

Internet Governance

DRAFT FOR DISCUSSION

Jovan Kurbalija and Don MacLean

September 2007



© 2007 International Institute for Sustainable Development (IISD)

Published by the International Institute for Sustainable Development

The International Institute for Sustainable Development contributes to sustainable development by advancing policy recommendations on international trade and investment, economic policy, climate change, measurement and assessment, and natural resources management. Through the Internet, we report on international negotiations and share knowledge gained through collaborative projects with global partners, resulting in more rigorous research, capacity building in developing countries and better dialogue between North and South.

IISD's vision is better living for all—sustainably. Its mission is to champion innovation, enabling societies to live sustainably. IISD is registered as a charitable organization in Canada and has 501(c)(3) status in the United States. IISD receives core operating support from the Government of Canada, provided through the Canadian International Development Agency (CIDA), the International Development Research Centre (IDRC) and Environment Canada; and from the Province of Manitoba. The institute receives project funding from numerous governments inside and outside Canada, United Nations agencies, foundations and the private sector.

International Institute for Sustainable Development
161 Portage Avenue East, 6th Floor
Winnipeg, Manitoba
Canada R3B 0Y4
Tel: +1 (204) 958-7700
Fax: +1 (204) 958-7710

E-mail: info@iisd.ca
Web site: <http://www.iisd.org/>

Internet Governance

By Jovan Kurbalija and Don MacLean
September 2007

Table of Contents

The World Summit on the Information Society: A Turning Point?	4
Acknowledging a role for governments in Internet governance	5
Establishing the principle of multi-stakeholder governance	6
Enlarging the vision of Internet governance	7
Success Factors	10
Preserving the global and integrated Internet	11
Promoting further development of the Internet	11
Preventing misuse and abuse on the Internet	11
Examples of successes in Internet governance	12
Problems	12
Decentralized vs. centralized structure of Internet governance	12
Basis of legitimacy of the Internet governance system	13
Technical vs. policy aspects of Internet governance	14
How to harmonize public and private interests on the Internet	14
How to anchor the Internet into existing political and legal geography	15
Risk of running society through software code	16
Crises and Internet governance	17
Strategies For Strengthening Internet Governance	17
Promotion of a holistic approach and prioritization	17
Make tacit technical solutions explicit policy principles	18
The principle of technological neutrality	19
Conclusion	19

The Internet's effect on our lives is pervasive. Over the past decade, the use of e-mail, the web, and blogs have become part of the daily routine of more than a billion Internet users, and the Internet has gradually become part of the vital infrastructure of global social, economic, cultural, and political life. Accordingly, it is not surprising that questions related to Internet governance have risen from relative obscurity to attract attention worldwide, particularly as a result of the debates that took place during the United Nations World Summit on the Information Society (WSIS) that was held in two phases, in Geneva (December 2003) and Tunisia (November 2005).

The World Summit on the Information Society: A Turning Point?

From the viewpoint of government policy-makers, researchers, civil society organizations, and businesses concerned with the relationship between information and communication technologies (ICTs) and the great issues of global development, WSIS was in some ways similar to the 1992 Rio de Janeiro Conference on Environment and Development.

Like the Earth Summit, WSIS elevated to the highest level of the international policy agenda a complex set of issues that had been discussed and debated in UN circles and other forums for the previous two decades. For the sustainable development community, the ground for Rio had been prepared by events such as the 1972 Stockholm Conference on Human Environment and the publication of *Our Common Future*, the 1987 report of the World Commission on Environment and Development (the Brundtland Report). In the case of WSIS, a similar role in preparing for the main event was played by the publication of *The Missing Link*, the 1984 report of the Independent Commission for World Wide Telecommunication Development (the Maitland Report) and a series of conferences that subsequently took place on the relationship between telecommunications, other ICTs, and development.

Like the Earth Summit, WSIS was a world gathering as well as an intergovernmental conference. Although there was some concern before the event that WSIS might be lightly attended—coming as it did in the wake of the dot-com crisis and a meltdown in the global telecommunications industry—175 governments and 12,000 delegates participated in the Geneva phase of the summit, while 174 governments and 19,000 delegates attended the Tunis phase. In spite of the downturn in the Internet and ICT industries, and the changes in the international environment that had occurred post 9/11, WSIS showed that a substantial global community remained interested in the issues on the conference agenda.

Like the Earth Summit, two of the main products of WSIS were a declaration and an agenda—the 2003 Geneva Declaration and the 2005 Tunis Agenda for the Information

Society.¹ However, unlike the Earth Summit, which adopted the Convention on Biological Diversity and the Framework Convention on Climate Change as well as the Rio Declaration and Agenda 21, WSIS did not produce any documents that constituted binding international agreements—although they may come in time².

