Internet governance and the World Summit on the Information Society (WSIS)

Adam Peake

Prepared for the Association for Progressive Communications (APC)
June 2004
APC gratefully acknowledges the funding support of CIDA.

TABLE OF CONTENTS

AUTHOR

Adam Peake is Executive Research Fellow at the Center for Global Communications (GLOCOM), International University of Japan

Introduction

Internet governance is one of the most high profile issues to emerge from the WSIS process.

The common vision for the 'Information Society' developed during WSIS was of a "people-centred, inclusive and development-oriented Information Society", its creation would require new forms of partnerships and cooperation among governments and all other stakeholders.[1] Yet these essential, commonly agreed principles jarred with the view that Northern-led processes dominated the governance of the Internet, and that developing nations were largely absent from those processes. Such concerns were accentuated by the perception that critical Internet governance functions were controlled by the United States.

The "rules of the game" for the 'Information Society' are being made in many different global policymaking frameworks, and developing nations and civil society have not participated to the extent they must. The global discussion starting now about Internet governance is an opportunity to redress this situation, and in discussions since the Summit the need to ensure that developing nation stakeholders have the capacity and opportunity to contribute effectively and meaningfully to ICT policymaking has been recognised.

The purpose of this report is to describe our current understanding of the debate about Internet governance in WSIS, and to examine the main policy issues that are being considered in that discussion. The report will also suggest opportunities for developing nation stakeholders to contribute to the processes that are defining the Internet governance landscape.

Internet governance and the Geneva Summit

Discussion about Internet governance during the preparatory meetings (PrepComms) leading to the Geneva Summit was confused.

Activities associated with the Internet Corporation for Assigned Names and Numbers (ICANN) --the domain name system, particularly country code top-level domain (ccTLD) names, IP number addresses, the root server system, and multilingual or internationalised domain names-- were the focus of debate. But multiple views were expressed about what was and was not "Internet governance", and what public policy issues were involved. Some developing nations noted that they were unable to participate in many of the decision making processes about these policies, and felt unable to manage resources they believed they had a right to manage, particularly a sovereign right in the case of ccTLDs. The level of disagreement was exacerbated by the perception of US domination of the Internet and its governance.

Civil society's contributions on these issues during the PrepComms were presented by the Internet Governance Caucus and focused on three main themes[2]:

Policy advocacy: For general principles of inclusive participation, transparency, and democratic accountability in ICT policymaking. Particularly reforms to facilitate the full and effective participation of developing nations and other marginalised groups.

---

[1] WSIS Declaration of Principles, paragraph 1 and paragraph 17 http://www.itu.int/wsis/

[2] The Internet Governance Caucus maintains a website with information about its activities, mailing list, etc. Like all civil society working groups and caucuses participating in WSIS the caucus welcomes all civil society members. see http://www.net-gov.org/

About ICANN: Civil society participants generally took the position that while it was far from perfect, ICANN was also not fundamentally 'broken.' ICANN needed further reform not replacing.

Multi-stakeholder processes: As it became clear that the discussion among governments was most likely deadlocked, civil society proposed that after the Summit some form of multi-stakeholder process should be established to discuss the problems and look for solutions.

Civil society participants also lobbied government delegates, particularly to correct misconceptions about what different entities involved in Internet policy and administration did, and in some cases about how the Internet worked. However, views on Internet governance, its problems and solutions varied among civil society participants almost as much as they did among government delegates. Today, civil society does not have a unified position on Internet governance, the range of issues involved are too broad and civil society too diverse. The Internet Governance Caucus is working to ensure that civil society is represented in all ongoing activities in WSIS around Internet governance.

Understanding the government's debate

Governments took opposing positions quite early in the preparatory process and negotiations towards final language took place in closed sessions with few opportunities for observers to participate. Unable to reach agreement in Geneva, governments used the Summit documents to ask the UN Secretary General to set up a working group to develop a working definition of Internet governance, and to identify the public policy issues involved. The working group should be created in an open and inclusive process that ensures the full and active participation of all actors both from developing and developed nations. It will report to the second phase of WSIS in Tunis, November 2005[3].

The closed nature of the final negotiations meant that details of the discussions, the compromises and areas of continued disagreement were not publicly known until some months later when Mr. Markus Kummer, a member of the Swiss government's WSIS team who chaired the negotiations, gave his interpretation of the texts and different positions. Speaking at the International Telecommunications Union (ITU) "Internet Governance Expert Workshop" in Geneva February 2004, Kummer described how the discussion among governments revolved around two issues, and how opposing camps emerged in both.

Defining Internet governance: narrow or broad

First, during discussions about the scope of Internet governance and the issues involved, some delegates envisaged a "narrow" or restricted definition of governance "Of" the Internet, i.e. technical coordination issues such as those carried out by ICANN. Others took a broader or extensive view of governance "On" the Internet, relating to what the Internet carries. There was some agreement that this broad definition should include critical issues such as Internet pricing and interconnection, and also policies regarding spam and network and information security and trust. Some delegates wanted to extend the definition further to

[3] WSIS Declaration of Principles paragraph 50, Plan of Action, paragraph 13.b. provide the terms of reference of the working group, and the principles by which it would be formed and operate, http://www.itu.int/wsis/

include consideration of appropriate content, international rules for e-commerce, taxation and encryption.

There is a concern that Internet governance will be defined so broadly that it becomes meaningless, a 'catch-all' for all ICT policies, and the tasks of the working group consequently become so diverse that it will have great difficulty in reaching any useful conclusion

Responsibility: a new intergovernmental process or the status quo?

The second issue discussed was about responsibility for Internet governance. Many developing nations, particularly China, South Africa, Brazil and most Arab States expressed the view that Internet governance was a matter related to national sovereignty and that an intergovernmental process, preferably under the UN (with the ITU being specifically mentioned), was needed where governments could discuss policy issues of international scope.

Most developed nations, including the United States, European Union, Japan, Canada and Australia, supported the current system of private sector leadership. They were referring to the narrower definition of Internet governance, particularly to ICANN's responsibilities, but also to general understanding that the Internet had developed successfully through self-regulation and that this should be encouraged to continue. They took the view that the system works so there is no need to change it.

Two major meetings on Internet governance have been held since the Summit, the ITU workshop mentioned earlier, and a United Nations Information and Communication Technologies (UN ICT) Task Force "Global Forum on Internet Governance". These meetings and other public statements clarified many issues, particularly about the different positions and concerns of governments, but they also made clear that positions have not changed much in the months since Geneva[4].

Working Group on Internet Governance (WGIG)

The decision to try to resolve differences of opinion through a working group established under the auspices of the UN Secretary General reflected a compromise between those governments that felt the WSIS process was not open enough to enable the full and active participation of private sector and civil society, and others who wanted a process within the UN framework. The working group will be a parallel and independent process to the PrepComms held during the WSIS Tunis phase, but will most likely report to the final PrepComm before the Tunis Summit so governments have the opportunity to consider the text. The working group will be formed at the beginning of June, with its membership finalised by October 2004. The working group will have less than one year in which to complete its work.

[4] ITU Workshop on Internet governance, February 26-27, Geneva.
http://www.itu.int/osg/spu/forum/intgov04/index.html
and UN ICT Task Force, Global Forum on Internet Governance 25-26 March, New York
http://www.unicttaskforce.org/sixthmeeting/

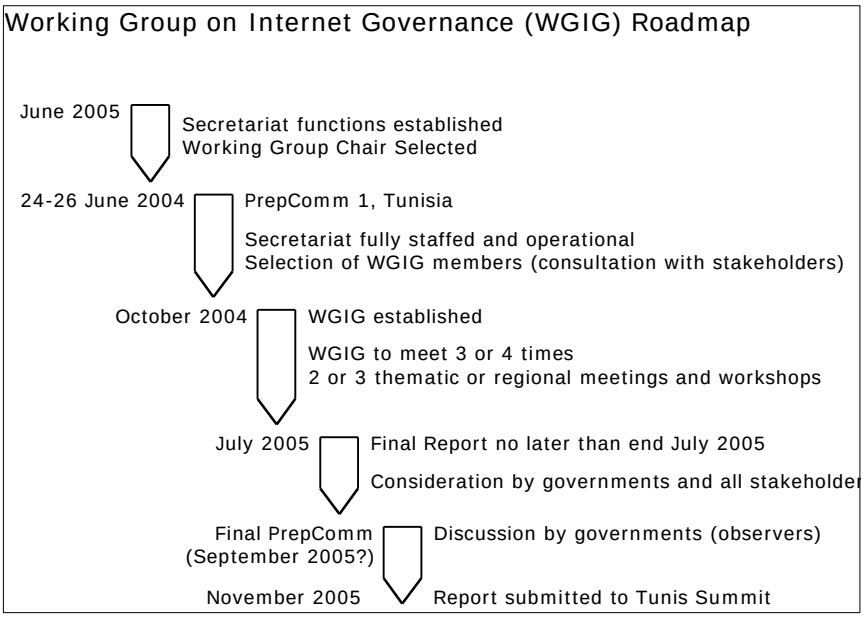


Figure 1.(above)

The working group has not yet been established, however, discussion about its structure, modalities and scope is underway. Ongoing discussions suggest that the working group will be quite small, between 15-20 people, but will take input broadly through a multi-layered structure. This structure will consist of the small high-level core membership of the working group itself, a wider network of stakeholders feeding into the core group through a series of two or three open-ended consultations, and perhaps regionally or thematically organised meetings and expert hearings.

