



Experts Group on Internet Governance
Project of the Fundación Telefónica – Polytechnic University of Madrid

Internet Governance and Sustainability: Proposal of Subjects for the Debate

Contribution to the IGF Conference in Athens 2006

31st of July, 2006

AUTHORS:

Governance Experts Group

(Coordinator: Dr. Jorge Pérez)

CONTACT

Dr. Sergio Ramos (assistant coordinator)

e-mail: sramos@gtic.ssr.upm.es

Tel./Fax: +34 91 336 73 20

Mobile phone: +34 647 77 62 50

ADDRESS

ETSI Telecommunications – Polytechnic University of
Madrid

Despacho C-431

28040 Madrid

Spain

INDEX

INTRODUCTION	3
PRELIMINARY ANALYSIS WITHIN THE CONTEXT OF THE IGF CONFERENCE IN ATHENS 2006: GOVERNANCE AND SUSTAINABILITY	5
PROPOSALS FOR THE SUSTAINABILITY AND GOVERNANCE DEBATE	7
NETWORK NEUTRALITY	7
<i>Groups and Positions</i>	8
<i>Issues for Analysis</i>	9
SECURITY, PRIVACY AND TRUST ON THE INTERNET	10
<i>Groups and Positions</i>	10
<i>Issues for Analysis</i>	13
DIGITAL GAP	14
<i>Groups and Positions</i>	15
<i>Issues for Analysis</i>	16
CONCLUSIONS	17
REFERENCES	18

INTRODUCTION

The management and control of the Internet is a subject that has led to a major worldwide debate since the Net became one of the most important economic, political and social phenomena of the last decade.

As regards the role of ICT as one of the pillars of the Information Society, where the Internet is a key element, and further assuming that the use of ICT promotes the development and improvement of the social practices and interactions in relation to infrastructures, transactions and the international exchange of information, the debate is focused on the need to determine the limits for the autonomy of the different nations and the level of participation of the different agents, not only in the management of technical resources of the Internet, but also as regards other issues, for example, the distribution of the responsibilities to defray and correct the costs of the digital gap between rich and poor regions, the security of the Internet and other communications networks, digital piracy or the illegal distribution of multimedia contents.

Therefore, we are talking about a new regulatory paradigm known as Internet governance which was defined in the last World Summit on the Information Society, held in Tunis in November 2005:

“Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet”

Among the conclusions of the Summit we can highlight the consensus reached on the expansion of the participation of all groups responsible for the development of the Internet in the governance process initiated, with the purpose of advancing in a common direction, based on dialogue and with the collaboration of the academic and research community in this area. As a result of this agreement, the United Nations¹ created the Internet Governance Forum, which will celebrate its first conference in Athens in October – November 2006².

At the same time, it acknowledged the need for each nation to design its own public policies, in accordance with the national and territorial identity criteria, as regards their own culture, language and respect for the liberties of each individual, always in tune with the international agreements.

Within this context, and thanks to the encouragement of Fundación Telefónica and the collaboration with the Polytechnic University of Madrid, an Experts Group on Internet Governance was recently created in Spain, with the purpose of identifying the

¹ We can highlight the words of the Secretary General of the United Nations: “...*But I think you also all acknowledge the need for more international participation in discussions of Internet governance issues. The question is how to achieve this. So let those discussions continue...*”

² See <http://www.igfgreece2006.gr/>

role of the Spanish ICT sector and its public administration, R+D organisations and the civil society in the development of the Internet and its governance practices in Spain and Latin America. All in all, their aim is to show the relevance of these issues in Spain and the need to address them between all interested groups and parties, with their active contribution to the development of the governance practices at the national and international level.

The said Group was appointed with the purpose of creating an opinion and debate forum that could provide expert knowledge for the evolution and development of the Internet and other information networks, participating and influencing the national and international decision forums on the said governance practices. The Group is composed of professionals from different areas, who carry out their professional activity directly or indirectly within the telecommunications, Internet and Information Society sector, as well as in the public and social policy area. Therefore, the main aim is to allow the different projects created by the group to integrate the different perspectives of participants, offering and integrating a group vision on the subjects addressed.

Thus, this document is an important contribution to the conference of the Internet Governance Forum which will be celebrated in Athens in from October 2006, with the purpose of participating in the debate and promoting the discussion of additional issues which are considered by the Group as vital and relevant for the development of the governance of the Internet and other information networks.

