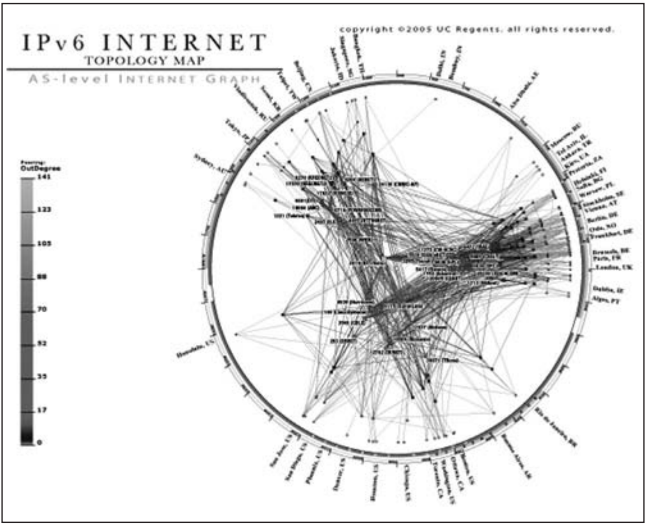


Source: Page URL: http://www.caida.org/analysis/topology/as_core_network/AS_Network.xml Last updated: Tue Jul 19 14:34:10 PDT 2005. Maintained by: Bradley Huffaker

The following chart shows that the number of IPv6 connections is increasing constantly, reaching a respectable size. Europe leads with over 50% of the connections. A comparison between the densely connected IPv4 and the IPv6 world demonstrates the readiness of the non-US based networks and the possible domination of their IPv6 services in the future

This visualization represents a macroscopic snapshot of the IPv6 Internet topology collected around March 4th, 2005. The topology data was gathered from 17 monitors probing approximately 860 globally routable IPv6 network prefixes include 2,913 IPv6 addresses and 7,905 IPv6 links.

This view aggregates the network into a topology of Autonomous Systems (ASes). Each AS approximately corresponds to an Internet Service Provider (ISP). Each IPv6 address is mapped to the AS responsible for routing it, i.e., to the origin (end-of-path) AS for the IPv6 prefix representing the best match of this address in Border Gateway Protocol (BGP) routing tables.



In comparison with the IPv4 AS graph, the IPv6 AS graph is much sparser with drastically fewer nodes and less richness of peering observed. The geographical patterns of the graphs also differ. While the majority of ISPs with the highest outdegrees in IPv4 space are all located in the U.S., the company with the richest observed IPv6 peering is NTT/Verio headquartered in Japan, with 141 peers. The largest cluster of high degree IPv6 AS nodes is in Europe (clustered around Tiscali which is headquartered in Germany – is actually headquartered in Italy, see http://en.wikipedia.org/wiki/Tiscali) in the graph.

THE WAY FORWARD

Industry worldwide is called upon to:

- Promote VoIP over IPv6: the other immediate and strategic area where IPv6 could be introduced immediately is in VoIP. An effort to convince the telecoms industry and operators is key, as in the US corporate operators are deploying VoIP to eat their own lunch. Operators need to be convinced to take a new approach to VoIP using IPv6.
- Promote IPv6-ready technologies and the companies working in the ICT domains, facilitate the development and growth of SMEs working in new innovative ICT fields, and promote the

use of SME products by the large groups. One area we should focus on is software. Innovation comes mainly from software. Off-the-shelf networking software drastically reduces time to market and costs.

- Promote open source Linux implementation of IPv6. http://www.bieringer.de/linux/IPv6 and BSD
- Promote IPv6 for home networking. The IPv6 Forum partnership with CENELEC outlines the technical guidelines and practices to achieve successful use of IPv6 in the home connectivity market: http://www.european-ipv6-tf.org/Whitepapers/Forms/AllItems.aspx
- Fully participate in the R&D activities with a view to put in place an integrated and structured set of IPv6 activities, covering the full range of IPv6 aspects, from basic research through the development of service enablers and associated software suites, to the large scale trialling and testing of IPv6 features, for a diversity of applications.
- Actively contribute to the acceleration and alignment of ongoing IPv6 work within standards and specifications bodies and urgently develop key guidelines permitting the rapid integration of IPv6 infrastructures and interoperability of IPv6 services and applications, especially in The IPv6 Forum Ready Logo Program: http://www.ipv6ready.org
- Where appropriate, develop roadmaps for the design, development and deployment of IPv6 services, equipment and networks, to include technologies such as AAA, DNS, xDSL, etc.
- Contribute actively to the work of the National IPv6 Forum /Task Forces, ensure the collectively increase of IPv6 awareness and permit its members to individually derive their own perspective of the IPv6 business case and their own IPv6 integration strategy.
- Devote efforts towards the establishment of a worldwide, vendor-independent training and education programme on IPv6.
- Consider in their manufacturing plans that the majority of mobile devices, and a growing number of household and consumer electronic devices will require some form of IP connectivity and that the simplest way to offer these devices the fullest range of services is to have a unique globally routable

IPv6 address available for all network-enabled components.

- Seek to develop innovative IPv6-enabled devices, e.g. biometric security devices, “IP in a chip” embedded systems components, in-car sensor devices. Seek to design and implement innovative peer-to-peer applications where appropriate, e.g. peer-to-peer gaming in the entertainment industry.
- Take early steps to obtain adequate IPv6 address allocations and where appropriate, and to either accelerate the offer of IPv6 capable services or consider on a priority basis how best to rapidly evolve towards IPv6.
- Address the multi-vendor interoperability issues impeding the wide-scale deployment of PKI (public key infrastructure) and to conduct extensive trials with IP security in IPv6 and the parallel implementation of a PKI.
- Promote IPv6 over satellite and HDTV over IPv6: with the advent of all-digital TV by 2010, there is a clear potential in this strategic market. It would be highly recommended to promote High Definition Video (HDV) delivery service over IPv6 Internet by:
  - Establishing operation and extension of IPv6 network infra for HDV content delivery service.
  - Applying network-monitoring tools for analyzing the number of users and IPv6 traffics with VoD service.
  - Developing HDV content service techniques based on VoD and its management schemes.
  - Building VoD servers & websites for HDV content (e.g., cultural, medical, educational multimedia content) service and testing operation and by developing multi-user remote videoconference system based on HDV

Stability, Security and Sustainability in ccTLD Management for the Internet

Elmar Knipp,
Chairman of the Board of DENIC eG, Frankfurt

The Internet is one of the world's most vital resources, playing an important role in nearly every aspect of our lives – be it business, education, politics, religion, health or personal and social relationships. As such, proper administration of the Internet, and its underlying technological infrastructure, is critical and should be handled with great care. One part of this administration is managing the domain name system, e.g. for a country code top level domain such as .de.

DENIC AS A COOPERATIVE – A TEAMWORK OF COMPETITORS

Although the various registries throughout the world have very different organizational forms, the work of all of them is based on a single fundamental document dating back to 1994: RFC1591 "Domain Name System Structure and Delegation". The term that RFC1591 uses in this context is "Trustee for the delegated domain". This TLD Manager is an organization that must comply with a number of requirements and duties:

- it must have the technical competence to do a do a satisfactory job of operating the DNS service for the domain
- it has a duty to serve the community
- it must be able to carry out the necessary responsibilities, and have the ability to do an equitable, just, honest, and competent job
- it must be equitable to all groups in the domain that request domain names

- significant stakeholders in the domain should agree that the designated manager is an appropriate choice.

So it is up to the local Internet community in each country to decide how to organize the administration of its specific national Top Level Domain which is known as the “country code Top Level Domain” or “ccTLD” for short. As a result there are many different models for structuring domain administration in the various parts of the world. Within Europe in many countries, including Germany, this organizational matter was carried out through a collaborative effort of the affected industry, academic institutions and users.

DENIC came about as a result of an industry initiative. This form of self-administration is entirely in harmony with the open structures of the Internet as a global medium, since it is based on the principles of decentralized distribution of responsibilities and resources as well as self-regulation through the interest groups concerned. DENIC's legal form is that of a registered cooperative. It was set up in December 1996 and has its headquarters in Frankfurt am Main, Germany. Its membership is comprised of companies and institutions who administer domains for their customers and who feel an active commitment to providing, within the principles of self-regulation, a key service for the whole German Internet community – namely, operating the registry for .de, Germany’s top level domain.

All members of the cooperative form the General Assembly, through which all fundamental decisions, such as the basics of business policy and changes to the cooperative’s bylaws, are made. The General Assembly elects the Supervisory Board and the honorary members of the Executive Board. Full-time members of the Executive Board are appointed by the Supervisory Board. The Executive Board is responsible for managing the cooperative in accordance with legal regulations and the bylaws. In this capacity, the Executive Board is advised, supported and supervised by the Supervisory Board. Alongside the Executive Board, there are two councils which advise the Executive and Supervisory Board in legal resp. [?] technical matters. For example, the Legal Advisory Council assisting DENIC's decision-making bodies on questions regarding registration policy is comprised of representatives of trade associations, academics and legal specialists as well as observers from the German Federal Ministry of Economics and Labor and the German Federal Ministry of Justice.

DENIC is a not-for-profit body and sees itself as a neutral service provider for a key infrastructure for the German Internet. This mission is also defined in its bylaws as a central element and thus represents the foundation for all its activities. Setting up DENIC in the form of a cooperative also has the advantage of having an open structure for the registry itself. New companies can join the cooperative at any time and participate in DENIC's discussions and decision-making. DENIC's bylaws provide that decisions shall be achieved by majority rule or, in important cases like changes to the bylaws, by supermajority, where each member has one vote. Corporate profits and company size of the individual members do not play a role, ensuring that small companies cannot be overruled by a few larger companies.