From today's perspective, less than two years after the summit took place, it is too early to tell if over the next ten-twenty years WSIS will have consequences similar to those engendered by the Earth Summit by reshaping the global policy agenda in the areas it addressed. However, while its overall effect long term is not yet known, even this close the event it is reasonable to view WSIS as a watershed in the evolution of Internet governance.

Although the original purpose of WSIS was to substantially advance the role played by ICTs in helping to achieve the Millennium Development Goals and other internationally agreed development objectives, for the most part the summit simply consolidated and confirmed actions that were already underway. Internet governance is arguably the only area in which the summit broke new ground and where a number of significant decisions were made.

Acknowledging a role for governments in Internet governance

WSIS was the first time that a large number of governments representing both developing and developed countries from all regions of the world had attempted to agree on a comprehensive international framework for governing the Internet that included principles, objectives, priorities, and governance arrangements. The fact that the framework that emerged from WSIS was not binding does not necessarily diminish the significance of their efforts.

Unlike telecommunications and broadcasting, which traditionally had been subject to laws, regulations and other forms of government control applying specifically to these media at both the national and international levels, the Internet traditionally had been self-governing. On this basis, as WSIS recognized, the Internet had “evolved from a research and academic facility into a global facility available to the public” and had become “a central element of the infrastructure of the Information Society”—a development unprecedented in the 150-year history of electronic communications media.

In the honeymoon phase of rapid Internet growth that took place during the second half of the 1990s, it was widely believed that the Internet had created a borderless world in which the concept of national sovereignty was increasingly meaningless, a realm of cyberspace that was inherently beyond the control of national governments and intergovernmental institutions. This sentiment was most famously captured in John Perry Barlow's “Declaration of the Independence of Cyberspace,” which sent the following message to all governments: “You are not welcome among us. You have no sovereignty where we gather.

¹ The WSIS output documents are available at <http://www.itu.int/wsis>. Although each phase of the summit produced two output documents, the 2003 Geneva Declaration was largely reprised in the 2005 Tunis Commitment, while the essence of the 2003 Geneva Plan of Action was incorporated in the 2005 Tunis Agenda for the Information Society.

² The Internet Governance Project (IGP), a consortium of academic researchers, has proposed development of a framework convention on Internet governance similar in principle to the Framework Convention on Climate Change. See <http://www.internetgovernance.org/pdf/igp-fc.pdf>

You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders.”

While not fully sharing the views of cyber-enthusiasts, before WSIS the governments of developed countries generally believed the remarkable success of the Internet was due in large part to the fact that it had developed free of direct government regulation at either the national or international levels, and that the best way forward was to continue this policy. For various reasons, developing countries generally did not share this view and believed that some level of government regulation was needed at both national and international levels, if the Internet was to serve their needs as well as those of developed countries.

Given the opposing views on this fundamental question, it was by no means certain that WSIS would be able to agree on an Internet governance framework that affirmed the relevance of the principle of national sovereignty to Internet governance, and which included an active role for national governments and intergovernmental organizations. The fact that such a framework was agreed signalled that a shift in thinking had occurred, even if the results of this shift were not binding. Although the specific implications of this shift are not yet entirely clear, the following extracts from the Tunis Agenda give a general sense of its direction:

- “We reaffirm that the management of the Internet encompasses both technical and public policy issues and should involve all stakeholders and relevant intergovernmental and international organizations. In this respect, it is recognized that policy authority for Internet-related public policy issues is the sovereign right of States. They have rights and responsibilities for international Internet-related public policy issues.” (§ 35)
- “We recognize that all governments should have an equal role and responsibility for international Internet governance and for ensuring the stability, security and continuity of the Internet. We also recognize the need for development of public policy in consultation with all stakeholders.” (§ 68)

Establishing the principle of multi-stakeholder governance

Perhaps unusually for a UN summit, although the roles of national governments and intergovernmental organizations in Internet governance were hotly contested items in WSIS negotiations, the roles of the private sector and civil society were not—at least in principle.

Whatever their views about the extent to which they should or should not be involved in Internet governance, all of the governments participating in WSIS acknowledged the obvious—that the development of the Internet had been driven in the past, and would continue to be driven in the future, by the research and academic communities, the private sector, and civil society. They therefore decided that these stakeholders deserved to be treated as full partners in Internet governance institutions and processes.