Markus Kummer has been appointed to lead the working group's secretariat and commented that if stakeholders do not feel adequately represented by the process from the beginning then it will lack legitimacy and struggle to achieve any goal. He also suggested that members of the working group would be selected through a consultation process. Stakeholders will be consulted on who should represent them, and not have people appointed for them.

The working group can be expected to take a broad view of Internet governance, but without loosing focus on the underlying issues associated with ICANN. The working group cannot start its work by deciding to discuss only a few of the issues that have been raised by governments, it must begin by taking an inclusive approach or risk immediately alienating some from the process.

Civil society organisations, particularly from the South, must engage fully in the processes around the Secretary General's working group

?? The Secretariat is discussing suggestions on working methods and structure. How can civil society contribute to this process, both in terms of suggesting modalities and in practical offers to help arrange consultations broadly?

?? Markus Kummer has already begun to travel and speak at meetings around the world, showing a great willingness to reach out. Civil society must encourage him, and later other members of the working group, with invitations and opportunities to speak and to share ideas.

?? Membership of the working group will be decided before October 2004, and civil society will be consulted about the names of people to join the group. A challenge for civil society will be to agree on the qualities of the people to participate in this important process.

Ensuring developing nation participation

Comments by representatives of developing nation governments at the ITU Workshop and UN ICT Task Force Global Forum, made clear that the underlying problem to the discussion about Internet governance is the difficulty many governments have in contributing to and controlling global Internet policies. Not just related to the domain name system and ICANN, which has raised some important and genuine concerns for many nations, but more generally in policy making for all ICTs. Policies are being made in forums ranging from intergovernmental regimes negotiating on multilateral and regional basis, to private sector industry self-governance regimes negotiating across industrial sectors, and they are addressing issues that have economic, cultural and social implications for all society. Developing nations believe they are not able to take part to the extent that they must[5].

A suggestion was made during the ITU Workshop that the Secretary General's working group take on the additional task of studying the problem of enabling the meaningful and effective participation of developing nation stakeholders in ICT policy processes. The suggestion has gained support, but it is not clear that it will be adopted.

This is not a new issue, capacity building and participation was raised by the G8 DOT Force, and has since been taken up by the UN ICT Task Force and others[6]. The Summit documents reflect these ideas, placing great emphasis on the process of the working group, stressing its openness and inclusiveness. Speaking at Telecom Africa 2004, Markus Kummer said, "developing countries need to be given the possibility of making their voice heard. Their full and meaningful participation in this process will be essential. This of course involves traveling costs, but not only. There is also a need for efforts aimed at capacity building among developing countries, to allow them to defend their interests effectively."[7]

Whether or not the issue becomes part of the new working group's agenda, enabling participation and capacity building in ICT policy making processes, particularly Internet governance processes, should be a priority for civil society and developing nations.

* Markus Kummer has said he hopes to ensure developing nation stakeholders have the capacity to participate effectively in the Secretary General's Working Group. It is not clear if he intends to also recommend capacity building and participation in ICT policy making broadly as an additional action item for the Working Group to consider. He should do so, and civil society should encourage and support him.

* DOT Force recommended that organisations and fora working on global ICT policy should make a special effort to bring representatives of developing nation stakeholders into their discussions. Although endorsed by the G8, this has not happened to any great degree. The new working group is well positioned to correct this by vigorously encouraging those responsible for ICT policymaking processes to open their doors to all appropriate stakeholders.

[5] For further discussion see the Civil Society Internet Governance Caucus contribution to the Civil Society WSIS Declaration, "Shaping Information Societies for Human Needs", Geneva, December 8, 2003, section 2.4.7 Global Governance of ICT and Communications. http://www.net-gov.org/docs.php
[6] Digital Opportunities For All, Report of the G8 DOT Force, July 2001. http://www.dotforce.org/
[7] "Internet Governance: The way from Geneva to Tunis", M. Kummer, ITU TELECOM Africa 2004 Forum, 4-6 May, Cairo http://www.itu.int/AFRICA2004/forum/index.html

Capacity Building and universal participation in global policy making for ICTs

There have been a number of attempts to map how, where and by who ICT policy is being made, but they typically only offer descriptions of the venues and what issues are being developed in each[8]. Additional information is needed on the opportunities and obstacles for participation in each venue, which would enable stakeholders to prioritise their participation, and explanations are needed about why particular issues are important to countries' development goals. This is the kind of activity that the new working group should encourage, and civil society could undertake. The working group will be studying the policy issues involved in Internet governance and there is overlap between this and further and more effective mapping.

Many developing nations lack awareness of the importance of ICT and Internet policy issues in achieving development goals. Their internal markets are sometimes too small and inefficient for some of the new policy regimes, and consequently they lack technical and policy capacity and other resources to participate in these new processes. In many cases they are also not invited. "Louder Voices", a study by Commonwealth Telecommunications Organisation (CTO) and Panos London, on strengthening developing nation participation in ICT policy processes, identified each of the problems mentioned above as obstacles to participation, and is an important document for understanding the complexity of the issues[9].

WSIS Internet governance test

The Summit documents gave us some principles to consider when thinking about Internet governance. They say Internet governance should be multilateral, transparent, democratic, and open to all stakeholders. In the next sections of the report we look at different public policy issues --narrow and broad-- and it may be useful to keep these recommended principles of Internet governance in mind and ask if a particular process and policy issue satisfies them or not. Don MacLean, keynote presenter at the ITU Workshop on Internet Governance suggested that the extent to which governance structures met these principles might be considered a WSIS Internet governance test[10]. These governance principles, along with the obstacles to participation identified by the Louder Voices study can be useful tools for civil society as it considers the problems of Internet governance and the contributions it can make to the Secretary General's working group.

---

[8] The Markle Foundation has produced a number of valuable reports mapping ICT Policy processes and these can form the basis for further work. Markle in particular discusses the work of other entities such as the OECD, WTO, WIPO, etc. and their respective areas of competence, see in particular "Guide to International ICT Policy Making", July 2003, Markle Foundation
http://www.unicttaskforce.org/perl/documents.pl?id=1312 The UN working group must be aware of the work of other expert bodies and complement not duplicate.

[9] "Louder Voices: Strengthening developing country participation in international ICT decision-making", Don MacLean, David Souter, James Deane, Sarah Lilley, June 2002,
http://www.panos.org.uk/resources/bookdetails.asp?id=1065&null=1002&
Five main obstacles faced by developing nations to effective participation in ICT decision-making: (1) Lack of awareness of the importance of ICT in supporting economic and social development (2) Lack of technical and policy capacity (3) Lack of easy, affordable and timely access to information (4) Weaknesses in ICT policy/governance processes (5) Financial barriers

10 "Herding Schrodinger's Cats: Some Conceptual Tools for Thinking about Internet Governance", Don MacLean, keynote and background paper for the ITU Workshop on Internet Governance, ibid.

Defining Internet governance: names and numbers

Internet Corporation for Assigned Names and Numbers (ICANN)[11]

ICANN and the technical and policy processes associated with it were at the heart of Internet governance discussions. There was some misunderstanding about what ICANN does, and particularly about what it controls and the nature of that control, but there were also genuine concerns about its operations.

Some governments complained they were unable to control their country's domain name, that IP address allocation greatly favoured North American companies, and the location and control of root servers put their countries at a disadvantage on the Internet. The most significant problems stem from US control over the root server system.

Discussions held since the Summit have confirmed that some aspects of the DNS need urgent reform, but while ICANN is far from perfect, it does not exert the degree of control that some fear. Developing nations stakeholders should also be aware of the opportunities to influence ICANN's policy development processes and to participate in its representative structures. Detail of ICANN's structure and policy processes are discussed in the attached Annex.

ICANN: problems raised during WSIS

Controlling the Root Servers

The DNS Root Servers provide the master, or "root", level of the hierarchical DNS directory. Collectively, they manage a single directory called the "root zone" file, which contains a reference to all "top level" DNS servers, including generic or gTLD, and country code or ccTLD, servers. For a TLD to appear on the global Internet, it must be installed in the root zone file by the operators of DNS Root Servers[12].

There are 13 Root Servers around the world, the number limited by technical considerations. 10 Root Servers are located in the United States. The locations of the Root Servers are partly historic, the Internet being conceived and developed in the United States, but are also based on practical technical considerations. Root Servers should be positioned so that the maximum numbers of users enjoy the minimum response time when sending DNS requests, i.e. the Root Servers should be as close to as many users as possible. As Internet traffic has historically concentrated on the Internet exchange points located on the US East and West coasts, having root servers nearby makes sense. Root servers are also difficult to move, not physically but in terms of IP address routing issues.

"Anycast" and the deployment of "regional" root servers

The WSIS Plan of Action recommends that action should be undertaken to "promote

[11] ICANN was created in 1998 to be responsible for managing and coordinating the Domain Name System, services that were originally performed mainly under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities.