So all of DENIC's work is impartial, independent, informed, responsible, non-discriminating and in conformity with internationally recognized standards for running a domain registry. The appeal of this model is shown in the steadily increasing number of companies that have joined DENIC over the years. In 2002, the bylaws were modified to open membership to a larger circle of applicants. In order to become a member, one must be active in the area of domain administration as well as be able to prove technical competence and financial stability. This modification of the terms of admission led to a further increase in membership.

The history of domain administration in Germany, which is also DENIC's history, has been a resounding success story. In just a few years, more than eleven million domains were registered and a stable, highly dependable infrastructure set up. In the end, every domain holder and user benefits from this. DENIC will continue to maintain this close cooperation and collaboration with its members and the German Internet community.

A COMPETENT, RELIABLE PARTNER

As the registry for .de DENIC administers a resource that is of crucial importance for the operation of the Internet. DENIC's functions and tasks are multifaceted: first, provision of an automatic electronic registration system for administering .de domains. Secondly, operation of a network of name servers distributed throughout the world. And last but not least, a range of additional services for the German Internet community to ensure the uninterrupted availability of information and data (24/7).

The network of name servers for the .de zone currently consists of 14 powerful name server locations, most of them serving in a state-of-the-art anycast setup. Having the name servers spread all over the world like this ensures that the information is available at any time and with very short response times everywhere. Together, the .de name servers respond to more than 2 billion queries every day, i.e. each location handles an average of around 2,000 queries per second. The current practice is to reload the .de zone with the latest domain data at least twelve times a day.

Since DENIC represents an important interface to the Internet, it must ensure that its services are always available. Accordingly, high demands are placed on the equipment. In addition to that, security aspects play a significant role. The system must be powerful as well as secure. Redundancy at all levels is not a luxury, but an absolute necessity. For this reason, DENIC operates two independent data centers. At both centers, every single component is redundantly organized so that each service is provided by at least four different servers. This ensures high availability and operating safety even in exceptional situations. Permanent monitoring of the services in state-of-the-art operation centers is an essential part of the security concept. Running systems are constantly supervised by DENIC's employees as well as by automated software routines. Trend analyses, runtime monitoring and the correlation of various technical indices provide the basis for quick adjustments and long-term planning. DENIC relies on redundancy for its Internet connection as well. It maintains several independent connections to the Internet, each of them secured with a staged firewall. Every externally accessible service is insulated by an additional firewall from the DENIC internal network in which the actual processing and storage of the data takes place. However, even the most elaborate security network could not fulfill its purpose without employees who are aware of the potential security gaps. So it is safe to say that DENIC's most important resource is its competent, motivated and qualified staff. Continual on-the-job training and outside coaching ensure that employees have the expertise to deal with an ever-changing and developing work environment. As an IT training provider, DENIC takes seriously its responsibility to train qualified entry-level associates. Due to the professionalism and know-how of its employees, DENIC has gained an excellent national and international reputation as a reliable, competent and influential partner.

DOMAIN DISPUTES

The Internet is not an unlegislated area. This is of course also true when it comes to the protection of trademark, name or company rights. Many companies invest a large amount of time and money in advertising and building an Internet website. A well-established domain therefore may represent significant value.

Domain registration is handled on a "first come, first serve" basis. But all domain holders are personally responsible for making sure that their domains do not infringe the rights of anyone else. For this reason, anyone who feels that their rights have been infringed by a domain must contact the holder of that domain and not DENIC. Compared with the total of over eleven million registered .de domains, the number of disputes is extremely low, and it would appear that little more than one domain in a thousand is affected by some sort of disagreement. However, that does not mean that disputes do never occur. Just like the real world, the Internet is not a place where the whole of humankind manages to live in uninterrupted peace and harmony. Whenever there are disputes over the Internet that concern names, these are settled by applying the same laws and rules as are used for analogous disputes elsewhere.

It is not DENIC's job to become involved in such disputes in any way. DENIC does not 'police' the contents and/or legality of domains; responsibility for any infringement of the rights of others resides entirely with the holder of the domain concerned. This view of the legal situation was also expressly confirmed by Germany's Supreme Court (Bundesgerichtshof) in May 2001 in its verdict in the 'ambiente.de' case. It is only when a dispute over a domain has been brought to a definitive conclusion, especially if there is a final and absolute court judgment on the substance of the case against the party holding the domain, that DENIC intervenes – if it is still necessary to intervene at that stage.

DENIC has, however, created a measure that can be of assistance to any claimant who feels that his or her rights have been infringed by a domain. It is known as a DISPUTE entry. When a domain involved in a dispute has a DISPUTE entry placed on it, it becomes impossible for its holder to transfer it to a third party. What is more, the party in whose name the DISPUTE entry has been lodged automatically becomes the new holder of the domain should the existing holder decide to abandon it.

COMMITMENT TO THE INTERNATIONAL INTERNET COMMUNITY

With regard to design and administration, the Internet is largely decentralized. Therefore, various organizations and institutions worldwide look after its general technical, administrative and conceptual coordination and further development. Thanks to its expertise, DENIC has earned much trust and respect in recent years, in Germany and internationally. However DENIC has no intention of resting on its laurels, since the Internet will continue to change and transform. Germany’s Network Information Center is in permanent contact with international bodies, organizations and associations who are concerned with the Internet, and maintains an active dialogue with representatives of the Internet community all over the world. The overall goal of this dialogue is to ensure the stability and sustainability of the Internet today and in the future.

Users and Internet Governance – The Structure of ICANN's At-Large Advisory Committee (ALAC)

Annette Mühlberg,
ICANN’s At Large Advisory Committee (ALAC), Berlin

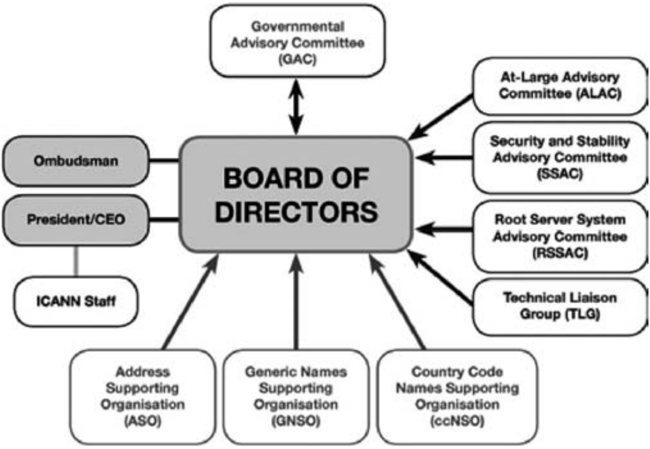
At present, there are one billion Internet users. Their participation – writing, reading, commenting, purchasing – makes the Internet the vibrant space it is. Who stands up for them – and the five billion users yet to come – and protects their interests with regard to the governance of the Internet?

At its founding, ICANN was designed to recognise the Internet-using public as not just a part, but as the most important part of the organisation’s constituency. Its original bylaws gave half the seats on its board to representatives of individual Internet users. In the year 2000, a first direct election of five directors of the ICANN Board took place, in which everyone who owned an email address could take part. Over time, this procedure has been changed step by step. A reform took place that led to the implementation of the Interim At-Large Advisory Committee (ALAC). „Interim“, until the ALAC would have been fulfilled the task of strengthening the regional representation of individual internet users and involving them in the ICANN decision making processes via a regional organisational structure.

The competences of the (Interim) ALAC were reduced to giving advice to ICANN in the interest of individual users and to have non-voting liaisons to the ICANN Board, Committees, Supporting Organisations and working groups.

HOW IS THE ALAC EMBEDDED IN THE ICANN STRUCTURE?

ICANN is based on several constituencies, supporting organisations and advisory committees; for example the Generic Name Supporting Organisation (GNSO) (with its five commercial and just one non commercial constituencies) and the Governmental Advisory Committee (GAC, which gives governmental perspective on public policy). More information about ICANN can be found under www.icann.org.



Governmental Advisory Committee (GAC)
At-Large Advisory Committee (ALAC)
Ombudsman
BOARD OF DIRECTORS
Security and Stability Advisory Committee (SSAC)
President/CEO
Root Server System Advisory Committee (RSSAC)
ICANN Staff
Technical Liaison Group (TLG)
Address Supporting Organisation (ASO)
Generic Names Supporting Organisation (GNSO)
Country Code Names Supporting Organisation (ccNSO)

In the chart above, the GAC is the only committee with arrows in both directions: if the Board of Directors does not follow the advice given by the GAC, the Board is obliged to provide an explanation to the GAC for why it did not do so. This should also be the case for the ALAC, for which the Board looks rather like a one-way tunnel: information and advice goes in, but the policies that come out may bear little relation to them. When that happens, the bylaws should obligate the Board to explain why.

The ALAC has several non-voting liaisons: to the Board, GNSO, ccNSO, SSAC, and to several working groups on IDNs, Whois etc. As the core function of ALAC is to give advice to ICANN relating to the interests of individual Internet users, the question is: what are these interests?

INTERESTS OF INDIVIDUAL INTERNET USERS

ICANN is supposed to be responsible for the technical coordination of Internet resources: domain names, IP addresses, protocols. It is designed to respond quickly to preserve the stability and security of the Internet's global network of networks. Individual Internet users are affected by many of these issues. They may want domain names to provide stable online identifiers for writings (blogs, websites), and e-mail addresses that last beyond a current employer or school affiliation; they use IP addresses when they connect to the Internet; as users and programmers, individuals have a stake in the ease with which new connections can be made and new protocols developed. As private citizens, they are concerned both by mandated disclosures of personal information in domain name registration records and the accountability of those who operate websites. Recently, as domain name registrar RegisterFly went rogue, throwing thousands of domain names into ownership limbo, and reports of domain name hijackings have increased, individuals wonder to whom they can turn to secure domain name registration rights.