As in the case of all UN summits, full participation in WSIS was limited to governments. However, in adopting the resolution that authorized the summit, the UN General Assembly

recommended the establishment of an open-ended preparatory process and invited not only governments, but also the private sector, non-governmental organizations and civil society to participate actively in this process. More significantly, the Internet governance framework adopted by WSIS was founded the principle that “the international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations.”³

The multi-stakeholder principle proved difficult to implement during WSIS negotiations. Nor is it yet clear what it means in practice—either in the new UN Internet Governance Forum that was established by WSIS, or in existing international organizations involved in aspects Internet governance, such as the International Telecommunication Union (ITU), the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO). However, it is generally believed by WSIS stakeholders that the summit’s adoption of multi-stakeholder engagement as a fundamental principle of Internet governance is an important innovation that may also be applicable in other areas of global governance, possibly including sustainable development.

Enlarging the vision of Internet governance

Prior to WSIS, Internet governance was generally considered as principally concerned with two things; standardization and other technical matters related to the design and operation of the Internet primarily handled by the Internet Engineering Task Force (IETF); and the management of two sets of resources that are central to the functioning of the Internet in its current form:

- Internet domain names, including generic top-level domain names (gTLDs) such as “.com,” country code top-level domain names (ccTLDs) such as “.uk,” and their respective lower-level derivatives;
- the numerical IP addresses that are assigned to computers and other devices connected to the Internet.

The WSIS debate on Internet governance was triggered by dissatisfaction, particularly among developing countries and civil society, with some aspects of the arrangements for managing Internet names and numbers that had been put in place by the United States Department of Commerce in the 1990s.

These arrangements had been developed with the aim of facilitating the transition of the Internet from a US-based academic and research network with a very limited number of users to a global communications medium, widely available to the general public, run mainly on a commercial basis that left it largely free from direct government control (with the potential exception of the United States government, which retained at least theoretical control over the management of key Internet resources through various contractual relationships).

³ Tunis Agenda for the Information Society, § 29

The concerns of those who were either uneasy with aspects of these arrangements or outright opposed to them centred on the fact that responsibility for managing Internet names and numbers had been transferred in 1998 to a private, not-for-profit corporation — the Internet Corporation for Assigned Names and Numbers (ICANN). Previously these responsibilities had been carried out by members of the Internet community on a largely informal basis.

Although ICANN was set up to operate as a globally decentralized organization with bodies in all regions of the world, and even though its structure included a Government Advisory Committee and mechanisms for representing the interests of civil society, the governments of a number of major developing countries and some other WSIS stakeholders strongly felt—albeit for very different reasons—that ICANN was the wrong model for managing core Internet resources at a time when the Internet was becoming a critical infrastructure for economic and social development in all countries.

From the point of view of some developing countries, this responsibility should have been entrusted to an intergovernmental organization, such as the ITU. From the point of view of civil society, a less commercial approach that was more respectful of the needs and rights of individual users would have been preferable. ICANN's status apart, the fact that the US government retained control over the operation of the root server system that enables the Internet to function by helping to map Internet domain name system onto IP addresses only added to these concerns.⁴

Although much of the debate about Internet governance in the early stages of WSIS centred on concerns related to the management of core Internet resources, a much broader vision of the scope of Internet governance evolved during the course of summit process.

The development of this broader vision was assisted by the report of the Working Group on Internet Governance that was set up to explore a number of key questions related to Internet governance between the first and second phases of the summit⁵. Largely on the basis of this report, the sections of the Tunis Agenda for the Information Society dealing with Internet governance include not only issues related to the management of core Internet resources, but also issues that had emerged in various forums in the decade before the summit took place. These issues, and some of the main forums in which they had been discussed, included:

- the development of the telecommunications infrastructure that underlies the Internet, particularly with respect to new mobile and broadband technologies, as well as the longstanding question of how to achieve universal and affordable access to this infrastructure in developing countries— *ITU and WTO*
- the structure of the global Internet service provider industry, particularly with respect to the prices charged to Internet service providers in developing countries for interconnection with global Internet backbone networks and the lack of regional Internet traffic exchange points

⁴ See Mueller, Milton L., *Ruling the Root: Internet Governance and the Taming of Cyberspace*, Cambridge MA, MIT Press, 2002, and Paré, Daniel, *Internet Governance in Transition: Who Is the Master of This Domain?* Lanham MD, Rowman and Littlefield, 2003 for detailed analyses of issues surrounding the management of Internet names and addresses

⁵ See <http://www.wgig.org> for the Final Report and Background Report of the Working Group on Internet Governance