PRELIMINARY ANALYSIS WITHIN THE CONTEXT OF THE IGF CONFERENCE IN ATHENS 2006: GOVERNANCE AND SUSTAINABILITY

An initial assessment has been made with the contributions of the conference in Athens, evaluating the level of interest of the different groups in specific issues related to the Internet and its development, with a particular focus on the Spanish context, so that a set of horizontal subjects can be extracted to facilitate the participation of the groups involved in the Internet governance process.

GROUP	AGENTS	AVAILABILITY	SAFETY	DIVERSITY	ACCESS	SUSTAINABILITY
PUBLIC SECTOR	SETSI	XXX	XXX	XXX	XXX	XXX
	CMT	X	XX	X	XXX	XX
	Red.es	XXX	XXX	XXX	XXX	XXX
	Operators (Telefónica, Vodafone, Jazztel, Ono, ...)	X	XXX	X	XXX	XXX
PRIVATE SECTOR	ISP (Google, Yahoo, ...)	XX	XXX	XX	XXX	X
	Manufacturers (Lucent-Alcatel, Nokia, Ericsson, Siemens, ...)	X	XXX	X	XXX	XX
	AETIC	XX	XXX	XX	XXX	XXX
R+D	Universities	XXX	XXX	XXX	XXX	XXX
	Foundations	XXX	XXX	XXX	XXX	XXX
	Institutes	XXX	XXX	XXX	XXX	XXX
NGO's	User Associations	XXX	XXX	XXX	XX	X
	Consumer Associations	XXX	XXX	XXX	XX	X

Map of agents in Spain

Source: own elaboration

X – low; XX – medium; XXX – high

The table shows a list of the Spanish agents with the assessment of their initial interest in the different generic issues that will articulate the conference of the Internet Governance Forum in Athens. These issues (**openness, security, diversity and access**) also include a vital element which must be included in the debate (as described in the next few sections): **sustainability**.

- **Openness**. Openness is defined as the quality of the Internet as the driving agent behind democratic participation, i.e., an open environment for everyone and everything, with no control or censorship.
- **Security**. Security is defined as the basic feature for the exchange and use of information through the Internet and its economic (i.e., e-commerce), political (i.e., protection of copyrights, intellectual property, cyber-crime) and social (i.e., consumer and user protection) implications.
- **Diversity**. Diversity is directly linked to the concept of openness, since we can consider it in the Internet environment as a synonym for pluralism, whereby the need for the respect of the opinion of others and equality of all groups is clear, especially as regards the integration of minorities and local groups.
- **Access**. Access represents the capability to connect to the Internet, through any system; in any location.

Thus, with the information included in the table, we can state that, from the general point of view of all issues linked to security and access, almost all elements are vital for practically all Spanish agents. Both the openness and diversity characteristics seem to represent a secondary level of importance. However, these are fundamental elements for the public sector and civil society.

These issues are very important but none of them include highly relevant factors when promoting specific measures or adopting a determined position. We are talking about the economic, political and social implications of any action, defined as **sustainability**.

In any case, all initiatives must be aimed at reaching the adequate balance between the economic requirements, political objectives and social impact generated, evaluating and promoting sustainable and durable actions, so that these are not materialised as a mere punctual momentum but rather as a long-term contribution.

After analysing the evolution of the governance debate in the World Summit of the Information Society, as well as other related international initiatives, the Experts Group on Internet Governance stated that the criteria set forth are not generally displayed in clear terms in the different proposals presented, leaving the analysis of the economic, political and social feasibility and sustainability on one side.

Therefore, we believe that we must include the sustainability concept in the framework of the IGF Conference in Athens to stimulate the present and future debate on the development of the governance of the Internet.

PROPOSALS FOR THE SUSTAINABILITY AND GOVERNANCE DEBATE

Given the need to address issues that lead to the creation of sustainability proposals and results as one of the main elements in the governance of any aspect of the Internet, the initial subjects respond to two basic criteria: horizontality (in other words, the participation of all groups is vital since all are directly involved) and sustainability.

With this focus, three horizontal subjects have been chosen to be included in the conference in Athens, in order to provide the necessary answer to their economic sustainability:

- Network neutrality.
- Safety, privacy and confidence on the Internet.
- Digital gap.