Further interests of individual Internet users include:

- Domain name pricing, and competition in the provision of domain names.
- Transparency of policies, such as how somebody can apply for running a new top-level domain (such as .com or .jobs)? It is a little bit like running for president in the USA – up to now, a lot of money for lobbying is needed.
- What new top-level domains will be made available, and who will be able to register there? Proponents have been suggesting new geographic TLDs, such as .paris, .nyc, .berlin, open to anyone in the region as a way to self-identify online materials. Will the namespace be censored on dubious morality claims or commercial special interests?
- Data protection: In many countries, privacy of personal information is recognized as a core human right. Must individuals give up that right in order to register a domain name?

THE AT-LARGE ADVISORY COMMITTEE

The Interim ALAC has been constituted as an advisory body. Tasked with aggregating the diverse views of individual Internet users around the world, through five regional structures and 15 representatives, it "is responsible for considering and providing advice on the activities of the Internet Corporation for Assigned Names and Numbers (ICANN), as they relate to the interests of individual Internet users (the "At-Large" community)."

Yet its many layers of structure and its interactions with ICANN staff, who frequently have conflicts of interest between ICANN policy staff and the community they are meant to serve, make it difficult for ALAC to involve Internet users in ICANN's decision-making processes. For many, there are too many layers of indirection between individual participation and impact on ICANN policymaking.

To strengthen regional Internet users' representation, the interim ALAC set up Regional At-Large Organisations (RALOs), one in each of the five ICANN regions: Asia Pacific, Africa, Europe, Latin America, North America. A lot of work went into this task, and it had been finalized by the last ICANN meeting in June 2007.

The Regional At-Large Organisations manage outreach and public involvement and are designed to be the main forum and coordination point for public input to ICANN in each region. The RALOs consist of individuals and so called At-Large Structures (ALSes) which are Internet-user-related organisations in general: non-profit, non-governmental, non-business (as there are other bodies in ICANN covering their interests, eg., governmental advisory committee, business constituency). Each RALO appoints two members from its region for the At-Large Advisory Committee.

On June 29, 2007, the last Interim ALAC member was replaced by elected representatives and the Interim ALAC therefore became the full-fledged ALAC.

REAL INDIVIDUAL REPRESENTATION AND PARTICIPATION

The time has come to look forward. Now that the structures are in place, it is time for ICANN to turn them into meaningful opportunities for the participation of individual Internet users. The ALAC needs to have a clear feedback procedure for the advice it gives to the Board (analogous to the GAC). ALAC's representation on the Board should be reconsidered if ALAC or individuals, as originally contemplated, are to be able to elect voting Board members and voting liaisons. The ALAC and its constituent parts should provide real policy advice, and should get substantive discussion of and response to their recommendations.

As for substance, ICANN should squarely address the questions of freedom of expression, privacy, stability, and market competition that individual users and many of its other constituencies have been raising.

Chapter 6

Emerging Issues

Towards Multi-Stakeholder Governance – The Internet Governance Forum as Laboratory

Bertrand de la Chapelle[1],
Special Envoy for the Information Society, French Ministry of Foreign and European Affairs

When Tim Berners Lee invented the World Wide Web, few people imagined it would so rapidly and deeply impact almost every human activity. Likewise, the apparently modest and informal Internet Governance Forum created by the World Summit on the Information Society in Tunis in 2005 did not immediately reveal its potential. Nonetheless, this innovative experiment is the laboratory of a new multi-stakeholder governance approach dearly needed to address the complex issues of our interdependent and interconnected world.

The IGF is a dialogue space for governments, the private sector and civil society actors to discuss Internet-related public policy issues in an innovative format. It is a self-organizing process whose working methods help define the very methodology of multi-stakeholder governance. Focusing on this procedural aspect, the present paper describes: A) the four key dimensions of the WSIS definition of Internet Governance, B) the innovative practices already pioneered by the IGF in each of them, and C) the critical path forward for this important but fragile experiment.

[1] Contact : bdelachapelle@gmail.com

A – THE FOUR COMPONENTS OF THE INTERNET GOVERNANCE DEFINITION

What is Internet governance? Do we all have a common understanding of this notion? The Tunis Agenda for the Information Society established a now well-known definition: “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes that shape the evolution and use of the Internet”. This definition can be broken down into the four major components of Internet governance: scope, instruments, process and actors.

1 – THE SCOPE OF INTERNET GOVERNANCE: “THE EVOLUTION AND USE OF THE INTERNET”

In the technical community, “Internet governance” initially covered the management of the Internet’s so-called “core resources”, particularly IP addresses and the Domain Name System (DNS), which since 1998 has been administered by the Internet Corporation for Assigned Names and Numbers (ICANN). Beyond technical aspects, the growing use and ubiquity of the Internet raise new public policy issues such as: the fight against spam and cybercrime, freedom of expression, the protection of privacy and personal data, multilingualism, right of access, etc. These issues are transnational, multi-actor, multilevel (local actions can have global impact) and non-linear (no proportionality between causes and effects: a few lines of code replicating virally can infect millions of computers in a few hours). The present intergovernmental framework has difficulties handling these complex issues: they often cut across institutional mandates and also challenge national sovereignties. Addressing them is nonetheless an increasingly urgent task.

During WSIS, participants progressively recognized “Internet governance” as covering not only the management of the infrastructure (as in the technical definition of the term) but also the public policy issues related to the applications it supports. In other words, Internet governance represents both governance “of” the Internet (the evolution of its infrastructure) and “on” the Internet (its use).

2 – REGIMES: THE TOOLSET FOR INTERNET GOVERNANCE

Some early pioneers envisaged an Internet beyond the bounds of traditional regulation, and expected this emerging medium to continue developing forever without much regulation, bypassing existing legal authorities. But there is broad recognition today that in fact a very wide variety of rules and regulations at national, regional or international levels apply to the global network. These rules are elaborated in numerous frameworks: standards organizations, business structures, national governments, regional groupings, international and intergovernmental organizations.

The result, in some domains, is a very complex mesh of competing, overlapping and sometimes conflicting rules and, in others, a lack of instruments to address pressing issues at the appropriate level. Business actors find it difficult to abide by sometimes incompatible legal rules; governments feel stripped of their regulatory capacity or unable to fight malevolent actions; civil society actors worry about the potential erosion of some fundamental principles.

“Principles, norms, rules and decision-making procedures” are the four components of a regime in international regime theory. Adding the word “programmes” to the TAIS definition of IG echoes Lawrence Lessig’s “Code is law”. It expands this notion of regimes to include technical standards and computer code because apparently technical options (eg the end-to-end principle) also shape the evolution and use of the Internet. Conversely, “embedding law in code” will be an important component of designing future regimes: integrating agreed legal provisions in technical standards facilitates their implementation and enforcement.

According to the TAIS definition, Internet governance is therefore about the broad range and diversity of regimes shaping the evolution and use of the Internet: existing ones (which need to be made more compatible or interoperable) and new ad-hoc ones (which need to be somewhat globally applicable).

3 – INTERNET GOVERNANCE AS DEVELOPMENT AND APPLICATION OF REGIMES

In an ever-changing environment, all sorts of new standards and new regulations are continuously created and implemented in a vast diversity of frameworks, each with their own membership and internal procedures. Yet, all these processes include development and application phases, as mentioned in the TAIS definition.

The development of new regimes (as well as efforts to harmonize existing ones) is an iterative process where the early stages of issue-framing and scoping are essential. Identifying existing applicable regimes, relevant actors and frameworks, as well as formulations acceptable to all actors involved is fundamental before any regime drafting can take place. The drafting phase is also iterative. It requires ad-hoc working groups, the composition, terms of reference and working methods of which are critical to the success of the discussions. In Internet matters at the international level, which involve complex technical, economical, social and political aspects, governments are not in a position to frame issues or define viable regimes alone: new, more open and inclusive processes for coordination and drafting are required.

But Internet governance is not just about the development of regimes. Their effective application is highly critical because the proper functioning of the network affects, on a daily basis, the activities of close to a billion people. Unfortunately, international negotiations have too often paid insufficient attention to the implementation and enforceability of otherwise carefully negotiated agreements. Internet governance therefore requires a deeper attention to the application phase of any agreed regime. According to the TAIS definition, Internet governance thus covers initiating, drafting, implementing and enforcing a wide variety of regimes.

4 – ACTORS IN INTERNET GOVERNANCE: THE MULTI-STAKEHOLDER APPROACH

The fourth component of the TAIS definition refers to the responsibility of "governments, the private sector and civil society, in their respective roles" in the development and application of regimes. This is the core notion of multi-stakeholderism produced by the WSIS.

On the surface, the World Summit on the Information Society looked like just another UN summit. Upon closer scrutiny, this dynamic and emergent process forced hundreds of diplomats, business people, civil society actors and technical specialists to interact during four years. In that context, governments progressively had to accept the undisputable competence, and therefore legitimacy and utility, of actors from business and civil society who had not only invented but built and managed the now-ubiquitous global Internet at a time when few governments were paying attention. By the same token, civil society and business actors were forced to recognize that the complex new policy issues raised by the growing use of the Internet could not be addressed without some government involvement. This ran contrary to early claims that the Internet made governments obsolete and that Internet-related issues should be the sole province of the private sector (via self-regulation) or the technical community. This mutual recognition allowed the use in the Geneva documents of a single generic term: "stakeholders", to designate the different categories of actors. But they were still implicitly supposed to remain separate. The second phase of the Summit, on the contrary, saw the emergence of the expression "multi-stakeholder", ultimately appearing more than 15 times in the Tunis Agenda for the Information Society (TAIS). This recognition of the joint responsibility of all stakeholders in Internet governance and the necessity of their cooperation can be considered one of the main achievements of the four-year UN process.

"In their respective roles" should not, however, be interpreted as assigning separate roles to each category of actors. Involving all of them together is necessary. First of all to guarantee that all technical, economic, social and political aspects are taken into account early on in the issue-scoping and elaboration of regimes; and secondly to facilitate enforcement: all actors are needed at the implementation stage, and they will only be willing to engage if they can participate and are taken into account at the drafting stage.