- in some developing regions—*ITU, the Organization for Economic Cooperation and Development (OECD) and the Asia-Pacific Economic Cooperation (APEC) forum*
- the development of multilingual or internationalized domain names (IDNs), particularly in languages that use non-Roman scripts—*IETF, ICANN, ITU, UNESCO, and the Multilingual Internet Names Consortium (MINC)*
 - abuses of the Internet including
 - annoyances such as viruses, spyware and spam—which has a particularly devastating impact on Internet users in developing countries who typically pay high prices for very limited Internet access—*OECD, European Union (EU), ITU and multi-stakeholder arrangements such as the London Action Plan*
 - various forms of cybercrime such as phishing, other forms of online fraud—*OECD and ITU, as well as in the Council of Europe which developed a Convention on Cybercrime*
 - threats to the security of the Internet as critical infrastructure, including denial of service attacks—*IETF*
 - the impact of the Internet on
 - human rights, particularly as embodied in the Universal Declaration of Human Rights and with respect to issues such as freedom of expression and protection of privacy—*UNESCO and the Council of Europe*
 - competition policy and consumer rights—*ITU, WTO and OECD*
 - international trade—*OECD, WTO, the United Nations Conference on Trade and Development (UNCTAD), and the United Nations Commission on Trade-Related Law (UNCITRAL)*
 - intellectual property rights—*WTO and the World Intellectual Property Organization (WIPO), which adopted a set of “Internet treaties” in 1996, as well as in ICANN (particularly the relationship between trademarks and domain names) and various standardization fora including the IETF and ITU*

In addition to these specific issues, there had been considerable discussion in the decade prior to WSIS of the general the implications of the Internet for overall economic, social, and cultural development, particularly in developing countries, including issues related to

- the development of e-commerce, e-health, e-education and e-government
- the preservation of traditional knowledge, the development of content in local languages
- the building of technical, financial and policy capacities in all these areas.

These more general developmental issues were extensively discussed in multilateral agencies such as the World Bank, the United Nations Development Program (UNDP), the ITU, and UNESCO. In addition, they were the subject of multi-stakeholder initiatives by the Group of Eight (G8) countries and the UN ICT Task Force in the years immediately preceding the summit.

This “top-down” discussion of Internet-related issues in intergovernmental organizations was mirrored in a more bottom-up fashion by the Internet Society (ISOC), which was founded in 1992 to provide an, international, non-governmental organizational structure in which members of the Internet community could discuss issues related to standards, public policy and capacity-building.

Today, it seems fair to say that international debate about Internet governance has been transformed by two things: the larger vision of Internet governance developed by WSIS, which drew together all these different discussion threads; and the multi-stakeholder approach to Internet governance WSIS derived from this vision.

The WSIS vision and framework have the potential to re-shape Internet and ICT-related policies, strategies and governance arrangements at both the international and national levels. In this sense, the vision of Internet governance developed through the WSIS process may play a role in the future evolution of Internet policy similar to the role that has already been played in the evolution of global development policy by the vision of environmentally, economically and socially sustainable development crystallized at the Rio summit.

Whatever the apparent similarities between the vision of Internet governance adopted by WSIS and the vision of sustainable development adopted at the Earth Summit—in terms of their comprehensive nature and potential role in transforming policy and governance internationally and nationally—the fact remains that there is at present relatively little contact between the Internet governance and sustainable development communities. David Souter, the author of one of the other papers in this collection, has demonstrated in a recently published study that, in spite of the large number of people who took part in the two phases of WSIS, only a relatively small portion came from the sustainable development community. Although its avowed goal was to link the transformative power of the Internet and other ICTs to the achievement of the MDGs and other internationally agreed development goals, WSIS was primarily an internal event, by and for the Internet and ICT community.⁶

The main purpose of this paper, as part of a larger project to help bridge the gaps that currently exist between the Internet governance and sustainable development communities, is to give a sense of the scope of Internet governance in terms of issues, institutions and processes, as well as the key challenges moving forward. As we shall see from the sections that follow, the complex web of Internet governance activities sketched out above will continue to develop along various evolutionary paths, many of which are likely to be of interest to the sustainable development community, whether or not WSIS was indeed a turning point.

Success Factors

As the previous section has attempted to demonstrate, Internet governance is very diverse. It is not one system, and this makes it difficult to make one evaluation of overall Internet governance. It is far easier to focus on specific fields, such as Internet names and numbers, intellectual property, and data protection. For an overall evaluation of Internet governance, the following factors could be used:

- preserving the global and integrated Internet (avoid risk of fragmentation)
- promoting further development of the Internet

⁶ See Souter, David, “The World Summit on the Information Society: the end of an era or the start of something new?”, Association for Progressive Communications, 2007 *Information Society Watch*, available at <http://www.globaliswatch.org>.