[12] The "HowStuffWorks" website has a plain English introductory description of the DNS which, http://computer.howstuffworks.com/dns.htm/printable The article is a little out of date, but technically sound.

regional root servers ... in order to overcome barriers to access."[13] What "regional root servers" are is not defined, but the recommendation seems to envision moving a root server from a current location (probably the United States) to some other place.

During 2003 while WSIS was in progress, a technique called Anycast 'was deployed that enabled one root server to be "cloned" in multiple locations. By January 2004 there were more functioning root servers outside the United States than inside its borders. An Anycast root server is an exact copy or mirror of one of the authoritative 13 servers; it contains identical data and performs exactly the same function, but can be located anywhere in the world. The request of the WSIS Plan of Action to deploy "regional root servers" was achieved even before the Summit was held[14].

Since the beginning of 2003, "cloned" root servers have appeared on every continent, to date, in 22 countries and territories. Anycast has significantly changed how DNS root services are distributed; yet it has been implemented with minimal involvement of ICANN, no formal policy development process, and no official consultation with the US Department of Commerce. That such a fundamental change to how the Internet works can take place with so little oversight certainly casts doubt on the view that ICANN rigidly controls the Internet. However, the US Department of Commerce does control the root.

Unilateral control of the root

The Internet Assigned Numbers Authority (IANA), now under contract to ICANN, publishes the content of the root zone file. The contract with the US Department of Commerce specifically prohibits IANA (ICANN) from making any "modifications, additions, or deletions to the root zone file or associated information that constitute delegation or re-delegation of top level domains" without permission[15]. There are two implications to this, one regarding deletion and the other re-delegation, and they represent the key problems with the DNS raised during WSIS.

The IANA contract gives the Department of Commerce the final authority on what appears or does not appear in the root. This situation where the United States has the potential to remove a country from the root, and therefore remove it from the Internet, is a serious concern for many nations. While it is extremely unlikely that the United States would use this potential power to remove a ccTLD, it is unacceptable to these nations that one country should have such control over the resources and rights of another. It also impacts on the good governance of countries' ccTLDs, and affects the introduction of future DNS services such as Internationalised Domain Names.

Right to appear in the Root

A solution that might be proposed and supported by civil society is to create a minimal international instrument that establishes a new inalienable right for a country/ccTLD to appear in the root zone file.

[13] WSIS Plan of Action, paragraph 13. d. ibid.

[14] An explanation about the DNS Root Server Mirror Service can be found here http://www.itu.int/itudoc/itu-t/com2/infodocs/023.html, and information about the locations of servers here http://www.root-servers.org/

[15] Contract Between ICANN and the United States Government for Performance of the IANA Function, 17 March 2003 http://www.icann.org/general/iana-contract-17mar03.htm

ccTLD re-delegation

The IANA contract also states that the US Department of Commerce must authorise the delegation or re-delegation of any TLD. Consequently, the US government has the final authority on who is responsible for administering a country's top-level domain.

Historically, the IANA assigned the right to administer a ccTLD to the first technically capable person from a country showing interest in its operation. The IANA made these assignments to a ccTLD manger on the basis that they were performing a public service on behalf of the Internet community, and the person or organisation is a trustee not owner of the ccTLD. Some of these early delegations have become contentious as they were made before many countries had any knowledge of the Internet. Governments are now aware of the importance of the Internet and either wish to take control of the ccTLD directly or assign control to an organisation they consider more appropriate.

To begin a transfer of a ccTLD from one designated manager to another, the old and new organisations must inform ICANN that the transfer is mutually agreed, and that the new manager understands the responsibilities involved. ICANN procedures say it is also helpful to have supporting correspondence from other parties affected by the transfer, and that it pays particular attention to the wishes of government. Where there is a conflict, perhaps the old manger refuses to give up the responsibility, ICANN tries to have the two parties agree rather than force a decision and become involved in local politics. This can be a very long process, one that many governments that have experienced contested re-delegations have found very frustrating[16].

This complex process is necessary as ICANN cannot re-delegate a ccTLD simply because someone asks it to do so. There are occasions when it is difficult to know who is speaking for the legitimate and responsible arm of a government. There are also technical considerations to the re-delegation. One of ICANN's key responsibilities is to ensure the security and stability of the Internet and a poorly operated or failing ccTLD could impact the operation of other parts of the global network, as well as provide bad service to users of the ccTLD locally. However, under the current arrangement, no government (except the United states) owns its ccTLD, and cannot order ICANN or the Department of Commerce to make any changes regarding its country's ccTLD.

> Lack of sovereign control is one the key issues in the Internet governance debate. Discussions since the Summit have made clear that for a number of countries resolving disagreement over unilateral control of the root, and the associated problems of deletion and re-delegation, are critical to making progress on Internet governance. They must be addressed quickly to the satisfaction of all countries or meaningful discussion on other issues will be difficult.

ccTLD operation

A government may not always be the right entity to run a ccTLD. A recent case study of Cambodia indicates that the ccTLD operation became less efficient and very much more expensive once the government took over control from the NGO that

[16] "Case study on .ke ccTLD redelegation" ITU Workshop on Member States' Experiences with ccTLDs, Geneva, 3-4 March 2003, http://www.itu.int/itudoc/itu-t/workshop/cctld/

founded the ccTLD[17].

Mauritius for Music

During the first phase of WSIS, a representative from the government of Mauritius claimed that the country's ccTLD, .MU, had been sold to a US-based domain name registrar to sell as the name for the music industry, and the government was begging to get it back. On the contrary, indications are that the .MU registry is operating efficiently, both technically and from a commercial and consumer service point of view. The registry serves the Mauritius market including the government. And the relevant Mauritius government department is in close contact with the ccTLD administrator. For a period of about 18 months a domain name registrar was marketing .MU partly for music related registrations, but that stopped some years ago[18].

The case of the Brazilian ccTLD, .BR, is more positive. The Brazilian ccTLD is controlled by the government, but operated as an "asset of the commons[19]", a shared common good for the benefit of all. It is a non-profit service, run on a day-to-day basis as a multi-stakeholder consortium. The Brazilian registry has built an international reputation as a well managed and technically sophisticated registry.

To register a name under .BR, a registrant must provide proof of legal status in the country (for example, national income tax registration.) This strict registration requirement has meant that Brazil suffers from very little domestic online fraud, as all registrants must prove who they are before receiving a domain name, and is an example of a country trying to create a secure domain for online, trusted commerce.

Many developing nations struggle with a ccTLD that is technically and operationally dysfunctional. Civil society together with government and private sector should document and promote ccTLD best practices. ccTLD managers and others from the Internet community in the ICANN process provide both technical and policy training and the new country code supporting organisation (ccNSO) will be a focal point for such support. ICT technical and policy capacity building around national ccTLD operations should be a priority

Despite Brazil's efforts to create a secure and trusted environment, a Brazilian delegate at the recent UNICT Task Force Global Forum on Internet Governance said that his government considers it cannot offer its citizens full security in the ccTLD until it has a guaranteed right regarding the appearance of .BR in the root server, and has the ability to decide who runs the country's name space[20].

[17] "Internet Governance Perspectives from Cambodia", Norbert Klein, 15 March 2004, submitted to the UN ICT Task Force's Global Forum on Internet Governance, New York, March 25-26, 2004.

[18] The .MU network information center describes some of the issues in a letter to users at http://www.nic.mu/mauritius/music.html?PHPSESSID=e8efb62b605976338ad28fb3cf6d6e01

[19] ".br: ccTLD as asset of the commons", Carlos A. Afonso, submitted to the UN ICT Task Force's Global Forum on Internet Governance, New York, March 25-26, 2004.

[20] Spoken comments by a Brazilian government representative at the UN ICT Task Force's Global Forum on Internet Governance, New York, March 25-26, 2004.

ICANN and ccTLD operations and policy

Beyond the contract requirements with the Department of Commerce, ICANN actually exerts very little control over ccTLD operations. ICANN does not say what fee a ccTLD operator should charge for a domain name, it sets no requirements on the structure of the ccTLD's name space. Some ccTLDs are run as de facto gTLDs, they don't serve their local community, but instead compete with the "ICANN" gTLDs. Tuvalu, the small Pacific Island nation with the ccTLD .TV, sold the right to market .TV to a corporation which promotes the name as a competitor to .COM and the other gTLDs. There are many similar examples: .TO, .NU, .CC, etc.

US government control over the root zone file and the re-delegation of TLDs, seems to have cast a cloud over how ICANN is viewed by some governments. It may also be adversely effecting how they view other organisations associated with ICANN.

Unequal allocation of Internet address space

IP Addresses are numbers used to identify computers and devices on the Internet. No two devices on the public Internet can have the same IP address so they must be uniquely assigned and this requires some degree of global coordination. The current Internet Protocol (IPv4) address pool has a limited number of addresses so assignments are made with a view to conservation[21].