This does not mean either that anyone can or should participate in all discussions at all levels. Participation of stakeholders is likely to vary according to the issues, the venue where they are discussed and the stages of the discussion. Defining transparent, non-discriminatory rules to identify "relevant" stakeholders for each issue will be delicate. But the basic principle of multi-stakeholderism is the fundamental right of any actor to participate, in an appropriate manner, in the governance process by addressing issues they are concerned with or impacted by.

Based on the four elements above, a more compact and simpler definition emerges: "Internet governance is the multi-stakeholder development and application of shared regimes that shape the evolution and use of the Internet". In this context, the innovative Internet Governance Forum (IGF) established by the Tunis Summit represents a unique laboratory for defining concrete modalities for this new concept of multi-stakeholder governance.

B – THE IGF PIONEERS' INNOVATIVE PRACTICES

Although formally attached to the United Nations Secretary General, the IGF is a self-organizing process which develops its own rules of procedure. In the four dimensions above, the inaugural meeting in Athens (and most likely the second one in Rio) introduced important pragmatic practices, markedly different from the traditional intergovernmental system. They demonstrate the feasibility and benefits of the multi-stakeholder approach.

1 – FLEXIBLE AGENDA-SETTING

The scope of Internet Governance is both governance "of" the network (its infrastructure) and governance "on" the network (its uses). But given the vast range of issues, how does the IGF set its agenda? And how does it handle contentious issues?

In traditional intergovernmental organizations, full consensus among all governments is usually required prior to putting any subject on the agenda. This often delays the handling of contentious issues. In stark contrast, the IGF bootstrapped itself with a flexible and adaptive agenda-setting procedure that empowers participants. Preliminary consultations for the Athens IGF meeting established a dual approach, combining top-down and bottom-up components, facilitated by a lean secretariat and a multi-stakeholder Advisory Group, under the chairmanship of the UN Secretary-General's Special Advisor for Internet Governance.

On the top-down side, four main sessions (Security, Openness, Diversity and Access) aggregated the exceptional variety of issues into a limited number of easily understandable thematic clusters. Capacity Building and Development were two additional cross-cutting themes. These themes were neutral and formulated as positive objectives. They nonetheless allowed discussion of some contentious issues in Athens, such as interconnection costs in the Access session or Freedom of expression in the Openness session. In the same vein, the preparation of the second annual event in Rio introduced a fifth theme, "Critical Internet Resources", to cover, among other things, sensitive topics that had put the whole WSIS at risk, including management of the DNS.

In parallel to this top-down definition of major themes, and in order to facilitate the bottom-up emergence of issues, all participants were given the opportunity to propose and organize workshops on their specific issues of interest or concern. As a relatively limited number of proposals were received, all were accepted and more than 30 self-organized workshops took place in Athens. The second IGF annual event in Rio generated a considerably higher number of workshop proposals. Their convenors were encouraged to merge them to keep numbers manageable in the available time.

In the future, as the number of workshop proposals increase, it will be necessary to establish criteria to select among them (such as the diversity of their organizers or panellists) and mechanisms to facilitate their merging. This should be taken into account when the mandate and composition of the Advisory Group created for Athens is reviewed.

This flexible process helps to prevent the risk of paralysis of traditional agenda-setting by formulating "Issues of Common Concern or Interest" that actors recognize should be addressed, even if they disagree on where to address them or on the solutions. The Rio meeting will organize a clearer link between workshops and the main themes they relate to. This combination of top-down and bottom-up approaches should allow a constantly evolving agenda for the IGF with faster reaction times than other, more traditional processes.

2 – THE EQUAL FOOTING OF STAKEHOLDERS

Another essential difference between the IGF and existing intergovernmental organizations is the absence of separation between the different stakeholders, and their participation on an equal footing. Seating in all sessions in Athens was on a "first come first served" basis. No United Nations-related organization had ever adopted such a radical format. Even the International Labour Organization (ILO) keeps its tripartite representation of governments, employers and trade unions as separate constituencies. Still, although the absence of nameplates and reserved seats was initially startling for many governmental participants, all attendees finally recognized that it illustrated the spirit of multi-stakeholderism and largely contributed to the informal and fruitful nature of the exchanges.

Participation in the work of the Internet Governance Forum is open to any interested actor, even individuals. This stands in stark contrast not only to the traditional exclusive competence of governmental representatives, but also with the heavy accreditation procedures for even the most open UN conferences or summits. More than 1.300 people participated in the Athens meeting with no other constraint than a simple online registration, and the same rule will apply to the larger Rio meeting. All major sessions were webcast and real-time transcription posted on the Web, facilitating remote participation and providing a high level of transparency.

This paves the way for a notion of "stakeholdership" that could well represent for thematic multi-stakeholder governance what citizenship is for intergovernmental processes: the basic unit of belonging and the foundation for process legitimacy, the criteria through which individuals with a common interest or concern are allowed to participate in its governance. But there are major differences. Citizenship is geographical, usually exclusive (few dual nationalities) and received (via rules relating to affiliation or birth location) rather than chosen. By contrast, individuals can claim several stakeholderships, even on a single issue, according to the different interests or concerns they have in the subject, the multiple organizations they belong to, or the different angles they choose to adopt in examining it. Considering citizenship (holding the nationality of a given country) as one particular type of stakeholdership even allows this broader notion to fully include the representative nature of governments while taking into account the complex social networks that Internet users are involved in.

3 – CATALYZING MULTI-STAKEHOLDER NETWORKS

A given issue is often addressed simultaneously by multiple frameworks with different memberships. The IGF is a neutral space bringing those different structures together annually to present their activities. Workshop "convenors" help key actors connect on an issue-by-issue basis, and encourage them to list relevant existing regimes (or lack thereof). For instance, Athens allowed groups and organisations separately dealing with spam to come together and exchange fruitfully.

Open consultations for agenda-setting as well as the event itself also help to gauge the "ripeness" of an issue, i.e.: the willingness of the various categories of actors to engage in discussions. The inclusion of Critical Internet Resources as a fifth main theme in the Rio Agenda is a case in point. Likewise, prominent business actors have taken public positions in favour of privacy standards in 2007, giving this idea increased momentum and visibility.

In this context, one of the main outcomes of Athens was the emergence of informal thematic networks, known as "Dynamic Coalitions". Set up by actors interested in a common issue (for instance Privacy, Freedom of Expression or Open Standards), Dynamic Coalitions have the ambition to help structure the work that occurs between sessions. Their members often participate in many meetings, acting as "connectors", ideally enabling the whole group to have a more complete vision of the thematic landscape. Rio will offer them time slots to report on their activities and the meetings their members participated in. Some may prepare background issue papers.

Some Dynamic Coalitions will develop and some not. Some will play an advocacy role and others more a facilitation role, organizing intersessional thematic forums, or workshops at the IGF. Some will have a more balanced multi-stakeholder composition than others. But, once again, the IGF has decided to rely on the spontaneous self-organization of participants. From the onset, it avoided establishing the complex rules for the creation of working groups that are customary in traditional international structures.

4 – DECISION-SHAPING VERSUS DECISION-MAKING

What is the function of the IGF? Can it take decisions?

A major challenge in Internet governance is making the complex mix of conflicting regimes more mutually compatible, while respecting the competences of the various public authorities. This involves two complementary approaches:

- establishing a better coordination among existing governance frameworks;
- collaboratively creating new and globally applicable new regimes for specific issues.

The IGF is not a negotiating space but a dialogue space. The Tunis agenda explicitly specifies that it is not a decision-making body. Some actors see this as a weakness. But it is a major asset in the early stages of its existence: it prevents participants, particularly governmental delegations, from falling into a natural but time-consuming pattern of drafting communiqués or resolutions. With the entire event devoted to informal interactions, participants are invited to listen to each other to grasp all dimensions of a problem, without relinquishing their own vision, like in the parable where five blind men each describe a portion of a whole elephant and collectively build a more complete picture than each could on his own.

This enhanced communication is a necessary preliminary stage for any progress. Because it is not a decision-making body, the IGF is a non-threatening neutral space for various institutions jealous of their prerogatives, as well as for governments. In full conformity with its mandate, the IGF becomes a space for "decision-shaping" rather than decision-making, through regular multi-stakeholder interactions. It respects the responsibilities of existing structures, increases their interactions and helps stakeholders identify common objectives.

More generally, the IGF is an annual "watering hole" for the community of actors involved in Internet governance. Many other activities are progressively articulating with it. Thematic preparatory conferences are taking place, and will be reported on (such as the one on Ethics and Human Rights in the Information Society held in September 2007 by UNESCO and the Council of Europe in Strasbourg). Some events may have titles that make them look like an integral part of the IGF process (such as the Forum Dialogue on Internet Rights organized in Rome by the Italian government). National and regional declinations of the Forum are envisaged. Finally, the perspective of the annual IGF often forces actors to report on their activities and prepare their positions through internal consultations. All in all, the simple existence of this annual rendezvous already has a coordinative effect on a broad range of independent activities, which contributes to the shaping of debates.

C – A NARROW PATH FORWARD FOR A FRAGILE EXPERIMENT

How far will the Forum go? How should it move forward? And what are the challenges?

Notwithstanding its promising beginnings, the IGF remains a very young and fragile exercise. Two opposite dangers threaten its future evolution. Too much informality and an incorrect handling of sensitive issues could transform it into a mere talkshop dominated by angry and/or sterile debates. This would prevent any real progress on issues and would progressively discourage earnest actors, including governments, making it an empty shell. On the other hand, premature introduction of formal procedures could stifle the positive and emergent dynamics, frustrate nongovernmental stakeholders and bring back the pitfalls of rigid intergovernmental processes. All participants – including the new ones – must be fully aware of these dangers. They have a common responsibility but also a vested interest in developing the full potential of this critical but still very fragile experiment that must remain faithful to the spirit and principles that presided over its birth.