- preventing misuse and abuse on the Internet.

Preserving the global and integrated Internet (avoid risk of fragmentation)

One of the main advantages of the Internet is its global nature. Once connected to the Internet, any user can access any website on the Internet. In some cases, this possibility has been gradually reduced through various filtering and content control mechanisms. For example, users in China and many Islamic countries cannot access certain websites whose content is declared unacceptable by national authorities. More recently, the governments of Turkey and Thailand have filtered access to YouTube because it was hosting material that insulted Kemal Ataturk in the case of Turkey, and the King in the case of Thailand. While filtering restricts access to the website, it is still a corrective mechanism to an otherwise unified and global Internet.

In the case of possible fragmentation of the Internet, there will be separate Internets established on national or regional bases. The main risk for such a development is dissatisfaction of some national governments with the current ICANN-driven system. Hypothetically, fragmentation could lead towards creation of national root servers, which is technically feasible and relatively simple to implement. However, economic and social consequences of fragmentation of the Internet along national borders could be far reaching. Such development could be avoided by having an Internet governance system that accommodates the interests of various actors, in particular those of national states. If actors are satisfied with the ways in which their policy interests are met, they will not have any particular reason to establish alternative Internets. So far, Internet governance has been highly successful in this respect.

Promoting further development of the Internet

Internet governance has contributed to the fast development of the Internet in two directions. First, the number of Internet users has increased substantially. With the exception of a few countries, it is difficult to find any part of the world without access to the Internet. Currently, the number of users is more than one billion, with a continuous and rapid increase. Second, due to its architecture of “end-to-end networking,” the Internet has fostered creativity and fast development of various applications. Skype, Wiki, and YouTube are the latest examples of creative solutions that have developed into successful business modules. One of the main challenges for future Internet governance is to preserve and further develop an architecture that facilitates growth of the Internet.

Preventing misuse and abuse on the Internet

This is possibly the field where Internet governance has not been particularly successful. The more the Internet has developed, the more it has been exposed to misuses and abuses. The

decentralized structure of the Internet, which is considered as its strength, can easily become a weakness if cyber-criminals and terrorists use it. The lack of central authority allowed creativity on the Internet, but it can also hamper law and order. The fight against cybercrime and SPAM are a few examples where success has been limited.

Examples of successes in Internet governance

Proactive action towards the risk of shortage of IP numbers

The response of the Internet technical community to the problem of a potential shortage of IP numbers is an example of prompt and proactive governance. The concern that IP numbers might run out and eventually inhibit the further development of the Internet led the technical community to take two major actions. The first was the rationalization of the use of the existing pool of IP numbers.¹ The second action was the introduction of IPv6 (a new version of the TCP/IP protocol), which provided a much bigger pool of IP numbers, namely (430,000,000,000,000,000,000).¹ The reaction of the Internet technical community could be described—in environmental governance parlance—as a “precautionary principle.”

Cybersquatting – Uniform Domain-Name Dispute-Resolution Policy (UDRP)

The Universal Domain Name Dispute Resolution Policy (UDRP) is an example of a fast, efficient, and multi-stakeholder reaction to problems in Internet governance. The UDRP was developed in order to curb cybersquatting—the practice of registering names of companies, usually protected by trademark, and selling them later at a higher price. The UDRP was developed by WIPO and implemented by ICANN as the main dispute resolution procedure in the field of domain names. Since then, cybersquatting has significantly reduced.

Problems

In spite of its success, Internet governance has already encountered numerous problems and challenges. New problems will come with new developments of the Internet. Who was able to predict in the 1990s that SPAM would become one of the major Internet problems? While it will be difficult to anticipate, it is essential to develop mechanisms that will be flexible enough to deal with new problems. Most problems of Internet governance were already discussed earlier; here, we will focus on a few structural problems likely to influence the future development of Internet governance.

Decentralized vs. centralized structure of Internet governance

According to the decentralized view, the current governance structure reflects the very nature of the Internet: a network of networks. Such a complex setup cannot be placed under

a single governance umbrella, such as an international organization. It includes interplay among different layers (global, regional, national, and local) as well as among different types of governance (inter-governmental, professional, and communal).

The decentralized and versatile governance structure has been the strength of the Internet and one of the main reasons for its growth. No central authority could have controlled or stopped innovation on the Internet. The decentralized approach is strongly supported by the Internet community and the developed countries.