NETWORK NEUTRALITY

A preliminary definition of “network neutrality” talks about the principle by which all Internet traffic must be treated equally, regardless of its contents and the sender and receiver.

The importance of the debate on neutrality lies on the approach of two different concepts about the structure of the Internet: first, a truly neutral network, as it was initially conceived or, on the contrary, a privatised network that must meet the new requirements, as a result of the social, technological and commercial development.

Internet was designed as a neutral structure, with an end-to-end architecture. It was thus designed as a simple network that could be used in the future to develop applications with the sole condition of using the IP protocol.

The network neutrality guarantees that all information flows are treated under the same conditions with no sort of discrimination and, therefore, a network that can process traffic under these conditions should not be capable of censoring or exerting an uneven competition pressure on the information transported³. This would guarantee the freedom of speech to any Internet user, since there is no censorship and there are no traffic modelling characteristics exerted by any organisation or company and the user would access the information directly. Therefore, this is a perfect design to maintain the freedom to access any sort of information which allows Internet users to have freedom of speech. However, this does not mean that a neutral network architecture must be discriminatory. All in all, one of the initial factors for the success of the development of the Internet (its neutrality) is now being questioned, since there are many doubts on whether it will be capable of facing the current and present challenges or not⁴:

³ See (Wu, 2003)

⁴ See (Comín, 2006)

- Provide safety to unfriendly conducts.
- Guarantee the quality of new applications.

The problem lies on satisfying the demands imposed by the new reality, whereby the Internet requires penetrating the network itself, thus entering a determined degree of intelligence that can control the packets being transported, that is, stopping them (for safety reasons) or giving them a higher level of priority (for business reasons).

GROUPS AND POSITIONS

As in the case of all aspects related to the governance of the Internet, there are also different opinions about the convenience of adopting an architecture that respects the neutrality of the Internet as a legal principle, and not as a *de facto* standard, as has been the case since its conception.

From the general point of view, the debate must be focused on the private sector, with clear antagonistic positions between Internet service providers and telecommunications operators. However, the development of this network neutrality project must be understood as a subject that affects all groups and due to its global character it must be treated as a priority in the Internet governance model described herein.

The main positions of the agent groups involved in the governance of the Internet and network neutrality discussion are described next:

- ***Public Sector.*** Conceptually, there are no clear arguments for or against any position, since, in theory, any of the options proposed should satisfy the public objectives. The integration of the expansive reality of the Internet within a regulated framework which was not carried out during its initial implementation and that exceeds the limits of its control due to its technological dynamism and that of its markets, is one of the main concerns of the regulating agencies in most countries, in particular, the Federal Communications Commission⁵ (FCC) in the United States. In fact, the proposal of the FCC for the regulation of the start of the *net neutrality* principle is in the middle of the debate, a characteristic which was yet to be established as a *de facto* element of the Internet⁶ and is now a reality.
- ***Private Sector.*** Most of the friction between agents is in the private sector, since there are diverse economic and business implications. Therefore, there is a large rivalry between the companies of Internet services and telecommunications operators (wideband access providers), for the ***final control of the client.***

⁵ See (FCC, 2005)

⁶ Currently, the North American regulation body has defended the network neutrality principle. Nonetheless, it has not formalised it in regulatory terms. In February 2004, its former president, Michael Powell, explained the organisation's policy on the freedom of the Net. During his speech at the University of Colorado (USA), he defined the Internet as a right of consumers to have a quadruple freedom: access to contents, use of applications, connection to any device and reception of information with a connection to the Net.

- **R+D.** The R+D group represents the scholars and researchers who participated in the management of the Internet and those who have collaborated directly in its evolution and development. The main opinion is to maintain the traditional architecture as a key element to promote continuous innovation, without prejudice to the exploration of other options due to the incredibly fast technological innovation and evolution of businesses on the Internet.
- **Civil Society.** Many associations and NGO's have shown their interest in achieving the neutrality of the Internet while respecting the rights of individuals, since these qualities have made the Internet a public space for creativity and innovation, as it is now. This is the tightest group which can exert its pressure on the power and control nuclei although its initiatives are sometimes unclear.

Given the aforesaid positions, the main issue deals with the evaluation of the suitability to promote a specific type of legislation for the neutrality of the network or whether the said suitability must be subject to the Internet governance activities.