Pointing to the fact that over 80% of IPv4 allocated addresses have been assigned to North American organisations, there was criticism during WSIS that IP addresses were being allocated unfairly. However, the majority of these allocations were made early in the Internet's history under a system that didn't anticipate the rapid growth of the Internet. The allocations were made in very large number blocks to Internet network service providers, universities and research organisations, and IT equipment corporations involved in early Internet projects. These early allocations account for more than 55% of total allocated IP address space. To resolve the problem, during the early 1990s the current system of regional allocation was introduced.

Geographically defined Regional Internet Registries (RIRs)

American Registry for Internet Numbers (ARIN) responsible for the North American region;

Asia Pacific Network Information Centre (APNIC) responsible for the Asia Pacific region;

Latin American and Caribbean IP address Regional Registry (LACNIC) responsible for Latin American and Caribbean

Réseaux IP Européens Network Coordination Centre (RIPE NCC) responsible for Europe and the Middle East;

AFRINIC, is being formed to serve Africa. Africa currently receives IP addresses from RIPE NCC and ARIN.

Today, organisations known as Regional Internet Registries (RIRs), manage the IP address space. All the RIRs are open, fee-based not-for profit membership organisations. They each develop policy through open, consensus based policy

[21] Internet Protocol version 4, IPv4, the current standard protocol for the Internet has over 4 US billion IP addresses, but this is not enough for future global needs. A new standard protocol called IPv6 is slowly being introduced and has an almost unlimited address space of many trillions of numbers.

development processes. The policy development process and policy decisions are archived so that they are publicly accessible[22]. At the global level, the IANA allocates IP addresses from pools of unallocated addresses to the regional registries according to their needs. The RIRs do not contract with the US government and are not subject to US government policy[23].

In the ICANN structure the RIRs form the Address Supporting Organisation (ASO) and provide the ICANN board with advice on global policy issues regarding the assignment of IP addresses. The final structure of the ASO is still being negotiated between ICANN and the RIRs. The RIRs recently established a new organisation, the Number Resource Organisation as a focal point for their global activities (http://www.nro.org/)

Addresses allocated since 1999 (percentage by RIR)

APNIC, 32%	(Asia-Pacific region)
RIPE NCC, 29%	(Europe, Middle East, North Africa)
ARIN, 37%	(North America, Southern Africa)
LACNIC, 2%	(Latin America began operating at the end of 2002.)

The regional registries have been operating fair and equitable allocation processes since the mid-1990s. However, many governments are clearly not aware of how they operate and particularly when compared to the ITU (which assigns responsibility for the management of the telephone numbering plan to nation states) the RIR system may be alien.

Problem of excessive early address allocations

The RIRs policy development processes should be used to begin examining the feasibility of reclaiming some of the address space allocated under the pre-RIR system (circa 1995). The open policy development processes present an opportunity for civil society to get involved in the work of the RIRs, and the formation of AFRINIC needs support and contributions from non-commercial organisations.

A positive response from the RIRs to the attention of WSIS would be to not only increase their outreach to governments (as they are bound to do), but to also seek to involve representatives of the public interest from civil society.

Internationalised Domain Names (IDN)

The promotion of multilingualism in the Information Society is one of the central features of the WSIS Declaration of Principles and Plan of Action. While the Internet can deliver text in email or by web pages in most of the world's languages and scripts, email addresses and web page addresses must be typed in English language "ASCII" characters.

During WSIS, some countries gave the impression that they considered the lack of IDNs to be the result of a pro-English language conspiracy. In fact, barriers to the

[22] A comparison of RIR policy processes is available from URL http://www.aso.icann.org/docs/rir-policy-matrix.html

[23] Authority for IP address allocation is not as clearly defined by historic contracts as other aspects of the DNS. The RIRs have accepted some US government oversight by virtue of having chosen to participate in the ICANN process, but there is no explicit control.

deployment of internationalised domain names had until very recently been technical, but new technical standards are now in place and the main obstacle to the deployment of IDNs today is a lack of resources to undertake what will be a very large global project.

The Internet Engineering Task Force (IETF) developed the technical standards for IDNs. ICANN began work identifying the technical and policy issues in 2001 and issued a comprehensive report in the autumn of 2002. Internationalised domain names at the second level, i.e. www.idn.org (where "idn" is the internationalised name in a non-English script) are now slowly being made available, but only western ASCII characters can be used for the top level domain names[24]. The technical standards are in place, but further cooperation regarding implementing is needed before IDNs can be added to the root zone.

The introduction of a fully internationalised system will require cooperation between countries and country code domain name operators, particularly between countries of the same language group. Internationalised top-level domain names will require new governance structures and policy development processes that are representative of the language groups they will serve. It is reasonable to assume that these structures will be very different from the current systems based on national or global scope. Furthermore, new internationalised TLDs will require entry into the root zone and this will make continued US unilateral control over the system even more contentious [25].

There are many problems to address and for the moment ICANN is not making significant progress. However, no other organisation is stepping up to support ICANN, or to take its place. The Multilingual Internet Names Consortium[26] (MINC) is one candidate, however as yet it has failed to earn the legitimacy and reputation required of an organisation capable of managing such an important global task. The ITU has held workshops on internationalised domain names, but lacks the core competency to address the issues and its policy development processes are too closed. Other organisations such as Unicode Consortium[27], the developer of the Unicode standard for representing language character sets and scripts in software and computer applications has yet to show interest. UNESCO does relevant work on preserving and encouraging local languages, but also has yet to show interest.

Internationalised Domain Names are a critical enabling technology that will make the Internet more useable and attractive to the majority of the world's population who do not recognise English. IDNs will encourage local communication and the creation of local content. Civil society, particularly from non-English speaking countries must be involved in activities to develop and deploy IDNs, and could take the lead in trying to bring together appropriate actors, such as a combination of those mentioned above, to re-start the IDN process.

[24] ICANN Internationalised Domain Name Committee http://www.icann.org/committees/idn/ . ICANN has many other issues to consider, from a lawsuit with VeriSign the largest domain name registry, to the introduction of a new set of TLDs, and the extra workload that the attention of WSIS has brought.)

[25] "The Multilingualisation of the Internet - Bridging the Digital Divide: Delivering Internet and Information Society Governance through Local Empowerment", Khaled Fattal, MINC. Paper submitted to the UN ICT Task Force's Global Forum on Internet Governance, New York, March 25-26, 2004.

[26] http://www.minc.org/

[27] http://www.unicode.org/consortium/consort.html

ICANN: obstacles to participation and the WSIS Internet governance test

Some ICT good-governance principles suggested by the Summit documents, and the five obstacles the Louder Voices study identified apply to ICANN. Discussions during the WSIS Geneva PrepComm made clear that many are not aware of what ICANN does, why it is important and how they can participate. Technical capacity is a significant barrier, and the range of policies ICANN's work touches requires that a government representative in particular must have a good understanding of matters ranging from competition policy to intellectual property rights, in addition to technical knowledge. Building the necessary technical skills may take years, but focusing on improving ccTLD operations in developing nations would be a logical place to start, as well as providing Internet IP training in technical colleges and universities (and ensuring that places of learning are connected to the Internet.)

Obstacles to participation and the WSIS Internet governance test

1. Awareness of the importance of ICTs
2. Technical and policy capacity
3. Access to information
4. ICT policy processes
5. Financing

And governance that is multilateral, transparent, democratic and open to all stakeholders.

ICANN's policy development processes and those of its related organisations are generally open to all, and access to information is, in theory, not an obstacle. However, ICANN is still trying to build relationships with many of its constituents and stakeholders and consequently there is no coordinated system for information and resources about the DNS[28]. Long established processes such as the ITU have become part of government's bureaucracies, with staff specifically responsible to handle the issues they raise. The Internet, ICTs and particularly organisations like ICANN, are too new for many developing countries to have developed such institutionalised internal policy processes and they find them difficult to deal with. ICANN also tends to operate in an ad hoc manner, some would say making up processes on the fly, which makes effective participation difficult.

ICANN is not the only new policy process that governments have to deal with and it is not surprising that many governments want a single international entity to coordinate Internet governance issues. As we consider the broader policy issues the working group on Internet governance will take on, the full scope of policy processes that some governments feel they are absent from, and need to engage in, becomes apparent.

For more detailed information about ICANN, please see the Annex at the end of this document.

Internet Governance Broadly

Internet pricing and interconnection, spam and network and information security and trust are described in the Summit documents as important issues that need to

[28] For example, an equivalent of the ITU's TIES network http://www.itu.int/TIES/intro.html

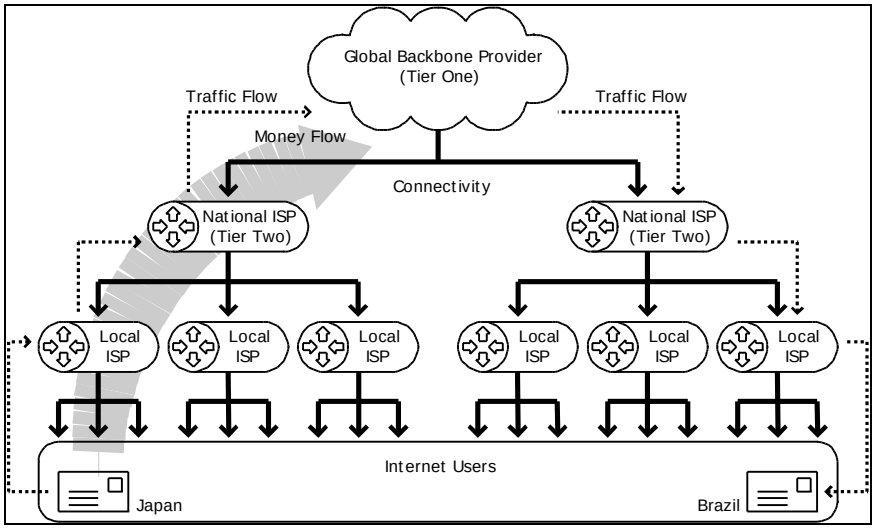
be addressed. They are referred to separately from the paragraphs about Internet governance, however since the Summit there has been support for having them considered by the Secretary General's working group.