However, a traditional Internet governance scheme poses certain challenges. First, it is difficult to coordinate such a variety of institutional and professional mechanisms. The lack of coordination could lead to duplication of efforts, and to failure to cover all issues and possible misunderstandings. It can also lead to fragmentation and, in the most negative scenario, balkanization of Internet governance. Second, it is particularly difficult for countries with limited human and financial resources to follow Internet governance discussions in a highly decentralized and multi-institutional setting. Such countries find it difficult to attend meetings in the main diplomatic centres (Geneva, New York), let alone to follow the activities of other institutions, such as ICANN, W3C, and IETF. These developing countries argue for “one-stop shopping,” preferably within the framework of an international organization.

Basis of legitimacy of the Internet governance system

One of the fundamental issues is the basis of global Internet governance. In the inter-governmental segments such as intellectual property, it is clear. A usual line of decision-making and implementation is followed. Governments sign international treaties and undertake international duties. Governments implement internationally adopted rules through national legislation. Similar situations occur in the field of human rights, taxation, and customer protection.

The main challenge is in the ICANN-related sector of managing Internet infrastructure. Traditionally, the main constituency was the Internet community, consisting mainly of technologists and other people involved in development and management of the Internet. While it was an acceptable approach with a limited number of Internet users, it is increasingly difficult to justify a predominant position of the Internet community in the Internet world of one billion users. Can their pioneering role in development of the Internet justify a privileged role in Internet governance? How might we articulate the interests of those billion-plus users of the Internet? Should it be done through governments as a regular channel for democratic representation? If yes, should we be led towards a more prominent role of governments in managing Internet infrastructure? Those are some questions that have been reoccurring in the Internet governance debate. The answer to those questions will be needed in order to create a stable Internet governance system and to avoid ambiguities and possible confusion.

Technical vs. policy aspects of Internet governance

Technical solutions are not neutral. Ultimately, each technical solution or option promotes certain interests, empowers certain groups and, to various extents, effects social, political, and economic life. Internet governance issues usually involve technical and policy aspects. One of the main problems in Internet governance has been how to draw a clear distinction between technical and policy aspects.⁷

The dichotomy between technical and policy management was mainly present in discussions on ICANN's activities. While ICANN has been trying to portray itself as the organization that deals with technical issues, the critics have stressed that there are no technically neutral solutions. However, the idea of techno-neutral management has been constantly reoccurring in the ICANN-related debate. It also inspired the *Economist*, which argued that ICANN “should rethink its mission and cut down as much as possible to the technical aspects of running the domain-name system, leaving more political issues to other organizations. ICANN would then stand a much better chance of becoming a model for consensus-based self-regulation.”⁸ The recent debate over the introduction of the “xxx” domain clearly showed that ICANN will more often deal with policy than pure technical decisions.⁹ Instead of basing its position on an indefensible point of “pure technical organization” ICANN should be reformed in order to handle policy aspects, as it had to do in the “xxx” case. Without clearly articulated and designed process policy, decisions could be influenced through informal lobbying and pressure on ICANN. Dealing with policy aspects will need a different organization with a stronger role of governments and a broader legitimacy base.

How to harmonize public and private interests on the Internet

One of the main strengths of the Internet is its public nature, which enabled its rapid growth and fostered creativity and inclusiveness. How to protect the public nature of the Internet will remain one of the core issues of the Internet governance debate. Likewise, how to strike the proper balance between private and public interests in Internet governance will continue to be at the forefront of discussion. The question of public and private interests emerges in discussion of any Internet governance issue, whether infrastructure, content, access, or intellectual property. In each of the specific issues, the public-private debate has a specific focus.

⁷ Karl Auerbach made the following distinction between governance and technical issues, “If you can make a wrong decision about the thing and that causes the Internet to fail in delivering its fundamental service, then it is a technical matter.”

⁸ Available at: http://www.economist.com/research/articlesBySubjectdisplayStory.cfm?story_ID=1011796&subjectid=348963.

⁹ The “xxx” domain was supposed to be a “sex zone” on the Internet. Proponents of the introduction of the “xxx” domain argued that this domain would reduce the risk of children accessing this type of materials. Others were against the introduction of the “exxx” domain based on various religious and cultural grounds. After long debate, the Board of ICANN rejected the “xxx” domain proposal in March 2007. The main criticism of this decision was that it was made under pressure of the US government, which strongly opposed the introduction of the “xxx” domain. Interestingly, the US government was supported by many other governments, including those who are usually against the US’ predominant position in ICANN system, such as Brazil and China.