With the previous analysis of the agents involved in the process, it would be logical to think that the said regulatory framework should not be created by the organisations in charge of the management of infrastructures and technical resources, since these are in charge of the supervision of the compliance with the pre-established standards. Therefore, the initiative of regulating the network neutrality legislation should be dealt by all other groups.

This issue comes into conflict with the national sovereignty scenario, since the vast complexity of these matters could lead to major changes in the economy and the businesses in the ICT and Internet sector. A potential scenario could be the adoption in favour of a country's own regulatory framework (*de facto* agreement vs. *de iure* regulations) that could come into conflict with a specific international position.

ISSUES FOR ANALYSIS

What would be the outcomes of a change towards the neutrality of the network? Initially, a move towards the neutrality of the network would lead to a drastic change in the telecommunications business and service marketing models, leading to many doubts about the sustainability of this change, particularly when having to face the continuous need to invest in order to guarantee the future development of new generation networks.

At the same time, we must know whether the change in the network neutrality principle could lead to the modification of the individual and group liberties in the Internet or not.

As regards the regulation of the network neutrality, the challenge lies on the compatibility of the neutral and decentralised essence of the Internet, which has enabled its development and has allowed it to deploy its high capacity wideband networks that require an investment that can only be addressed within the adequate profitability scenario.

Therefore, in the network neutrality and Internet governance area, the following issues must be addressed:

- Define the different scenarios that could be configured due to a change in the network neutrality principle, from the economic, political and social point of view.
- Evaluate the role of the groups involved in the adoption of the different scenarios presented.
- Propose a future scenario that guarantees the sustainability of the telecommunications and Internet business.
- Assess the network neutrality implications for the regulation of electronic communications and the Internet and the capacity of the different groups to have an effect on the adoption of a specific international model.

SECURITY, PRIVACY AND TRUST ON THE INTERNET

Internet offers many opportunities for the progress of social, economic and political objectives, becoming an alternative space for the physical world, where different parties can market and offer contents, services and goods.

The Internet is a complex environment, which is also heterogeneous and constantly changing, where no traditional authority models can be applied. Power is distributed amongst different sectors of activity, although none can control the distribution of the said power. Each network within the set of interconnected networks is in charge of its small section, all of which can be considered as sections which are owned by various agents and all collaborate to achieve a common set of rules and standards.

Within this context it is hard to identify the parties which should lead the implementation of measures that will guarantee the security of the Internet, since there is no party which is legitimised to manage the development of the Net. These challenges mean that it is hard to establish responsibilities and directives, and they are presented from different points of view: legal, social, technological, political and cultural⁷.

The implementation of security in the Internet is a very complex task which requires the simultaneous start-up of different level strategies, with the participation of different agents. This type of coordination is required to attain a safe network with a common dialogue between the major players in each sector.

GROUPS AND POSITIONS

The main positions of the agents involved in the governance of the Internet and the security of the Net are described next:

- **Public Sector.** The public sector has a keen interest for guaranteeing the security of the net. Internet users have to face the information technology problems related to security, such as viruses, and other social problems, such as fraud or Internet theft. However, many of the users are not aware of the problems they have to face.

Thus, some issues must be addressed, such as the development of the eGovernment,

⁷ See (Miller, G. et.al., 1999)

which requires users who trust the use of network applications. Similarly, within the context of the New Economy, the development of electronic commerce and growth of companies through the Internet is vital. Trust is one of the fundamental characteristics required to promote the use of ICT and the Internet. With the development of electronic services and business operations through the Net, the safety of the information and trust on the said applications have become key requirements for the development of a successful business. The challenge for public authorities deals with the creation of an environment that promotes the safety required, without the imposition of excessively strict conditions or very high costs.

The public sector must be responsible for implementing different initiatives, such as awareness campaigns, public education, promotion of good Internet practices, incentives for private sector companies, implement the adequate regulatory framework and guarantee that the laws are observed⁸.

- **Private Sector.** In the private sector, the interests for the increase in the security of the network are directly linked to their own business model. Internet service providers and DNS servers are responsible for the operation of the network and the growth of the Internet provides direct benefits to them. Therefore, they have a direct interest in improving the network and expanding it so that anyone can have access to it.

Service providers are concerned for the security breaches that can harm the feasibility of offering Internet services and those that have an impact on the quality of the service being offered to its clients. For example, *spam* is one of the biggest concerns of the private sector. In addition, DNS servers are worried about the service cancellation attacks that can be caused by the excess traffic, which can lead to the interruption of the service in some cases.