Internet pricing and interconnection

"*When an end user in Kenya sends email to a correspondent in the USA it is the Kenyan ISP that bears the cost of the international connectivity from Kenya to the USA. When an American end user sends email to Kenya, it is still the Kenyan ISP that bears the cost of the international connectivity, and ultimately the Kenyan end user who bears the brunt by paying higher subscription fees.*"[29]

In traditional telecommunications, the cost of international connectivity has typically been shared, either by each party paying for half the cost of the connection, or by settlements based on the amount of traffic exchanged. Unlike telecommunications, which for more than 100 years has evolved a complex system of international charging agreements, there has been no economic regulation of the Internet. The Internet industry is based on an economic model of bilateral agreements between customers and providers, and on mutual peering.

Figure 2. Traffic and payment flows across the Internet



The diagram shows a very simplified picture of the Internet industry and how traffic and payments flow when email is sent from one country to another. From the top down, the diagram illustrates how providers at each layer resell Internet connectivity to providers at the layer below. Connectivity flows down, and money flows up.

The end user buys connectivity from a local ISP. To carry the user's email across the Internet, the local ISP sends it to an upstream provider, a national or perhaps regional provider that has a network connecting different towns and cities in that country or region. The local ISP, known as a "tier three" provider, pays the larger "tier two" provider for this connectivity service.

[29] ICT Policy: A Beginner's Handbook. Association for Progressive Communications, 2003, http://www.apc.org/books/. The handbook provides a good description of peering and interconnection, and many other ICT policy issues.

To carry the email internationally, the national ISP routes traffic via global carriers, known as Internet backbones or "tier one" providers. These are companies with high capacity continental and international connections. Again, payment is made from the customer to the provider of service, i.e. from tier two to tier one.

Tier one providers connect with other tier one providers, and tend to do so on the basis of peering, their traffic flows are about equal so it is mutually beneficial for them to simply exchange traffic as equals. Unless there's a large imbalance of traffic, tier one providers don't usually pay each other. Instead they operate on a "sender keeps all" model, i.e. they keep the fees they receive from the providers below them. After peering across the tier one providers' networks, traffic then flows downstream, from tier one to tier two, and on to the end user. But money only flows upstream. At each layer, the customer receives service from a provider and pays for that service.

The result of this model is that developing nations and smaller ISPs must pay for the full cost of connectivity to the Internet, and they regard this as fundamentally unfair.

Comparison with the most commonly used traditional telecommunications settlement regime only makes matters worse. International telecommunications settlements tend to favour high cost monopoly carriers over those operating at lower costs in competitive markets[30]. Settlements are made on the basis of the amount of calls terminated by one country in another, and the payers under the regime tend to be developed nations, and the recipients developing nations. Settlements are made in US$ and can amount to hundreds of millions each year. For many developing countries telecommunications settlements are among their most important sources of hard currency[31].

Origins: International Charging Arrangements for Internet Services (ICAIS)

The problem of Internet interconnection pricing was first raised by APEC Tel (Asia-Pacific Economic Cooperation Telecommunications & Information Working Group) in 1998 in a study called International Charging Arrangements for Internet Services (ICAIS), and has since been taken up by the ITU. It is not just an issue for developing countries, one of the main complainants is Australia, which because of its remoteness pays very high charges for connectivity to the United States.

ITU T Study Group 3 is now the main forum where these issues are being discussed, and unfortunately most of the relevant documents are only available to ITU members (national governments or ITU sector members), meetings are typically for members only or invited experts and decisions are made by members.

[30] The traditional telecommunications model is known as the "Accounting Rate" and is very complex. The ITU provides a useful overview http://www.itu.int/ITU-T/studygroups/com03/accounting-rate/

[31] The accounting rate and the high revenues it brings is the main reason why many developing nation governments refuse to allow voice over Internet calls. For background discussion of the issues see a series of reports on International Charging Arrangements for Internet Services (ICAIS) at http://www.tmdenton.com/pub/reports/

Three main types of connection relationship being discussed

Peering - the largest international ISPs, tier one providers, operate peering arrangements for the exchange of traffic. The payment structure is "sender keeps all", the providers consider themselves peers and anticipate a rough balance in traffic exchanged. Peering arrangements tend not to be transparent.

Transit - where the client, usually a tier two or tier three provider, supplies the access line in both directions, and pays the full charge to connect to the upstream Internet supplier. Most providers connecting to the US and Internet backbone use a transit arrangement and this is the model that is being challenged.

Settlement peering - the cost of the connection is shared and traffic is measured. The party with more traffic pays the difference. Such arrangements involve negotiated bilateral commercial agreements between providers.

The ITU working group is now apparently trying to reach agreement between two proposed solutions. One based on allowing market forces and negotiations between providers to determine appropriate interconnection rates and conditions (with a provision for development aid to support countries where there is market failure.) This position is supported by "Industry", mainly large telecommunication operators. The second is a solution based on settlement peering, where if a mutually satisfactory negotiated agreement cannot be reached then the entities involved may use economic measures and traffic flow to determine who pays what. However, Internet traffic (packets) is much more difficult to measure than voice calls and this seems to be the main sticking point in negotiations at the moment. This second solution has been supported by China and some other developing countries.

This is a critical issue, but one that is very difficult to follow as most of the discussions and documents are not publicly available.

Internet Exchange Points and regional backbones

The WSIS Plan of Action recommended measures to keep Internet traffic as local as possible as part of the answer to the problems of Internet charging and interconnection. It encourages the build-out of local and national Internet Exchange Points (IXPs), to keep traffic in-country that might otherwise be sent to the US backbone before returning, and the creation of regional Internet backbones, so that traffic to neighbouring countries does not need to flow via more expensive international routes.

IXPs can be established relatively easily and cheaply and can bring significant benefits to the local Internet in terms of reduced costs, reliability, and ease and speed of use. IXPs also aggregate demand for bandwidth and so are in a better position to negotiate rates for international connectivity[32].

[32] Global Internet Policy Initiative's Project's "Internet Exchange Points: Their Importance to Development of the Internet and Strategies for their Deployment - The African Example" http://www.internetpolicy.net/practices/ixp.pdf June 2002.

The ITU Study Group 3 fails the WSIS governance test of being "multilateral, transparent, democratic, and open to all stakeholders"

If Internet pricing and interconnection is to be considered by the Secretary General's working group, then the main forum where it is being discussed should be more open and transparent. Documents should be made freely available, and all relevant study group discussions and meetings should, within reason, be open so that all stakeholders are able to participate.

Spam: Unsolicited Bulk Email

Spam is one of the most significant problems facing the Internet. The enormous volumes of spam are a significant pricing factor for Internet service providers of all sizes, and their costs are passed on to end users. Given the problems of Internet pricing and interconnection just described, the effect of spam on developing nations is especially severe. It also degrades quality of service, particularly on the low-bandwidth and already congested links of poorer users.

According to the anti-spam company Brightmail inc., in April 2004 64% of all Internet email was identified as spam

Brightmail provides data on spam by subject category, and claims that 15% was Adult content, 7% Scams such as pyramid selling schemes, and 5% fraudulent, often used to trick people into revealing personal information. In February 2004, Sophos Plc., another anti-spam company, produced a 'dirty dozen' of top spam producing countries, and claimed that almost 57% of all spam messages originated from the United States. Canada was a distant second as the source of 6.8% of the world's spam. China and South Korea were third and fourth respectively with approximately 6%, and in twelfth place, Spain with just over 1%. The US is by far the largest producer of spam[33].

Spam is also increasingly associated with network security problems. Spammers use software viruses and worms to infect computers and hijack user's email address books as a source of more addresses to spam. Software viruses can also take control of a computer, usually without the owner being aware, so it can be used as launch pad for sending spam.

Spam is undermining the reliability of the Internet, has become a major drain on productivity, and is negatively affecting user's confidence in online commerce. Email was widely considered the Internet's "killer application", offering cheap, fast global communications. Spam is making email a chore.

Stopping Spam

Many countries have introduced legal and regulatory measures to combat spam, and combined with other consumer protection and business laws have made many of the practices used by spammers illegal or in contravention with existing regulation. Yet despite these efforts spam continues to grow rapidly: spam accounted for 10% of Internet email in 2000, 48% in May 2003, and 64% in April 2004. Spammers hide their tracks well and finding and prosecuting them is difficult and costly, particularly across jurisdictions. International cooperation is clearly

[33] Brightmail http://www.brightmail.com, Sophos http://www.sophos.com.au/pressoffice/pressrel/au/20040227dirtydozen.html

essential, but countries should also examine their existing enforcement measures, add new measures where required, and enforce such measures if or once they exist.