In the US, priority has been always given to the protection of private interests as the engine for business growth. For example, when Morse, one of the inventors of the telegraph, offered to sell his invention to the US government, Congress declined the offer based on its interpretation that the Constitution limited government involvement in commercial affairs. Consequently, the network of telegraph lines was financed by the private sector. The same approach applied to the development of the telephone, radio, and television. It continued with the Internet. The first principle of the *White Paper on Internet Governance* (1997), which is considered the founding document of ICANN, is that “the private sector should lead.”

Unlike the US, in other countries telecommunication infrastructure has often been developed and owned by government organisations, such as the post-telegraph-telephone. This underlying conceptual and historical difference between the US and other countries has influenced the Internet governance debate on the relationship between public and private interests.

How to anchor the Internet into existing political and legal geography

As mentioned previously, one of the early assumptions regarding the Internet was that it overcame national borders and eroded the principle of sovereignty. John Perry Barlow’s previously cited “Declaration of the Independence of Cyberspace” is an example of the predominant techno-optimism typical of the mid-90s. It was inspired by the notion that the Internet would cut the link between geography (where we live) and the political and legal systems governing our social reality.

Since Barlow’s declaration, there have been many developments, including more sophisticated geo-location software. Today, it is still difficult to identify exactly who is behind the screen, but it is fairly straightforward to identify through which Internet service provider (ISP) the Internet was accessed. In addition, the latest national laws around the world require ISPs to identify their users and, if requested, to provide necessary information about them to authorities.

Most international court cases reflect this tension between cyber and real space. It includes a considerable number of court cases starting from the CompuServe case (1996) when a German court prohibited access to pornographic materials, even if the websites were located outside of Germany. In 2001, the Yahoo case brought the question of cyber and real space in sharper focus. A French court requested the US-based company Yahoo to prevent access to Nazi materials to French Internet users. While in the CompuServe case, the solution was found in restriction to all users, in the Yahoo case, technology helped to introduce a more sophisticated filtering by using geo-location software.

The more the Internet is anchored in geography, the less unique its governance will be. For example, with the possibility to locate Internet users and transactions geographically, the complex question of jurisdiction on the Internet can be solved more easily through existing laws.

Risk of running society through software code

One significant aspect of the relationship between technology and policy was identified by Lawrence Lessig, who observed that with its growing reliance on the Internet, modern society may end up being regulated by software code instead of law.¹⁰ Some legislative functions of parliament and government could *de facto* be taken over by computer programmers and technical developers. Through a combination of software and technical solutions, they would be able to influence life in increasingly Internet-based societies. Should the running of society through code instead of laws ever happen, it would substantially challenge the very basis of the political and legal organization of modern society.

DRAFT

¹⁰ Lawrence Lessig, *Code and Other Laws of Cyberspace* (1999).

Crises and Internet governance

One of the main features of the Internet is its robustness and stability. Since the Internet was created in order to survive a nuclear attack, the complete failure of the Internet is very unlikely to happen. Although there have been many warnings of possible cyber-terrorist attacks, none have been recorded. The robustness of the Internet has been proven in a few recent global crises. While the telephone system collapsed during the 9/11 attack, the Internet functioned. Similarly, after the terrorist attack in London (2004) the Internet was the most reliable communication medium.

The doom/crisis argument was used in early WSIS negotiations on Internet governance when some argued that the failure of the root server could lead to a collapse of the Internet. Initially it captured the imagination of a few delegates and provided an argument that such an important system must be put into the hands of the UN or some other public authority. The misperception of an Internet-doom scenario was addressed quickly and debate on Internet governance became more informed and substantial. The WGIG made one of the main contributions to awareness building and learning on Internet governance.

While it is unrealistic to have the collapse of the Internet or a major Internet crisis, the Internet may be affected by other security and political crises. For example, a “9/11” influenced adoption of anti-terrorist laws in the US (Patriot Acts) introduced broad and lawful surveillance of Internet communication. The main justification for increasing surveillance is the use of the Internet as the main communication medium for the preparation of “9/11” and other terrorist attacks. The Internet is also employed by terrorist organisations for planning, recruitment, fund-raising, and delivering manuals for preparing terrorist activities. The side-effect of increased surveillance of the Internet could be the endangerment of the delicate balance between the need to protect national security and civil liberties.

According to current global trends, it is reasonable to expect future terrorist attacks and other security threats. In such a context of increasing security threats, it will be important to design response mechanisms and regulations to avoid adoption of *ad hoc* solutions. The precautionary approach would involve the adoption of international legal instruments and the establishment of necessary institutional mechanisms on the global level.