Thus, service providers will be interested in offering a determined level of security to its clients and must ignore all events that occur outside its network. However, some of the risks that are inherent to the Internet depend on the collaboration and agreements reached to implement a common code of practice, so that the protection of the network increases in global terms.

Currently, one of the theories that is growing in importance is the self-regulation of the private sector, providing their collaboration to the State's armed forces, increase user rights with access to practical tools, promote responsible business customs and educate the general public.

- **R+D.** The academic institutions and private organisations dedicated to the technological development and research are also promoters of Internet security. This sector is interested in creating a high quality network that can be used to develop new technologies.

The different R+D agents set their efforts on the study of the security problems from

⁸ See (Racicot, M. et.al., 1997)

the technical point of view, identifying the weak points in the infrastructure of the Internet. These institutions are in a good position to guide the private sector on the strategies that must be followed to increase the security of their networks.

- **Civil Society.** The consumer and user associations collaborate to increase the security of the Net. They are mainly interested in avoiding the dangers and risks of the Internet to the user: illegal contents, *spam*, viruses and the protection of information are the main concerns.

On the other hand, users also want to increase the quality of the Internet. They consider that the contents must not only be legal but also adequate for the public. Ideally, users would be able to implement tools to select and adapt the contents to the public, addressing the requirements of specific sectors, such as children.

Some initiatives are oriented towards the improvement of the security and these have been presented by private associations which have been created by individuals, with no participation from the governments and international organisations. For example, the organisations that have been at the forefront of the control of the quality of web sites with “trust markers” meet these requirements⁹. In addition, these issues are presented as independent mechanisms that act as intermediaries between the Administration and users.

As regards the security, all parties involved have interests that point towards the same direction. However, the different solutions present the same problems, whereby everyone has different views and a different involvement, depending on the type of group and sector. The establishment of common objectives must be the result of a balance between the interests of all parties involved.

The implementation of safe networks requires a free flowing dialogue and a series of collaboration agreements between the different groups in each sector and between different sectors. On the one hand, this is necessary so that the Internet network can develop in a way that pleases everyone. On the other hand, and even more important, none of the sectors have enough capacity to start the security measures or has the power to guarantee that other sectors will adopt the measures imposed.

Even though governments are responsible for enforcing the current legislation (even in *on-line* scenarios), the changeable nature of many activities carried out in the Internet, added to the anonymity of participants and the international aspect of many of the transactions, make it difficult to detect illegal activities and apply existing laws. The collaboration of the private sector is required (implementation of security technologies), as well as that of the civil society (for example, NGO’s that start initiatives oriented towards guaranteeing the security of the Internet) and research and development centres (evolution of the technologies that allow covering up for security problems).

The coordination of the strategies and effective collaboration between the different groups that strive to attain the same objectives and share a common vision can be

⁹ See (Industry Canada, 2006).

complex, i.e., many different organisations are interested in carrying out the same task and this might be an obstacle, since the excess participation can increase the level of confusion of users. For example, a “quality seal” or “trust marker” will be more effective as long as Internet users are aware of their existence and when more web sites choose to become part of this initiative. Within this context, the presence of different “quality seals” hinders the creation of a universal brand that all users will recognise.

National laws are hard to enforce on the Internet, an international network where illegal activities can easily pass through frontiers and infringe the laws of different countries. Measures should be proposed and investigated to globally combat the illegal activities in the Internet or which grow in importance in this environment, so that the legal gaps are eliminated in the cyber-crime environment.

To generate confidence, the user requires a series of measures that are adopted by other sectors, with a transparent approach and with well-known criteria. The civil society must form part of the process for the implementation of the security and must be aware of the measures implemented and their results.

The NGO’s that start security initiatives, such as the marking of web pages or the creation of direct lines, must know about other entities that are carrying out the same tasks and must promote the creation of alliances from other sectors, for example, from the public sector. In addition, for a greater effectiveness, the said NGO’s must help other organisations to achieve these goals.

The self-regulation process is characterised as one of the measures with the greatest potential for success. However, the collaboration from other sectors is necessary (users, research and development centres, etc.) in order to develop a series of security requirements that satisfy the needs of all users and parties involved. In this model, the group creates the rules for itself and it is also responsible for the fulfilment and application of the said rules. The involvement of other sectors will require the collaboration from different levels of activity.