A Northern problem to be addressed by the South

Over 90% of spam is currently generated by OECD nations, but as more people come online, spammers will no doubt be among the new online population. Nations in the process of developing e-Strategies and ICT policies should ensure that anti-spam measures are included, and appropriate laws and regulations are in place.

As the Sophos 'dirty dozen' shows, spam is a cross border problem and solutions will require some form of international cooperation and coordination. Yet there is no common international agreement on what constitutes spam, even at a fundamental definitional level. In the United States, commercial speech can be regulated, but other forms of speech cannot. Consequently, in North America, spam is usually described as "unsolicited commercial email", most other parts of the world say "unsolicited bulk email". In cross border situations, lack of common agreement on what spam is leads to confusion over what law or regulation may have been broken.

Limited impact of technical solutions

Technical solutions are only having a limited impact. Client and server filtering software is available for incoming mail, and these filters identify and reject spam quite effectively. Large ISPs filter email as it travels across their networks. But spammers have responded by devising methods to fool the filters, and economics is on the side of the spammer who can easily and cheaply send more and more spam in the knowledge that some will get through. Filters are not perfect and often reject legitimate email along with unwanted spam. User surveys indicate that most people believe filters prevent some of the email they send from being delivered, and some email sent to them from being received.

The Internet Engineering Task Force (IETF), the Internet's main standard's making body, has been discussing spam for some years and recently began work on a solution to attack spam by authenticating that email is being sent from a real email address. The IETF's measures will prevent a common spammer technique called "spoofing" that fakes an email header to make it look as though the message comes from a legitimate sender. Preventing spoofing will only eliminate a small proportion of spam, but it will prevent an increasingly common form of online fraud known as "phishing". Microsoft and Yahoo! are also developing email authentication systems to prevent address spoofing.

Phishing, don't be fooled

A phishing attack uses fraudulent email to lure sensitive information such as passwords, credit card details and other personal information from a victim. The email uses spoofed headers to pretend to be a trustworthy party such as an online banking service or online auction --Citibank and eBay are common targets-- and directs the user to a website designed to fool the recipient into giving up their personal data. The email and websites look very authentic and a recent study by the Gartner Group claimed that phishing attacks cost US credit card companies and banks US$1.2billion in 2003.

Spam is much more than a nuisance, it costs billions of dollars each year, and is increasingly associated with criminal activity. Internet service providers and organisations running their own mail servers have an obligation to improve their network and security management practices to prevent their users from either

deliberately or unwittingly sending spam. The adoption of industry best practices and improved user education are essential as many organisations and individuals fail to protect their networks and computers because they don't know how.

Spam: international solutions

A risk associated with regulating against spam, particularly any centralised international regime, is that it might easily become a first step in the global regulation of Internet content. Given cultural and other differences, and the nature of the decentralised Internet, a centralised regime would be unlikely to be effective, any temptation to coordinate broader content regulation must be resisted. As the Internet governance working group can be expected to focus on international coordination and harmonisation issues, this concern should be emphasised.

So what form should international cooperation take? The European Union issued a directive on spam that member states were required to implement in locally appropriate form by October 31, 2003. More than six months later, and more than half the EU's members have not complied.

EU policy development typically follows a subsidiary model requiring that problems should be addressed at the most local level possible. For the implementation of legislation this usually means at the national level. However, directives are developed and agreed regionally at the EU as general requirements that are then adapted by member states to suit local conditions. The principle of subsidiarity is valid, but a more effective implementation would be for nationally developed solutions, emerging in a bottom-up fashion, to be coordinated and harmonised at the regional and international level.

> Develop policies at the national level, coordinate internationally, learn from the best practices of others.

The development and sharing of best practices should be supported, as should knowledge and acknowledgment of different legal and regulatory systems. Mutual recognition through bilateral agreements and Memorandum of Understandings can give more binding power to loose arrangements. Monitoring compliance is important, and organisations such as the OECD, the European Union, as well as individual governments and civil society must be willing to "name and shame" nations that persist as major generators of spam.

> * Civil society ICT programs should include toolkits and best practice guides for organisations running their own email servers, particularly providing advice on network management issues such as preventing open email relays, implementing spam control measures, use of anti-virus software, and appropriate outgoing mail filtering[34].
>
> * User education about spam, particularly not to buy from spammers, on using personal filters, etc. might also become part of civil society ICT programs.
>
> * Within the UN secretary general's working group, civil society needs to be aware of the risks of anti-spam activities becoming a first step to other content filtering and regulation.

[34] Civil society organisations should be aware that filtering technologies have implications for free speech.

Network, information security and trust

"*In order for the Internet to contribute to economic growth, human development and democratisation, it must be trustworthy and secure. Lack of trust and security jeopardises development goals that could be supported by a widely accessible and widely trusted Internet*."[35]

Creating a trusted environment in cyberspace is essential for the development of Information Society, and was one of the central themes of the WSIS process. Network security, information security and trust and privacy and consumer protection involve a broad range of complex issues that will be a challenge for the working group to address in sufficient detail. The Summit documents suggest they should be considered in a holistic way, that is, security and the fight against cybercrime should not come at the cost of reduced privacy and other rights.

Cybercrime and network security

Countries need to ensure that new types of computer-mediated and online crime can be prosecuted under national criminal law, and that these laws permit the international cooperation necessary to investigate and prosecute crimes carried out over the global network. Developing nations working on e-strategies should make sure such laws are included in new policy and legal frameworks. At the same time, these new laws and new types of law enforcement methods must not infringe on any human rights standards, particularly rights to speech, privacy, and freedom from surveillance.

Hacking attacks, viruses, worms, spam and other email borne malevolent software and scripts are a serious threat to the security and stability of the Internet. Users can take some measures to combat these threats by, for example, using anti-virus software and by following good network practices when using the Internet and downloading files. Service providers can ensure their networks and servers are as secure as possible by acting on security advisories, upgrading equipment, and installing patches, etc. National strategies to use free and open source software and avoid more vulnerable proprietary systems can be effective. But there are no easy solutions, and responses must be coordinated internationally. This might include supporting and improving the network of centres specialising in coordinating information about computer and network security incidents (CERTs), and by adopting model legal conventions to create more binding international cooperation.

CERTs and Civil Society

Organisations known as CERTs have been operating internationally since the early 1990s as focal points for information about computer and network security incidents. Usually operating at a national level, they are also centres for providing advice on best practices and training. There is a CERT or organisation with a similar function in most developed nations, but there are too few in the developing world. Civil Society can usefully develop and support activities to pool knowledge about new attacks and vulnerabilities, and provide training for service providers and users.

There are regional CERTs in Europe and the Asia and Pacific to coordinate among national activities, and to support the creation of new national CERTs. CERTs usually have origins in the academic and research community, and often have close ties with national government. Establishing national and regional CERTs should be considered in civil society ICT development programmes[36].

[35] Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime, August 2002, Global Internet Policy Initiative. http://www.internetpolicy.net/

[36] CERT Coordination Center -- originally the computer emergency response team (CERT), however the acronym does not describe a CERT's purpose which is computer security incident response and

Model laws and international agreements

The Council of Europe Convention on Cybercrime has been discussed in WSIS, both before and after the Geneva Summit, as a potential model international legal agreement[37]. Non-EU member states can sign the Convention and as such it can be the basis for creating national laws on a foundation of internationally accepted principles. The convention addresses substantive computer crimes, and also laws on search and seisure, interception, the disclosure of records, and on transborder cooperation with respect to those issues.

The Convention provides a starting point, but it is controversial, particularly in extending cross border surveillance, and critically it offers very weak support for human rights and privacy. This is not a concern for EU member states as they have signed international human rights conventions and EU directives on privacy and the Cybercrime Convention defers to those other "higher" conventions and directives. But the Convention would be a dangerous document for nations that are not signatories of universal human rights, privacy and other similar declarations[38]. This makes the Convention very problematic as a model for many developing nations, and for WSIS.

International agreements must respect WSIS principles

Cyber-Crime Convention

WSIS documents explicitly mention consideration for privacy as an essential element of building confidence and security in the use of ICTs. It would be inappropriate for any WSIS process to support the Convention unless it was amended to reflect privacy and other human rights needs. The Internet governance working group, intended to be an open and representative process, could be well positioned to advise on how the Convention should be amended. The thematic and expert meetings suggested as part of the working group's consultation process, could serve to bring in a broad range of views on what would be necessary to make the Convention acceptable. However, the Convention should not be adopted as an international model supported by WSIS unless it satisfies the concerns raised by all stakeholders.

Digital Millennium Copyright Act (DMCA)

Other national and regional legislative packages are also becoming global standards. In the area of intellectual property rights the United States' Digital Millennium Copyright Act (DMCA) has been widely criticized, yet other countries are gradually adopting many of its provisions. Before the DMCA is adopted further, the Internet governance working group could offer improvements agreed by all stakeholders to make the Act more globally appropriate. The Secretary General's working group is well positioned to ensure that any model laws and processes supported and promoted by WSIS are consistent with the intent of the WSIS Declaration on Principles and Plan of Action.