Like a sailboat slowly cruising out of a narrow harbour towards the high sea, the IGF must structure itself progressively and carefully, in a dynamic tension between flexibility and formalism. IGF working methods should continue to emerge on an ad hoc basis. Some key challenges outlined below will determine in the near future whether the IGF falls into one of the two traps described above or continues along its present critical success path.

Leadership. The special advisor to the UN Secretary-General for Internet Governance, Nitin Desai, as Chair of the Advisory Group, played a decisive role in placing the IGF on the right trajectory in its early days. After he leaves his position, modalities for the designation of his successor(s) will be important. While a nomination by the UN Secretary General provides global legitimacy, real support (and perhaps ultimately identification) of candidates by the Forum participants themselves is necessary. Critical competence criteria will be: knowledge of the process history, trust from all categories of stakeholders and a recognized capacity to foster consensus. A co-chairmanship by the host country has clear benefits for logistics. But it will raise concerns if it seems to alter the general multi-stakeholder balance in favour of governments, and gives the host government in particular too prominent a role.

Process steering. The multi-stakeholder nature of the Advisory Group is a notable achievement, now firmly established. Still, the necessary discussion on its future composition, designation modalities and mandate could prove divisive. In a spirit of careful and progressive structuring, modalities for the 2008 IGF in India should be conceived as a step in an ongoing evolution, rather than as a final result applicable to all future meetings. Furthermore, how this discussion will be conducted is as important as its outcome: this will be a test of the real commitment of all actors to the principle of multi-stakeholderism.

Secretariat. The leanness of the IGF Secretariat, under the responsibility of its executive coordinator, Markus Kummer, allowed for bootstrapping without delay and forced it to be exceptionally efficient and thrifty. It will nonetheless be necessary to secure appropriate funding to guarantee its viability, neutrality and independence.

Contentious issues. Credibility of the IGF (and the multi-stakeholder approach it pioneers) will depend in large part upon its capacity to induce progress and better understanding on contentious issues. In that respect, Critical Internet Resources is a major test case. It can only bolster recognition of the IGF if it allows a better understanding by all actors of the present system and current issues (new gTLDs, IPV4 depletion, IDNs, etc…) while also reducing tensions regarding possible evolutions at the end of ICANN's Joint Project Agreement.

Dynamic Coalitions. These thematic groupings emerged informally. Most of them have spontaneously produced documents describing their coordinators, their participants (ideally multi-stakeholder), their purpose (advocacy and/or facilitation) and their expected outcomes. This forms the skeleton of an emerging common Charter template, to facilitate attribution of the label "IGF Dynamic Coalition". Clearer working methods are nonetheless needed to progressively transform Dynamic Coalitions into true multi-stakeholder governance networks.

Outcomes. If only to ensure efficient use of the limited time, IGF annual meetings should not be burdened with the negotiation of formal outcome documents. Publishing workshop and main session reports established along simple common templates is a pragmatic way for the IGF to "publish its proceedings", as requested by paragraph 72 l) of its mandate. In fact, the emergent multi-stakeholder working methods of the IGF are the main outcome of the Forum.

Progress reports. Provided it avoids excessive informality and sclerosis, the IGF will become attractive for organizations and various actors willing to report on activities in other contexts. In particular if, in the future, stakeholders undertake the development of various regimes during the time between sessions, the IGF will be a natural space for them to present progress reports and to gauge the level of consensus they generate at various elaboration stages.

CONCLUSION

As the number of Internet users grows, so does the need for common rules and regulations. At the same time, the heterogeneity of the value systems and legal frameworks involved increases. Hence, paradoxically, the more common rules are needed, the more difficult it is to elaborate them, and even to reach agreement on priorities.

The IGF is not the space where all issues will be solved. But it is a test bed for a new multi-stakeholder governance approach indispensable for complex global issues, whose multi-dimensional nature strongly calls for an early and worldwide involvement of all the different actors concerned. Building upon existing governance frameworks (including national governments), multi-stakeholder governance organizes their interoperability.

The Internet and the World Wide Web have emerged in a bottom-up manner: the TCP/IP protocols allows hundreds of thousands of heterogeneous networks to interoperate to create a global Internet; the HTML / HTTP protocols unify heterogeneous information systems to produce the seamless World Wide Web. Likewise, the IGF can be seen as the laboratory to define simple interaction protocols among governments, the private sector and civil society actors, the simplest of which is its open consultation format. Endorsement of those multi-stakeholder interaction protocols could allow heterogeneous governance frameworks to interoperate and create, from the bottom-up, a seamless Global Framework for Internet Governance.

If the IGF demonstrates that the multi-stakeholder approach is simpler, produces better consensus and shapes more efficient and enforceable regimes, actors in all domains, including various intergovernmental or international organizations, will progressively adopt it for their Policy Development Processes and their interactions with other governance structures. This will gradually transform, one regime at a time, the international system and Global Governance as deeply and peacefully as the Internet and the Web have transformed our societies.

This exercise is just a beginning. Its future is not yet written and the IGF will certainly be confronted with major challenges. But it offers a glimmer of hope in the debate on global governance, and points towards a potential paradigm shift in the way the international community will confront global issues It is now the common responsibility and interest of all participants in the IGF to ensure the success of this fragile experiment and to guide it carefully along its narrow and critical path.

Encouraging Implementation of the WSIS Principles on Internet Governance Procedures

William J. Drake,
Graduate Institute for International Studies, Geneva

At the first World Summit on the Information Society (WSIS) held in Geneva in December 2003, governments adopted a Declaration of Principles that was said to reflect a global consensus on a range of global policy issues. During the extended preparatory negotiations, among the most hotly contested of these issues was Internet governance, which was dealt with in paragraphs 48-50 of the declaration. Paragraph 48 establishes guiding principles on the conduct of governance processes, namely that, they "should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations." The latter point is amplified by Paragraph 49's statement that Internet governance, "should involve all stakeholders and relevant intergovernmental and international organizations." Going further, Paragraph 50 holds that Internet governance issues "should be addressed in a coordinated manner." While this point is raised as a preface to the call for the UN Secretary-General to convene a Working Group on Internet Governance (WGIG) to study the issues, the need for coordination was invoked often enough in the course of the WSIS process to suggest that it stands as a generalizable principle as well. Taken together, these prescriptions constitute what could be called the procedural component of what came to be known as the "WSIS Principles on Internet governance." In addition, Paragraphs 48-50 set out a substantive component, i.e. that Internet governance "should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism."

This brief chapter is concerned with the former, procedural component of the WSIS Principles. Concerns about the conduct of Internet governance processes occupied governments from early in the WSIS process. The Latin American Caribbean Regional Conference held in Bávaro in January 2003 adopted a declaration calling, inter alia, for, "multilateral, transparent and democratic Internet governance" that would "take into account" the needs of governments, industry, and civil society. This language was incorporated into the declarations of subsequent regional meetings, repeated during the Preparatory Committee negotiations, and improved along the way (by replacing "take into account" with the "full involvement" of all stakeholders). After the above formulation was adopted in Geneva, it was routinely reiterated in the documents and work of the Preparatory Committee meetings of the second, Tunis phase of WSIS. Finally, the Tunis Agenda for the Information Society agreed at the November 2005 summit reaffirmed the centrality of the "WSIS principles" in the first paragraph of the Internet governance section, and mandated the new Internet Governance Forum (IGF) to, "Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet Governance processes."

The fact that the procedural principles were routinely reiterated for three years and then positioned as a guide to follow-on activity would seem to suggest that governments believed they were important and should influence Internet governance in the years to follow. Nevertheless, there has been little real effort in the post-WSIS era to assert such influence. The Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU) have both referred to the WSIS principles in their respective internal reform discussions, but have not attempted to systematically assess and enhance their conformity with these prescriptions. Nor has the matter received serious attention in the wide array of other intergovernmental, private sector, and multi-stakeholder organizations and networks involved in the distributed architecture of Internet governance. And most strikingly of all, the IGF has yet to even discuss its specific mandate to promote and assess the principles' embodiment in Internet governance processes. Indeed, some key stakeholders have seemed to regard the principles, and the WSIS outcome documents more generally, as artifacts from a difficult past that should not receive any further public attention.

Given stakeholders' varying interests and perspectives on the merits of the WSIS agreements, the desire of some to not look back is understandable. Nevertheless, to so swiftly bury the results of a three-year UN summit process would be somewhat unusual, and is hardly the best way to foster international dialogue on critically important issues that require greater cooperation. It would also be unfair to the many diverse stakeholders that spent an enormous amount of time, money and effort laboring through the WSIS process in the belief that it mattered and would have some configurative influence going forward. But more to the point here, even if parts of the agreements raise difficult issues on which some parties would prefer not to re-engage, the procedural component of the WSIS principles should not be one of them. After all, if one sets aside memories of the WSIS' political dynamics and focuses just on the text itself, what the Geneva summit agreed on was the outlines of what in other contexts would be called principles of "good governance." In recent years, good governance has become a major concern both at the national level and within a variety of international institutions because it can enhance the functional effectiveness and political legitimacy of decision-making. If good governance is worth promoting in other national and international arenas, why should this not be true for Internet governance as well? The procedural component of the WSIS principles provides, for the first time, a baseline set of tools the international community could use to promote holistic collective learning about and improvements in Internet governance as it was broadly defined in the Tunis Agenda. Allowing these tools to drift off our collective radar would therefore constitute a significant missed opportunity. With this in mind, in the following I will briefly offer some suggestions on how the procedural component of the WSIS principles could be usefully refined, applied, and carried forward.

CLARIFYING THE PRINCIPLES

It can be stipulated at the outset that the WSIS Principles are not a model of clarity and textual perfection. Clearly, they suffer from shortcomings that are fairly common to negotiated texts on divisive topics, three of which are particularly noteworthy. First, the core terms are left undefined. The meanings of "multilateral," "transparent," and "coordinated" may seem intuitively straightforward, but consequential differences in interpretation remain possible. Devising conceptual and operational definitions that are both sufficient and consensual would present some challenges, but these should be tractable. In contrast, agreeing on the precise meaning of the "full involvement" of all stakeholders could engender greater controversy since the concept is somewhat unconventional and revisits all the unresolved WSIS-era battles concerning multi-stakeholderism. And "democratic" is unquestionably the most problematic of the principles, since the notion rests on conditions that do not apply at the global level, e.g. an identifiable public and a polity in which there is a strongly shared understanding of what makes decisions legitimate.