The strategies must be adopted within collaboration and agreement framework between the companies in the sector, since the effectiveness of the technologies proposed depends on the joint collaboration for their implementation, as required to improve the network in global terms. In addition, since service providers and server operators are starting security techniques aimed at protecting incoming and outgoing traffic, these measures must be implemented jointly, with the purpose of creating truly beneficial measures for everyone.

ISSUES FOR ANALYSIS

Despite the research activities being carried out within the security and technology area to improve the net, the current scenario is focused on guaranteeing a level of security for the Internet that is not possible today. One of the reasons is that none of the current technologies is fully effective. Another reason is that all measures that could mean important advances require the collaboration of different sectors for their implementation.

This poses a challenge: the collaboration of the different sectors for the implementation of security measures, at the national and international level.

The international forums must be a place for dialogue and gathering, to focus on the different perspectives and thus explore the many different possibilities that these new perspectives offer. The problems posed by the Net have a global character and, therefore, so must the solutions proposed. The players must be aware of the actions being carried out and implemented in other countries and their effectiveness and suitability must be analysed.

Some of the activities within the security framework of the Internet governance practices are the following:

- Create a joint proposal for the definition of the characteristics and elements of the Internet, as required to guarantee the security, privacy and trust deposited by users.
- Analyse the convenience of developing self-regulation codes at the national level in the private sector, coordinating strategies that protect the network, at the national and international level.
- Analyse the convenience for developing self-conduct codes that are respected by all Internet users, especially in the fight against the distribution of illegal contents.
- Elaborate an Internet security action plan, based on three main pillars of action:
 - Social awareness. The government must play a special role in this activity, but the participation of the private sector and user associations is required to inform all citizens about the risks and techniques available to avoid these risks¹⁰.
 - Multilateral cooperation between groups. One of the factors for the success of electronic commerce is the security of networks, the trust of users and the efficacy of determined authentication and digital signature technologies. This sector thus requires a common point of view and the development of a strategy that increases the security of electronic commerce through the Internet.
 - Collaboration with the State's armed forces in the fight against cyber-crime. The private sector can help detect illegal activities and identify authors. The problem is that the reason for the creation of this collaboration is not so clear: user's privacy must be respected¹¹.

DIGITAL GAP

The development of the Information Society is a chance for the integration of the less developed groups of the society within a new model. However, this could lead to

¹⁰ See (Centre for Socio-legal Studies 2003)

¹¹ See (Cameron-Waller, 2001).

the increase in social differences, the well-known digital gap. Therefore, national governments and supranational institutions are fully aware of the need to eliminate the barriers in social differences, and they are thus making a huge effort on the expansion of the Information Society so that it can reach all levels, avoiding the exclusion of the less developed groups. The challenge aims at changing the situation while guaranteeing that everyone can benefit from it.

The problem of the digital division is complex and there is no easy solution. The digital gap defines the differences in access and an equal technological experience based on different categories, such as revenue, gender, geographical location or education received.

The term “digital gap” does not only describe the difference between individuals, but also that between family groups, companies and geographical areas who can or can not access ICT and the Internet, for many different purposes.

On the other hand, the “gap” does not only talk about the access to the said elements, but also to the employment and intelligent use of ICT in particular, the Internet, linked to the production, communication, marketing and administration activities.

Internet has positioned itself as one of the society’s and economy’s pillars, and must be regarded as a common good for everyone. The digital gap prevents the groups that have no access to “computer systems or information” from participating in the recruitment processes that require this knowledge, including electronic governance and on-line education.

GROUPS AND POSITIONS

The governance of the Internet plays a very important role in solving the problems of the digital gap, which requires the participation of all groups involved. The main positions of the groups of agents involved in the governance of the Internet for the solution of the digital gap are described next:

- ***Public Sector.*** The public sector is represented by the Public Administration and is one of the main groups involved in the reduction of the impact of the digital gap in specific regions. Its actions are mainly focused on the promotion of initiatives to expand the access of the Internet to all citizens, thus promoting the participation of everyone in the digital age, encouraging the creation of an economy based on knowledge through the training and education of its citizens, favouring the development of electronic commerce and the eGovernment as factors that stimulate the use and adoption of the Internet by everyone.