---

coordination. The first CERT was established in 1988 at Carnegie Mellon University, and is federally funded. Many CERTs are now run as industry supported non-profits.)

[37] The Convention website is at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=16/05/04&CL=ENG

[38] Global Internet Policy Initiative, ibid. The GIPI report offers a good summary of the convention, the issues it addresses and its failings.

Civil society must monitor new legislation on cybercrime and security and ensure that fundamental rights to privacy, freedom of expression, and freedom from surveillance are not weakened.

Within the Secretary General's working group, civil society should ensure that any model laws and processes supported and promoted by WSIS are consistent with the intent of the WSIS Declaration on Principles and Plan of Action.

Establishing national and regional CERTs should be considered in civil society ICT development programs.

Broader policy issues

The Secretary General's Working Group must take care to ensure that it does not become a 'catch-all' forum for discussing all pressing ICT policy issues. Spam, security and Internet pricing and interconnection were identified by the WSIS Declaration and Plan of Action separately from the paragraphs about Internet governance, but are important policy issues that many believe should be looked at by the working group. Other issues such as developing guidelines on appropriate content, international rules for e-commerce, taxation, encryption, intellectual property rights, and so on are also being suggested as relevant policy issues. But the list of issues before the working group must stop somewhere or it will not be able to complete any work.

Conclusion: Making the most of Internet governance

The Secretary General's working group on Internet governance, and the provisions of the WSIS Geneva Summit documents provide an opportunity for developing nation stakeholders, particularly those of civil society, to begin to play a greater and more equal role in ICT policy making processes[39].

The working group is being formed now, its structure and modalities are being decided, and opportunities to contribute to these activities are there to be taken immediately. Civil society faces a particular challenge in that it must decide how to agree on the criteria and then names of people it can recommend to participate in the working group. Civil society can either decide for itself, or have people appointed for it.

The secretariat appears very committed to supporting the participation of all developing nation stakeholders. The secretariat's attempts to reach out must receive a positive response -- organising national, regional and issue-oriented consultations, and offering the secretariat and working group members the opportunity to participate in such activities. Civil society must actively engage.

The working group is already short of time having to complete its work by July of 2005. The broader the range of tasks the working group takes on, the more likely it is to be unable to deal with any issue in sufficient detail. A risk then is that the working group might become a means to rubber-stamp the adoption of new international agreements with little or no public scrutiny. For example, encouraging widespread ratification of the Council of Europe Convention on Cybercrime without adequate national level debate. Civil society's participation in the working group and through contributions to consultations can guard against this. Civil society can

[39] The working group and secretariat do not yet have a website or way of distributing information, but the civil society plenary <http://mailman.greennet.org.uk/mailman/listinfo/plenary> and Internet governance caucus <http://www.net-gov.org> mailing lists provide regularly updated information.

also ensure that the provisions of the Geneva Summit documents that explicitly support essential human rights are upheld and taken into consideration if and when the working group supports the adoption of any new international policy framework.

The Summit documents and the rights they endorse and protect can be used to ensure that Internet governance is defined in such a way as to preserve these universal rights. But this can only happen if civil society takes every opportunity to engage in the working group and all its activities.

Appendix: ICANN structure and civil society

Evolution of ICANN

ICANN is a California based non-profit corporation established by the US Government to begin to take responsibility for the management of the Domain Name System (DNS).

The development and management of the DNS had historically been carried out by an organisation called the Internet Assigned Numbers Authority (IANA) under research and other grants from the US government. The IANA is more a set of technical functions than an actual entity, and when ICANN was created it took responsibility for the IANA functions under a contract with the United States Department of Commerce[40]. Those functions include the assignments of technical protocol parameters, coordination of IP address space allocations, the oversight and implementation of polices for DNS registries and registrars, and oversight of the root server system. ICANN also took responsibility for the Department of Commerce's contract with Network Solutions, Inc. (NSI) to manage the generic top level domains (gTLDs) .COM, .NET and .ORG [41].

The avowed intention behind ICANN's creation was to privatise and internationalise the DNS, to introduce competition, and over time hand over responsibility for DNS management to the global Internet community. ICANN has introduced competition to the registrar business for domain names, and has created a very limited number of new TLDs. However, the United States is showing few signs of loosening its oversight on ICANN.

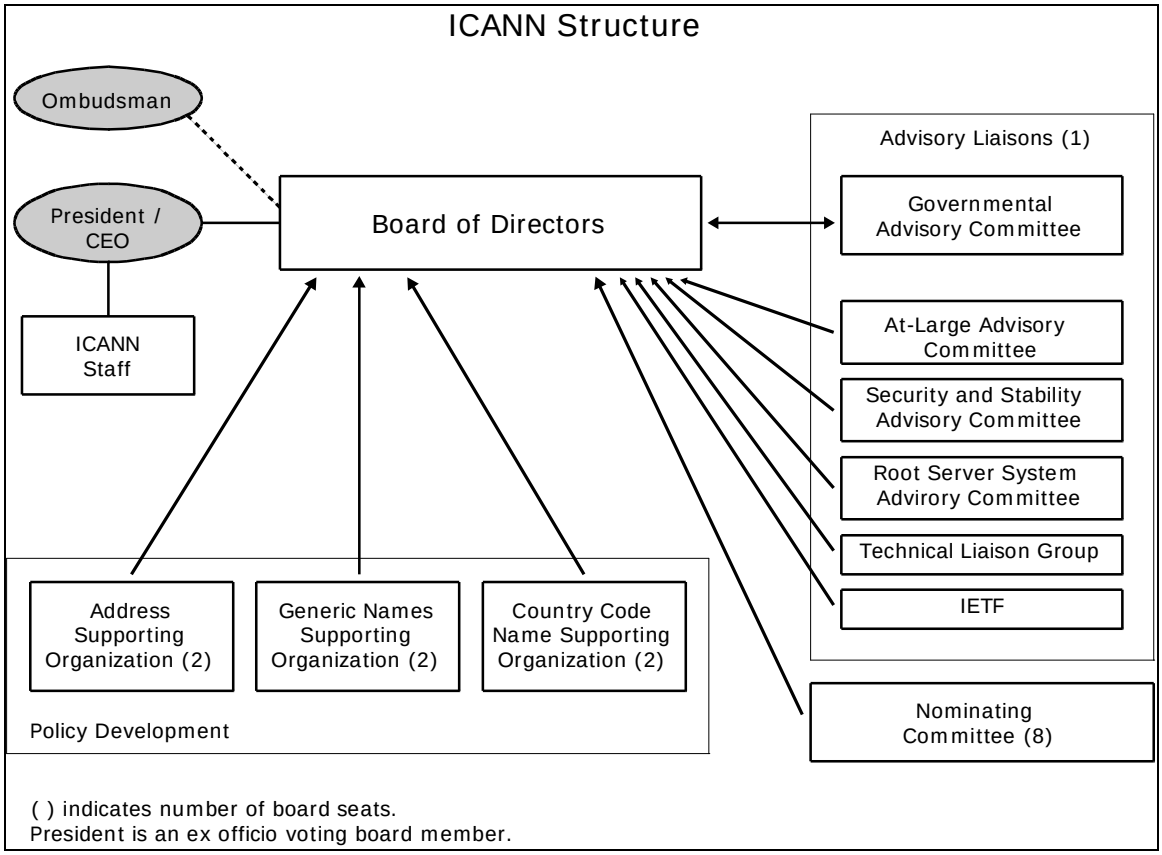
Participating and ICANN and making policy

ICANN's representative structure and policy making process has undergone a number of reforms since its creation in 1998. It aims to represent the Internet community via Supporting Organisations made up of stakeholders who receive resources from ICANN, provide services for or with ICANN, or whose business interests are affected by the ICANN's decisions. There is also an "At Large" organisation to represent the interests of individual Internet users.

[40] Contract Between ICANN and the United States Government for Performance of the IANA Function, 17 March 2003 http://www.icann.org/general/iana-contract-17mar03.htm

[41] The security software maker VeriSign bought NSI in 2000. In 2002, as part of ICANN's program to introduce competition to the domain name market, .ORG was divested and assigned to a new registry operator the Public Internet Registry.)

Figure 3.



The ICANN Board has 15 voting members. A nominating committee selects eight board members, and three supporting organisations, an Address Supporting Organisation (ASO), Generic Names Supporting Organisation (GNSO) and Country-Code Names Supporting Organisation (ccNSO), each select two members. The user and technical communities each select one non-voting board liaison, as does a Government Advisory Committee. The three supporting organisations also advise the board and develop policy on issues relating to their respective areas of competence. Supporting organisation typically manage their policy processes through a representative council, for example the GNSO "Names Council".

Geographic Diversity

One of ICANN's founding principles is to support geographic diversity in all its representative structures. Each of five regions -- Europe; Asia and Pacific; Latin America and Caribbean islands; Africa; and North America -- shall be represented on ICANN's decision making bodies, with a view towards creating diversity and balanced representation.