Second, depending on their interpretation, two of the terms may be contradictory with one another. "Multilateral" is generally construed as referring to intergovernmental cooperation among three or more states (although this overlooks the integral role of substantive ordering principles, like the diffuse reciprocity of such states). If multilateral is taken to mean cooperation only among states, at least with respect to final decision-making, then it would be incompatible with at least some understandings of the "full involvement" of all stakeholders. And third, the principles' scope of application to Internet governance processes is unclear. On the one hand, save for perhaps the most sensitive aspects of security, it seems reasonable to suggest that all Internet governance processes should be transparent, or should at least meet some baseline standards of transparency. But on the other hand, it would be nonsensical to suggest that all Internet governance should be multilateral, since much of it occurs in private sector and multi-stakeholder environments that states could not take over or manage effectively.

Conversely, other arenas of Internet governance involve public policymaking processes in which states do not and would not accept the truly "full" involvement of all stakeholders.[1]

All this suggests not that the principles are irretrievably unworkable, but rather that some clarifications are needed to make them workable. The core terms should be defined and operationalized in terms of baseline sets of illustrative measures or actions, and their interrelationships and scope of application should be clarified. Tackling these tasks would be facilitated by drawing on the relevant and substantial bodies of scholarly and policy literature, and on the dialogues and actual experiences within both Internet governance arenas and other realms of global governance like the Bretton Woods institutions. Absent such antecedent clarifications, any effort to promote and assess the WSIS principles' embodiment in Internet governance processes would be fraught with controversy and would probably fail.

The experience of the WGIG is instructive in this regard. During its second meeting in February 2005, the WGIG conducted a preliminary assessment of the WSIS principles' applicability to a few key governance environments, most notably ICANN and the ITU. The discussion usefully illustrated that these organizations varied in their degrees of conformity with each principle, and led to the consequential conclusion that any "oversight" of the governance of core resources could not be conducted within the ITU because, inter alia, it is not sufficiently multi-stakeholder. But the discussion also revealed that it was impossible to carry the exercise beyond such generalities absent

[1] In addition to these problems with the procedural component, other aspects of the WSIS Principles and related text also raise issues. For example, paragraphs 48-50 of the Geneva declaration include the problematic assertion that the Internet is a "global facility available to the public," which seems like a telephony-inspired way to conceptualize a vast agglomeration of public and private networks that employ a common set of technical protocols; attempt, through rather artificial differentiations, to specify the respective roles of the different stakeholders in Internet governance processes; and, in the substantive component, and call for, "an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism," without defining these terms or saying to which domains of Internet governance they are supposed to be applicable.

share definitions and understandings of the terms' interrelationships and scopes of application. These issues could not be resolved in the context of a single short meeting; clearly any effort to tackle them now would require more time, preparation, and dialogue.

It would be well beyond the scope of this brief chapter to attempt a first cut at clarifying the outstanding issues, each of which would require some elaboration. My view is that the essence of the procedural principles could be distilled down to three definable and operationalizable guidelines, namely that Internet governance should be characterized by transparency, inclusive participation, and coordination, to the extent practicable given the specific properties of the issues and institutions involved in a particular instance. "Inclusive participation" would capture both the multilateral and multi-stakeholder ideas, with the precise balance between state and non-state actors varying as merited by the case at hand. And given the inherent problems with the notion of "democratic" and the fact that other principles capture some of its elements, it arguably would be sensible to simply set aside this ill-chosen term. This seems like a sufficiently manageable starting point, although obviously any collaborative assessment might come to a different conclusion.

APPLYING THE PRINCIPLES

Once the terms and their interrelationships and scope of application have been specified, the procedural principles could be utilized to two important ends. First, they could be used to stimulate the gathering, aggregation, and presentation of information on how the various organizations and collaborative networks involved in Internet governance address common operational challenges, e.g. promoting transparency, inclusive participation, and coordination. The side-by-side arrayal of information on the approaches taken to these matters in different institutional settings would allow us to draw comparisons and contrasts, detect patterns and variations across cases, and identify general lessons learned and good practices. Making such information available in a readily digestible format is a pressing challenge because the architecture of Internet governance is highly distributed, with a wide array of governmental, private sector, and multi-stakeholder organizations and collaborations playing diverse roles on a wide variety of issues. This makes it very difficult to get a sense of the whole, which in turn reinforces the tendency to focus attention on a few bodies, most notably ICANN, at the expense of other arenas requiring greater awareness and engagement. Horizontally organized information on what is happening across the governance landscape and its component parts would help to promote a holistic understanding of Internet governance and to facilitate collective learning within and across governance mechanisms.

Second, the procedural principles could be used to encourage Internet governance mechanisms to assess their practices and undertake reforms as merited. Such encouragement could come from both internal and external sources and take a number of forms. For example, if the participants in a given governance mechanism could readily see how peer mechanisms address the same challenges they face, they might be moved, of their own accord, to ratchet up their levels of conformity with good governance standards. Preferably they would do this due to a real conviction that reforms would improve their functional effectiveness and political legitimacy, but even a more grudging response based on beauty contest considerations might be a useful first step upon which to build. Conversely, external actors – academics and research institutions, civil society organizations, the technical and administrative community, industry associations, and so on – could individually or collaboratively produce analyses that outline current practices and patterns and point to operational measures worth considering.

Of course, it is possible that the parties to some governance mechanisms would not initially welcome outside scrutiny and suggestions. Indeed, the prospect of eliciting turf-oriented reactions has already given rise to concerns in some quarters that it would be too sensitive to try implementing the IGF's mandate to, "promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet Governance processes;" to, "interface with appropriate intergovernmental organizations and other institutions on matters under their purview;" or to, “facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall within the scope of any existing body.” But on the other hand, one might note that the international community did, after all, agree that the IGF should do these things; that governance mechanisms do have public interest obligations that are not best advanced by operating like moat-protected castles; that vibrant, learning organizations can and do benefit from external viewpoints; and that the need for external reviews might be obviated by proactively undertaking their own internal reviews and inviting public inputs.

THE ROLE OF THE IGF

The early arguments for what became the IGF tended to concentrate on the need for a global, multi-stakeholder space for dialogue and analysis without delving much into speculation about its precise institutional form. Nevertheless, if one goes back and looks at some of the early statements from its academic and civil society proponents in particular, they suggested functions that would require a lean but sufficiently resourced secretariat with the institutional capacity to undertake or at least coordinate analytical work, as merited. For example, the civil society declaration to the Geneva summit called for the establishment of a multi-stakeholder observatory committee that would track and map the most pressing developments in governance decision-making, and assess and solicit stakeholder input on their conformity with the stated objectives of the WSIS agenda. Similarly, the Internet Governance Caucus and some of its individual members variously argued for an IGF that would be able to undertake, inter alia, the systematic monitoring of trends; the comparative, cross-sectoral analysis of governance mechanisms, with an eye toward lessons learned and best practices that could inform individual and collective institutional improvements; and the assessment of horizontal issues applicable to all arrangements, e.g. the promotion of transparency and inclusive participation. Some of this thinking was carried forward into the WGIG Report and ultimately into the Tunis Agenda’s mandate.

Things have evolved a bit differently since then, and it is difficult to imagine how a series of broadly-framed annual conferences alone could fully realize the mandate's objectives with respect to the WSIS principles. However, the IGF could still provide a facilitated environment within which interested parties could assess and encourage their implementation. Three options suggest themselves.

First, a multi-stakeholder dynamic coalition could be established to coordinate the ongoing monitoring and analysis of the procedural principles' implementation within Internet governance mechanisms. Dynamic coalitions being informal creatures without any authority, there would be no reason for the organizations involved to be particularly alarmed by the prospect of one of them assembling information, highlighting good practices, and so on with regard to repeatedly agreed objectives like transparency and inclusion. Participation in such a coalition would of course be open and voluntary, and representatives of the governance mechanisms themselves could join in the effort if they were interested. Moreover, synergies could be exploited between the coalition's work and any internal evaluations and initiatives these organizations and collaborations might wish to undertake.

Second, and in parallel, the governance mechanisms could use the opportunity of the annual IGF meetings to report on their embodiment of the procedural principles. The IGF's Advisory Group has created a space in the program that would be well suited to this purpose. At the 2007 meeting in Rio de Janeiro, all major organizations dealing with Internet governance issues will be given a slot, at their request, to hold an Open Forum at which they can present and discuss their activities. In future years, a portion of these forums could be set aside, on a voluntary basis, to address how they address questions like transparency, inclusion, and coordination. They could do this either alone or in conjunction with the dynamic coalition, as they prefer.

Third, at future meetings, a single two-hour session in the main hall could be set aside for discussion of the issues. If the existing topography of sessions on openness, security, access, diversity, and critical Internet resources is maintained and space in the program is thereby limited, such sessions could be held in an off-peak period, i.e. the early morning, lunch time, or after 6pm. In this setting, the dynamic coalition could provide some highlights from its work program and prior meeting; interested Internet governance bodies could offer their own views; and the issues could be vetted in an interactive manner with a larger audience. To help identify good practices and potential problem areas, relevant experiences of international institutions involved in other global issue-areas could be brought into the discussion as well.

CONCLUSION

Transparency, inclusive participation, and coordination, to the extent practicable, ought to be regarded as comparatively anodyne principles on which the international community can readily agree. In fact, it already has. All that is needed now is to put in place a process to assess and promote their implementation. Such a process could be entirely positive in tone and concentrate on highlighting the good practices adopted by relevant bodies, leaving it up to others whether they wish to follow suit or find other, more locally optimal paths to the same ends. The IGF, with its specific mandate to address cross-cutting issues, would be the most appropriate context in which to take up this challenge.