The public sector is responsible for carrying out initiatives that strive to attain the said objectives. Among these initiatives we can highlight the awareness, education and training campaigns, attracting investments, creating the adequate legal framework and guaranteeing the optimum development.

- ***Private Sector.*** The private sector is one of the key players in the promotion of the development of the Information Society and its collaboration is vital to reduce the

impact of the digital gap. The wideband services market is undergoing an impressive growth and expansion stage, although it is initially focused on the areas with the highest commercial interest, where less developed regions are observed as a secondary objective and the high level of investment required and low potential demand does not provide enough incentives for the creation of offers for these users.

Thus, the private sector demands a greater institutional support to receive the aid required to guarantee the presence of Internet infrastructures and services in those regions that are not included as the highest market priorities. In these conditions, the private sector must assume the leading role, provided that it has the support and stimulus of the public sector.

- **R+D.** This group is quite aware of the problems of the digital gap, although it does not find the adequate means to channel specific actions with their potential and expert knowledge. They have a clear vocation for research and development, promote the distribution of information on ICT to citizens and in many occasions collaborate with cooperation and aid programs and projects.
- **Civil Society.** This group promotes many local initiatives for the promotion of the access to technology and to help its implementation in populations with insufficient access. Likewise, they defend the need for the participation of minorities, guaranteeing pluralism and the participation of all community groups.

ISSUES FOR ANALYSIS

The digital gap must be addressed by more than simply a single initiative. However, it is important for organisations that carry out community ICT projects to satisfy the needs of its inhabitants; the issues being dealt in the national and international digital gaps are vast and organisations must cooperate to solve these problems together. The programs of the private sector, universities and philanthropic efforts are also vital in the said collaborations.

Given the need for the participation and collaboration of all groups involved, the following issues for analysis are set forth within the governance of the Internet framework:

- Analyse the role of the different groups in the development of the Information Society and the fight against the digital gap.
- Assess the level of coordination of the different initiatives at the regional, national and international level for the development of the Information Society.
- Propose different financing and sustainability scenarios for the said initiatives to reduce the impact of the digital gap.
- Analyse the potential mechanisms that facilitate the participation of minorities and disadvantaged groups in the Internet, especially as regards the creation of contents and social integration.

CONCLUSIONS

The purpose of this document is to provide more information about the debate on the governance of the Internet, to include additional issues that have a great relevance in its development. If we set off with an initial basic analysis of the Spanish case, the results obtained show how the economic, political and social sustainability must be considered to address vital issues for the future development of the Internet, such as the network neutrality, safety and the digital gap.

The three aforesaid issues are being studied and analysed in many international forums, but the need to guarantee the feasibility and sustainability of the initiatives set forth for the governance of the Internet are not usually considered to be a priority. Therefore, and as a result of the IGF Conference in Athens, this document presents specific proposals that should serve to focus the debate during the next few months and advance in the multilateral dialogue process to promote a feasible and sustainable model for the governance of the Internet.

REFERENCES

Comín, S (2006): *La net neutrality... ¿permitirá que se regule Internet?* Boletín de la Sociedad de la Información. Telefónica (*Net neutrality... Can the Internet be regulated? Information Society Bulletin*).

Drake, W (2006): *Internet Governance in transition: trends, challenges, and the global debate*.

FCC (2005): *The FCC's net neutrality guidelines*.

Finkelstein, L (1995): *What is global governance?* Global governance, vol.1, pp. 367-372.

Froomking, M (1997): *The Internet as a source of regulatory arbitrage. In borders in cyberspace*.

Froomking, M (2000): *Wrong turn in cyberspace: using ICANN to route around the APA and the Constitution*.

Industry Canada (2006): *Promoting safe, wise and responsible Internet use*.

Lessig, L (1999): *Code and others laws of cyberspace*.

Miller, G; Sinclair, G; Sutherland, D; Zilber, J (1999): *Regulation of the Internet. A technological perspective*.

Racicot, M; Hayes, M; Szibbo, A; Trudel, P (1997): *The Cyberspace is not a "No Law Land"*. A study of the issues of liability for content circulating on the Internet.

Rosenau, J (1992): *Governance order and change in world politics*. Cambridge University Press.

Centre for Socio-legal Studies (2003): *Website quality labelling*. University of Oxford. Comparative Media Law and Policy. Support for cooperation and coordination projects in Europe.

Wu, T. (2003): *Network Neutrality, Broadband Discrimination*.