Strategies for Strengthening Internet Governance

Promotion of a holistic approach and prioritization

A holistic approach should facilitate addressing not only the technical, but also the legal, social, economic, and developmental aspects of Internet governance. This approach should also take into consideration the increasing convergence of digital technologies, including the

migration of telecommunication services towards Internet protocols. The holistic approach to Internet governance was adopted by the WSIS and it is in the basis of the Internet Governance Forum.

While maintaining a holistic approach to Internet governance negotiations, stakeholders should identify priority issues depending on their particular interests. Neither developing nor developed countries are homogenous groups. Among developing countries there are considerable differences in priorities, level of development, and IT readiness (e.g., between ICT-advanced countries such as India, China, and Brazil, and some least-developed countries in sub-Saharan Africa). On the national level, considerable diversity of position and views is apparent. In the US, it was particularly noticeable in the recent debate on Net neutrality, where the main companies of the “Internet economy” (Google, Yahoo) argued for preserving neutrality of the Internet (not discriminating different traffic on the Internet) while telecommunication and entertainment companies argued for different “Internets.” They argued for providing special facilities for distribution of video and other multimedia materials. In this debate, many developing countries are strong supporters of net neutrality because any differentiation of the Internet would leave them with inferior services.

A holistic approach and prioritization of the Internet governance agenda should help stakeholders from both developed and developing countries to focus on a particular set of issues. This should lead towards more substantive and, possibly, less politicized negotiations. The stakeholders would group around issues, rather than around the traditional highly politicized division-lines (e.g., developed vs. developing countries, governments vs. civil society).

Make tacit technical solutions explicit policy principles

It is a common view that certain social values, such as free communication, are facilitated by the way the Internet is designed technically (the “end to end” principle). However, this is not necessarily correct. The latest developments in the Internet, such as the use of firewall technologies for restricting the flow of information, prove that technology can be used in many, seemingly contradictory, ways. Principles such as free communication¹¹ should be clearly stated at the policy level, not tacitly presumed at the technical level. This does not mean that certain technological solutions cannot contribute to the promotion of certain values, as has been the case with Internet infrastructure (openness, creativity, inclusiveness).¹²

¹¹ For discussion on Internet architecture and freedom of expression, consult Julien Mailland, Note, Freedom of Speech, the Internet, and the Costs of Control: The French Example, 33 N.Y.U. J. INT'L L. & POL. 1179, 1198 (2001)

¹² Many studies argue that the growth of the Internet and promotion of certain values (free flow of information, decentralization, creativity) was facilitated by the Internet infrastructure. Some of those sources include:

- Lawrence Lessig, *The Future of Ideas: the Fate of the Commons in a Connected World* 5–23 (Random House 2001);
- Michael L. Dertouzos, *What Will Be: How the New World of Information Will Change Our Lives* (HarperEdge 1998);
- Manuel Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (Oxford University Press 2001);
- Michael Hauben & Ronda Hauben, *Netizens: On the History and Impact of UseNet and the Internet* (IEEE Computer Society Press 1997).

The principle of technological neutrality

According to technological neutrality, policy should not depend on specific technological or technical devices. For example, regulations for the protection of privacy should specify what should be protected (e.g., personal data, health records), not how it should be protected (e.g., access to databases, crypto-protection).

Technological neutrality provides many governance advantages. First, it de-links governance from any particular technology and makes it ready for future technological developments. Second, technological neutrality is the most appropriate regulatory principle for the future convergence of the main technologies (telecommunication, media, Internet).

The EU has introduced technological neutrality as one of the cornerstones of its telecommunications policy. While technological neutrality is clearly an appropriate principle, one can envisage many difficulties in the transition from existing telecommunication regulations to new ones. This is already obvious in areas such as Voice over IP.

Conclusion

The Internet and the entire Internet technology revolution is ultimately based on 1s and 0s. Everything we experience online has its roots in 1s and 0s. These two digits have had such an impact on society that they can be included with other major breakthroughs in the history of mankind, including fire and the wheel. They have deeply influenced social, political, and economic life.

Paradoxically, the world created by them cannot be managed by binary logic and dichotomous approaches of either/or, good/bad, progressive/regressive, open/closed, us/them. The governance of the Internet requires an appreciation of different perspectives, various approaches, subtle differences, and managing paradoxes. It has to be analogue.

The need for a careful balancing act can be found in almost any Internet governance issue. This does not make Internet governance a simple and easy governance solution. It is most likely that future Internet governance will require a difficult interplay of international and national, public and private, democratic and expert, open and efficient elements.