The Internet Identity Crisis

Louis Pouzin,
Eurolinc, France

With the worldwide penetration of the Internet, and the greedy chase for cost cutting, we are dealing with ever more automated services lamely aping human with sets of predefined menus. Browser-based forms require typing lots of items in specific formats, and often do not even let the user keep a copy of what was really transmitted. For a person traveling in a country using a different language and keyboard, the service interface becomes definitely dissuasive.

WHEN DID I LOSE MY IDENTITY?

Information commonly collected includes name, address, phone numbers, account details, password, etc. Repeating them every time one connects to a service is a hassle. Typical browsers offer an option for automatic form filling. However, this may result in providing superfluous information to the service provider. Whatever method is used to enter one's data, they end up in thousands of archives out of the user's reach. No one knows which companies store their data. We have lost control of our identities.

WHAT IS KNOWN ABOUT ME?

Collecting personal data is a favourite sport in marketing. Data are exchanged, sold, matched and analyzed, to yield clues on personal tastes, habits, revenues, relations, and perhaps, political, religious, sexual, racial information. Data mining tools are thriving. This opens up major potential for tracking individuals, for whatever purpose. Profit-driven companies know no limits when trying to expand their revenues, unless constrained by the law, or strong societal rejection.

HELP! ANYBODY LISTENING?

Not only we do not know which companies keep track of our identities, but we have no idea of the level of security and confidentiality practiced by these companies. It may be very weak. We also quite often read in the press that thousands of user files have been stolen from the database of some supposedly reputable organization. Then, the next threat is someone pretending to be you, by using your name, password, credit card number, etc. Or a hacker has succeeded in breaking into a database and changed some data, such as name and password, so you can no longer access your own bank account. Or there was an error in updating the files, or some other gremlin. With human systems such contingencies may be corrected by talking to someone, at the cost of some wasted time. When the only interlocutors are computer boxes, there is just no way out. Or is there?

CENTRAL SYSTEMS

Common sense says don’t put all your eggs in one basket. Still, this is what some organizations are trying to sell: a central system hosting personal identities. Once a person has been authenticated by the system, it would feed other service providers with the requested data. That is, single sign on (SSO).

Central systems also mean single authentication providers. As we should expect competition, we would have to subscribe to several central systems, with little or no capacity for interoperability. In addition, companies offering this service would very likely be based in countries where there is no legal protection of personal data, and unlimited monitoring by the government.

HOW MANY YOU'S ARE YOU?

In real life, individuals use multiple identities depending on the context in which they are needed. e.g. family, employer, bank, hospital, tennis club, library, etc. Each identity may include distinct set of items, and they may need different levels of security. This is quite antagonistic to any centralized scheme, because individuals as well as the organizations in which they are identified want to maintain autonomous management and security policies. So, is SSO possible?

Dealing with multiple autonomous service providers and enjoying SSO is indeed possible. What is required first of all is a number of “certification authorities”, agreed by the states and all stakeholders, in charge of issuing “certificates” proving that the holder is the right person. Second, there is an agreement between a large enough variety of providers offering the most frequently used services. Agreement means mutual trust between partners whereby they accept to service their own users once they have been authenticated by another provider. Technically this requires common secure protocols to exchange identity data among partners. If such protocols reached a stage of international standard, there would be no technical limitation to the number of associated providers. It seems, however, that lack of trust is a limiting factor.

This partnership scheme among autonomous providers brings about a significant plus in service. An identity is often perceived as simply a key opening access to a service. In a multiple provider context an identity may drive a distributed process, or transaction, running on several systems. For example, a visit to a doctor could lead to tests at a hospital, buying medicine, and missing a few workdays. A single process attached to an identity could work through every organization involved, including employer, bank and social security.

HEY, I CAN MANAGE ME!

While the previous scheme shows some attractive capabilities, it is still constraining for users. Their identities are managed by external organizations, and they may not control precisely what is disclosed to whom. A further refinement is to give users total control of their own identities.

Being user-centric, this scheme has to be all the more flexible, hence with lots of personal variations. Roughly speaking, a user makes a list of items he may have to provide when using services over the Net. Some may have to be certified, but probably not all. Then he can spread these items to any number of identity servers he trusts, including his own. When connecting to a provider he will receive requests for identity items. In manual mode, the user can respond with URL's leading to each requested item. In automated mode, he can connect with the URL of an identity server, which will run a dialog driven by a user-defined script.

This allows detailed control of which identity item is released where, so bogus information can be given when the service provider is asking for irrelevant items, as is often the case with commercial sites. Furthermore, identities can be modified and relocated as often as is desired, making life more difficult for predators.

As for any user-defined automation, this scheme can be customized for handling multiple couplings of identities and service providers. However, it requires careful analysis of every condition, and may not be the best tool for less sophisticated users. Some assistance and predefined settings would be helpful. Nonetheless, this may be the most effective counterweight to attempts by hyperpowers to hem the world into a 1984 nightmare scenario.

So, to fight Big Brother: have many identities, divulge minimum info, install errors whenever possible, change identity servers frequently, and…pay in cash.

The Next Internet Governance Battles

Kenneth Neil Cukier,
The Economist, Tokyo

INTRODUCTION: TOMORROW'S NETWORK WILL BE DIFFERENT FROM TODAY'S

The current debate over Internet governance risks becoming obsolete because the technology, architecture and use of the network are undergoing radical change. Yet policymakers are largely unaware of these changes. As a result, they are "fighting the last war," so to speak. Rather than looking at the new challenges of naming and numbering in the next decade and beyond, they presume that the Internet that existed in 1998 when ICANN was created, and which operates today, will be the one that exists tomorrow.

But this is just not so. And trying to devise policies based on this would be like establishing rules for the telegraph just as the age of the telephone begins. Three forces are transforming the way the Internet works: ubiquitous networking, new technical architectures and the developing world's telecoms growth. This essay provides an overview of the changes taking place and considers their impact on the management of critical Internet resources (while noting shortcomings with existing approaches). The first force is technology: the Internet is going from a network comprised of PCs with people typing behind them, to one in which all manner of devices – from cars to washing machines to sensors on buildings, bridges, trees and in people – communicate over a network. It may sound like science fiction but initial versions already exist and the technology will be commonplace in about ten years' time. This "ubiquitous networking" will place new demands on naming and numbering policy. It may even be the case that the most efficient approach is to bypass the current domain name system altogether.

The second change is in the architecture of the network: Internet engineers are redesigning the underlying protocols of the Internet so that they can better mature for more robust uses. In so doing, the engineers are calling into question certain tenets of the network dating back 35 years, which are enshrined in the way that Internet names and numbers are managed. Although it is too early to say how the new network might look, it is clear that the network will be different. Indeed, the very "uniformity" of the Internet's architecture may be among the first Shibboleths to go.

The third change regards international development: the most impressive network growth has been in developing countries, not the West, and via the mobile phone, not the PC. New devices are being designed especially for this market. New applications and uses are also emerging. So far, the Internet has been created and used by "the first one billion" users -- and its infrastructure coordination naturally reflects this. Yet when the second and third billion users from developing countries join the information society, as they are starting to do, it calls into question certain naming and numbering policies. As a result, issues germane to the developing world will need to be better taken into account.

The result of these changes is that as governments discuss Internet governance and the management of critical Internet resources, they do so in a time capsule. Ultimately, by trying to assert more control, governments may find they have planted their flagpoles into a sandbar, as the network is in the process of a dramatic transformation for which the Internet governance community is unprepared.

THE ERA OF UBIQUITOUS NETWORKING

The Internet today has slightly more than one billion users, and mobile phones subscribers number around 2.7 billion. But this is nothing when compared to the amount of things that can be attached to a network, to send information about their status, location and operation, as well as to link with other devices to do new things. Over the next ten years, the Internet will be characterized by all manner of machines, structures, environments and people’s bodies connected to a network at all times, rather than just humans interacting with a personal computer or mobile phone. The network will need to accommodate a trillion devices, engineers estimate.

The groundwork for this has already been laid. For instance, around ten billion microprocessors will be sold this year, embedded in everything from computers and coffee-makers to cars. Today, most of them “think” but do not “talk” – that is, they perform certain tasks but do not communicate. This is changing. As the cost, size and power requirements of chips decline, and their performance increases, communications functions are being integrated into processors, mainly with wireless technology. Moreover, the wireless industry is investing billions of dollars to deploy 3G and nascent 4G (WiMax) high-speed mobile networks.

The technologies that already exist are staggering. For instance, a wireless chip for mobile phones that in 2003 cost $50 today costs $5. Chips used for the Global Positioning System or Bluetooth wireless links now cost as little as $1 and are the size of a matchhead. Chips for Zigbee technology, used for short-range sensors, which currently cost around $4 and are the size of a fingernail, are expected to shrink down to a quarter of the price and size in five years. A far simpler kind of chip called a radio-frequency identification (RFID) tag, which sends a tiny bit of data over a short range when activated, can already be manufactured for 4 cents apiece. Hitachi has a prototype chip that fits into the groove of a thumb-print. In 2006 one billion RFID chips were sold and the figure is expected to nearly double in 2007.

These technologies enable all sorts of things to connect to a network. For example, industrial building firms are preparing to commercialize products that add a small wireless node to every light fixture. This would enable them to be turned on and off remotely, as well as serve other functions, such as networked smoke detectors and security alarms. Cars are going beyond satellite navigational systems to include wireless modules that aid in alerting emergency services in case of an accident, electronic toll charges and traffic monitoring. Consumer electronics manufacturers are embedding networking modules as a way to sell content services. Appliance manufacturers are looking at adding communications to their products to better regulate power consumption, upgrade software and provide "preventive maintenance."