ICANN's representative structure has been criticized for being dominated by business interests, particularly after it cancelled a commitment to select half the board by a direct vote of Internet users, and replaced the election with a nomination process[42].

[42] The author was a member of a study, The NGO and Academic ICANN Study (NAIS), critical of ICANN's treatment of the At Large, see http://www.naisproject.org

This report will not go into details of problems with ICANN, needless to say ICANN has been criticized as suffering from a lack of legitimacy and accountability, and failing to fairly represent all stakeholder interests. After more than five year's, too many of ICANN's policy processes are still ad-hoc.

Despite disappointment over the fate of the "At Large", the supporting organisations and other representative processes offer opportunities for civil society to participate in ICANN and should not be ignored.

gTLD policy development

The GNSO is responsible for the policy development processes for gTLDs. Its work is the heart of ICANN's business and in the WSIS process was the least controversial of ICANN's activities. The management of the generic top level domain space has always been carried out by organisations under contract with the US government, and ICANN's rights to make policy in this area are not disputed[43].

The GNSO is comprised of six constituencies, five representing commercial interests and one, the Non-Commercial Users Constituency (NCUC), the interests of civil society. Like all supporting organisations and their councils, the GNSO and its constituencies must follow ICANN's requirements to be geographically representative.

The GNSO makes policy recommendations to the ICANN board that effect consumers and the Internet industry on a range if issues, from the creation of new domain names, to matters such as privacy concerning the Whois database and mechanisms to protect intellectual property rights through new dispute resolution procedures. These policies have an impact on the Internet broadly and the unequal civil society representation in the policy development process is problematic.

GNSO constituencies: favouring business

The Non-Commercial Users Constituency is the lone civil society voice among GNSO constituencies, its influence is limited but not insignificant. There is also a Commercial and Business Users Constituency, which has only one member from a developing nation, and no Southern SMEs (although the constituency has a number of large international business associations as members and they indirectly represent many SMEs, some perhaps from the South.) There is an Internet Service and Connection Providers that is also dominated by members from Europe and North America, it currently has just one member from Africa[44].

The NCUC is a membership organisation, and charges a small fee, $50/year, which may be waived for members from developing nations. Information about the work of the NCUC and how to join is available on the constituency website <http://www.ncdhc.org>

Civil society and southern commercial and non-commercial organisations must take the opportunity and participate in these GNSO constituencies. ICANN's principle of supporting geographic diversity in its representative structures is an opportunity that should not be ignored.

[43] Although how ICANN makes policy has been the subject of a lawsuit from VeriSign, see http://www.icann.org/general/litigation.htm

[44] Details of GNSO constituencies can be found on the organisation's website http://gnso.icann.org/

At-Large Advisory Committee

The At-Large Advisory Committee (ALAC) was created in 2003 as an outcome of ICANN's reforms to replace the original commitment to elect half the board "At Large", i.e. not as representatives of any industry or user group represented by the Supporting Organisations. The global election process was replaced by a Nominating Committee, which selects eight of ICANN's 15 member board, and makes appointments to the ALAC, and to the GNSO and ccNSO councils. ALAC provides policy advice on issues related to the interests of individual users. It appoints one non-voting liaison member to the ICANN board, five members of the Nominating Committee and one non-voting member to the GNSO council. It is expected that ALAC will appoint one non-voting member to the ccNSO council once agreement about the ccNSO has been reached.

ALAC is designed to facilitate "bottom-up" user participation to ICANN process. Eventually, 10 ALAC members will be selected by "Regional At Large Organisations" (RALOs), and five by the Nominating Committee. There will be a RALO for each of the five geographic regions, and each RALO will select two members to serve on the ALAC. Each RALO will be made up of more than three At-Large Structures (ALS), which are essentially existing or new organisations that represent individual users, i.e. membership organisations of some kind that are interested in ALAC's work in ICANN.

For many ALAC is tainted by its association with the broken promises over commitments to hold direct elections for half of ICANN's board. However, ALAC members have had a notable impact on GNSO policy development, and its members have been instrumental in helping ICANN understand and become involved in WSIS. When the ccNSO Council is formed, ALAC will hopefully be at least as influential in that forum as it has been in the GNSO[45].

> ALAC offers a means for individuals to participate in ICANN and should not be ignored, and civil society organisation's support for the At-Large Structures would help to more quickly legitimise ALAC and enhance its standing with ICANN. It is hoped that the At-Large Structures, as confederations of ICT users organisations, will over time develop the capacity to give users a voice in other ICT policy processes. They have the potential to be useful representative structures, particularly for civil society in developing nations.

Nominations replace elections

In 2003, ICANN's Nominating Committee filled eight ICANN board seats, five ALAC positions and three seats on the GNSO Council. The Nominating Committee process was well publicised, however only 110 people put their names forward as candidates.

5% of candidates from Africa
8% of candidates from Latin America and Caribbean
17% of candidates were female

ICANN's policy development process favours large corporate interests and organisations from the North. ICANN needs further reform, but there are still opportunities for civil society and the South to participate in ICANN and to try and make it more responsive to their needs. Responding to the Nominating Committee's

[45] ALAC's website can be found at http://alac.icann.org

call for candidates is one such opportunity[46].

Country-Code Names Supporting Organisation (ccNSO)

ICANN's relationship with the ccTLD managers has always been poor. Under ICANN's original organisational structure all TLD policy was the responsibility of a single supporting organisation, the Domain Name Supporting Organisation (DNSO). ICANN's most pressing tasks after it was created were related to gTLDs --particularly ending VeriSign's monopoly in both the gTLD registry and registrar markets -- and while ccTLDs were paying to support ICANN they were getting nothing return. Some ccTLDs mangers also said they believed ICANN was withholding some services as a bargaining chip in an effort to persuade them to sign agreements with ICANN. But this situation at last seems to be improving. A new ccTLD supporting organisation, ccNSO, was created in March 2004, and while a majority of large European ccTLD managers have not yet joined, they are continuing to negotiate towards reaching a solution that will make it acceptable for them to do so[47].

The ccNSO, like other ICANN supporting organisations, selects two people to join the ICANN board and is also represented on the Nominating Committee that fills the At Large board seats and other positions. The ccNSO is only responsible for developing and recommending global policies relating to country code top level domains to the ICANN board. Domestic issues are not ICANN's concern, they are the responsibility of the ccTLD manager and the country's local community, however that is constituted.

The GNSO inherited the multiple constituency structure mentioned earlier from the DNSO, however there is no similar arrangement in the ccNSO, where only ccTLD managers and their representatives discuss and make policy. Consequently there is no non-commercial users' voice in the global ccTLD policy development process. Businesses and the Internet industry are typically well represented in the local ccTLD organisation, however civil society representation is often missing.

> The good technical operation and representative structure of ccTLDs is of great importance to developing nations and civil society. Developing best practice for all aspects of ccTLD operation and participating in any local Internet community participation in a ccTLD cannot be stressed too strongly. The ccNSO is an important new organisation in the ICANN structure and the current lack of civil society representation in it further emphasises the importance of the Nominating Committee process, which seats representatives on the ccNSO council, and the role of the ALAC liaison to the ccNSO as the only civil society participant in the ccNSO council.

Address Supporting Organisation (ASO) coordination of IP address policies

Organisations known as Regional Internet Registries (RIRs), manage the IP address space. As the names suggests, they are regionally based organisations providing services to designated geographic regions.

---

[46] The Nominating Committee selects new board members and council representatives on an annual basis. Details can be found on the Committee's webpage http://www.icann.org/committees/nom-comm/ The author is a member of the 2004 Nominating Committee.

[47] The ccNSO webpage http://ccnso.icann.org/

Regional Internet Registries (RIRs)

American Registry for Internet Numbers (ARIN) responsible for the North American region;

Asia Pacific Network Information Centre (APNIC) responsible for the Asia Pacific region;

Latin American and Caribbean IP address Regional Registry (LACNIC) responsible for Latin American and Caribbean

Réseaux IP Européens Network Coordination Centre (RIPE NCC) responsible for Europe and the Middle East.

AFRINIC, is being formed to serve Africa. Africa currently receives IP addresses from RIPE NCC and ARIN.

All the RIRs are open, fee-based not-for profit membership organisations. And all develop policy through open, consensus based policy development processes. Any person may propose an issue during an open policy meeting. The policy development process and policy decisions are archived so that they are publicly accessible[48].

In the ICANN structure the RIRs form the Address Supporting Organisation (ASO) and provide the ICANN board with advice on global policy issues regarding the assignment of IP addresses. To date, very few global issues have been raised to the ICANN board, policies tend to be handled regionally. The final structure of the ASO is still being negotiated between ICANN and the RIRs. The RIRs recently established a new organisation, the Number Resource Organisation as a focal point for their activities (http://www.nro.org/)

ICANN is not perfect, but it offers many opportunities for developing nation stakeholders to participate and make a contribution. It is probably one most open of all new ICT policy making processes, yet has come in for the most criticism for not being open enough.

[48] A comparison of RIR policy processes is available from http://www.aso.icann.org/docs/rir-policy-matrix.html