Meanwhile, bridges and buildings are getting sensors to continually monitor their structural health – an important issue in light of a devastating bridge collapse in the US in the summer of 2007. The environment is also being monitored by sensors for climate change, as well as for more efficient farming. Amazingly, new networking technologies are starting to be introduced inside people's bodies for medical purposes, such as to explore the intestinal tract or monitor the blood fluid inside of a person's heart to detect and prevent congestive heart failure. It bears noting that these technologies are not scribbles on paper in R&D labs, but products undergoing regulatory approval and already being sold by major companies like General Electric, Philips, Honeywell and others.

This will change the Internet governance debate in profound ways. The Internet addressing system was designed for individuals to locate content. This is already changing, as "Web 2.0" data flows mean the network must integrate many discrete operations from numerous servers into a single, interoperable service. Yet tomorrow, the demands of the infrastructure will multiply exponentially, as ever more devices link together. So, things as basic as ensuring identity and security – tricky even on today's far simpler Internet – will be much harder.

The current approach to Internet coordination is not perfectly suited to this environment. To give just one example, ICANN's rules covering domain name registries assume that names are used to identify websites, as they mainly did in 1998 when ICANN was created and the Web was less than a decade old. The idea that a name might refer to site that is simply a continuously changing instantiation of information or a temporary service that comes together and disbands on the fly is not envisaged. Web site names might be automatically generated and only "alive" for a day, or even a few seconds. Who is to say? Yet ICANN's policy of taking part of registration fees to support its operations throws a wrench into these potential uses. This example is not imaginary. In the March 2003 ICANN meeting in Rome, a representative of SITA, the airline consortium that operates .aero, explained that the group wanted to create a specific domain name for every commercial flight every day, so that the aviation industry as well as consumers could obtain information about it, from ground maintenance to flight delays. But SITA could not deploy it due to ICANN's fee structure. Add to this a world in which every plane engine has 20 different sensors all generating data in real-time, and the extent of the problem only grows. The point of this example is not to address this problem per se, but to underscore how policies can unwittingly stifle innovation.

With the need to provide identifiers to every networked object, there will probably be an engineering incentive to bypass the Internet's domain name system altogether. If this happened, it would mark an ironic twist. Just as governments started to get their heads around what Internet governance means by way of venues like the World Summit on the Information Society and the Internet Governance Forum, the very nature of what they debated changed shape, rendering their huffing and puffing rather moot.

RE-ENGINEERING THE NETWORK'S DESIGN

The Internet is not a series of tubes. It evolved like sedimentary rock, with newer technologies layered upon older ones. This has so far worked, but it does not scale well. To meet the future demands of a trillion connected devices, efforts are underway among Internet engineers to redesign the Internet. It is a way to pull out superfluous things, as well as incorporate features that were not originally a priority but are today regarded as important, such as better identity to minimize spam and hacking.

Two initiatives are taking place under the US National Science Foundation. One is the Global Environment for Network Investigations (GENI), to build an advanced test-bed network for piloting new protocols and applications. The second is Future Internet Design (FIND), which considers specific ways the Internet can be changed to address future needs. A number of research proposals have come forward that would change the way the Internet works, and with it, aspects of Internet governance.

One technique is “Internet indirection infrastructure.” This would overlay an addressing system on top of current Internet Protocol addresses, which would better enable mobility and multicast applications by bypassing the current point-to-point approach in circumstances when routing traffic that way is inefficient. A second idea is called “active networks” or “metanets.” It would permit diversity at the core of the network, not just at the edge, by replacing routers with devices that can dynamically load new protocols. Applications would be able to reprogram the devices through the network for a specific protocol, optimized for the communications. The device would partition itself internally to support multiple, mini private networks.

These sorts of changes, however, might require that IP address assignments be done differently -- or change the nature of IP addresses themselves. Would the institutions that exist based on the current DNS system be comfortable ceasing operations due to changes in technology? Or, would their first inclination be to resist the technical changes under the banner of upholding the Internet’s “stability”?

THE DEVELOPING WORLD JOINS THE NETWORK

In 1995, when the US government first hosted discussions that would eventually lead to the creation of ICANN, around 94 percent of Internet hosts were located in the 31 industrialized countries that comprised the OECD. Today, the figure is closer to 50 percent. China has the most broadband subscribers in the world with over 100 million users, and the Chinese language has surpassed English as the dominant language on the Web. China also has the most mobile phone subscribers, with more than 500 million users. India is coming up fast behind; and with China, its companies are the biggest owners of sub-sea fiber optical Internet cables.

Meanwhile, the Gulf states are pouring some of their enormous oil wealth into major IT initiatives, allocating mobile phone licenses and even buying mobile networks around the world.

Africa has the highest new mobile-phone subscription rates in the world; in many countries the number of new users more than doubles annually. Around the world, 1.6 million new mobile phone subscribers are added every day. More broadly: in 2006, for the first time, more than half of the world's gross domestic product came from developing countries.

The striking thing about these trends is that the developing world is joining the information society using a different model than the West. Instead of one person-one PC, as in industrialized countries, computers are more commonly shared among many users and the mobile phone is the device by which most people participate on the network. Today, it is mainly for phone calls – the networks and devices do not support much Internet access and illiteracy is a major issue. But the variety and richness of mobile services are increasing rapidly, tailored to local needs. In time, the phones will basically be primitive Internet devices.

Moreover, they may operate in ways that are different than today's Internet. For instance, in the "One Laptop Per Child" project, the networking modules for the $100 laptops are being designed to enable peer communications rather than merely linking onto the Internet backbone. This means that more network traffic may be off the public Internet and privately routed. New addressing systems might be created to make this smoother. Furthermore, mobile phone numbers rather than ICANN's domain name system may be the prominent identifiers used. This would give developing nations more control of information than they enjoy via ICANN - as China learned when it was able to censor mobile phone SMS messages during the SARS outbreak in 2002.

The online rise of the developing world affects how the Internet's infrastructure is managed. For instance, setting a wholesale rate of a few dollars for a domain name is prohibitively expensive in many countries – an issue to which ICANN is sensitive. It also focuses a spotlight on Internet governance in a world in which the 5 billion people who live in poor countries need to share the network resources with the 1 billion that are already connected. (Chinese officials used to grumble in the late 1990s that there were more IP addresses at some US universities than in all of China.) How IP addresses are allocated and root servers are maintained and deployed may be open to scrutiny. Most importantly, it poses embarrassing questions to ICANN about why it is taking so long to introduce "internationalized" domain names, so people can use local scripts to send emails and navigate the Web.

CONCLUSION: THE HERACLITIAN INTERNET

Taken together, the forces of ubiquitous networking, new Internet architecture and the developing world's network growth, render today's Internet governance discussions somewhat passé. The magnitude of these changes is on a similar scale to the revolution of the Internet itself relative to the telephone system, a change that is still being digested by the telecoms industry, policymakers and society.

The Internet is only 35 years old, and as a mainstream medium, not much older than a decade. Yet already there has been much iteration. In 1969 the national backbone ran at 56 kilobytes per second; by 1997 that speed was possible on a home modem; in 2007 users in Japan, Korea and Hong Kong enjoy 100-megabyte access. When the Internet was first designed, it linked 13 supercomputer centers at American universities and supported several hundred users, each of whom had to be approved to go online. Commercial traffic was forbidden. The domain name system was not created until 15 years later, in 1985, and today seems an archaic technology.

This history bears remembering, since it highlights the degree to which the network we have today is not set in stone but mutable, plastic, ever-changing. Likewise, its "governance," viewed in historical perspective, is a series of changing rules and rulers. First, officials from DARPA, the US military's research arm, called the shots – though they largely let the engineers from academia do what they considered best, a process referred to as "Internet self-governance" (later, the term "self" would get left out). Then the academic-funding agency NSF had control, but again deferred to the "Internet community." This grouping of researchers and network operators from academia and industry had around a dozen organizational structures over two decades, each with a new abbreviation: ICCP, NWG, IAB, IESG, IETF, IANA to name a few. But the end result was that a set of institutions and mechanisms were established to manage the network.

Yet they never lasted long. One notable feature of the history of Internet governance is that institutions do not adapt to the changes in the network; they become obsolete and are superceded by new ones. By 1998, because these self-governance processes were considered too informal and relied too much on the US government, the US privatized and internationalized it – by creating ICANN. The group, ironically, then spent most of its time fighting off criticism that it was too informal and too American.

If the past offers a lesson, it is that both the network and its governance are in a constant state of transformation, not something static that can have a set definition or rules applied. In the Internet's early stages, both protocols and policy were made on the fly by engineers addressing concerns as they emerged. But in trying to formalize this with ICANN, policy became "ex ante" (i.e. something that must be known in advance) rather than "emergent" (i.e. continually revised, based on changing circumstances).

The mismatch is that while ICANN (like any administrative institution) sets rigid polices, the technology remains emergent and ever-changing – witness the rise of ubiquitous networking, new Internet architecture and telecoms in the developing world. This tension is inherent to ICANN and a reason why it is by nature a conservative force. Ultimately, the Internet is like Heraclites' river. Just as we never step into the same stream, so too we never log onto the same network twice. Will tomorrow's Internet governance institutions prove as fluid? What are the consequences if they do not?

The establishment of the Internet Governance Forum (IGF) by the UN World Summit on the Information Society (WSIS) is seen as an innovative new approach to global policymaking. Designed as a multi-stakeholder discussion space, it offers a unique opportunity for bottom-up policy development by linking together governments, private sector, civil society, and the technical and academic community around existing and emerging public policy issues related to the Internet.

By discussing the five main subjects of the IGF – access, openness, diversity, security and critical Internet resources – all governmental and non-governmental players can enhance their understanding of their specific roles and responsibilities in the management and development of the Internet.

“Germany – Land of Ideas” wants to make a contribution to the debate during the 2nd Internet Governance Forum in Rio de Janeiro, November 2007, with the publication of this book. Authors from all parts of the world, representing the various stakeholder groups, present their views about key issues of Internet Governance.

Germany
Land of Ideas