

INTERNET GOVERNANCE

Pedro Veiga

Full Professor at the *Faculdade de Ciências (Universidade de Lisboa)* and President of *Fundação para a Computação Científica Nacional (FCCN)*. He was the President of the College of Computing of the Engineering Council and Manager of *Programa Operacional Sociedade da Informação* and a member of the Mission Team for the *Sociedade da Informação*

Marta Dias

Jurist in charge of the area *Comunicação&Imagem* at *Fundação para a Computação Científica Nacional (FCCN)*. She has a postgraduate diploma in Administrative and Juridical Sciences. She has worked at the administrative, financial, and legal departments of the *Inspecção-Geral da Educação* and of the *Direcção-Geral das Autarquias Locais*

Abstract

It has now become quite obvious that the Internet has brought significant changes to our society and a break on how we lived before its emergence. It is still too early to assess the impact on society of the new services at our disposal, such as the capacity to communicate faster and cheaper on a global scale, access information and, perhaps more importantly, to produce and disseminate information in a way that is accessible to all.

It is clear that the advent of the Information Society implies changes in our society that constitute a point of no return. However, contrary to what happened when we entered the Industrial Age about three centuries ago, when the changing process was slow and led by older individuals, these days the entrance into the Information Society is taking place rapidly and the decisive players are younger people.

The global nature of the Internet, the possibility of producing and distributing any type of content in digital form at almost zero cost, as well as the vast number of people who use the web, have highlighted the need for new forms of intervention in a sector where there are many types of players. It is in this context that the problem of Internet Governance becomes a very current issue, inasmuch as one feels the need to guarantee a diversity of rights and duties, which may appear difficult to reconcile.

This paper presents a brief overview of the main players and initiatives which, in the field of Internet governance, have tried to contribute to turning this network into a factor for social development and democraticity on a global scale.

Keywords

Governance; Internet; Security; Information Society; Privacy

How to cite this article

Veiga, Pedro; Dias, Marta (2010) "Internet Governance". *JANUS.NET e-journal of International Relations*, N.º 1, Autumn 2010. Consulted [online] on date of last visit, observare.ual.pt/janus.net/en_vol1_n1_art6

Article received in July 2010 and accepted for publication in September 2010



INTERNET GOVERNANCE

Pedro Veiga e Marta Dias

1. Introduction

Internet governance can be defined as the development and application, by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet¹.

When referring to Internet governance, one cannot ignore the vital role played by a group of organisations², on a national and world scale, which deal with the issues and problems that stem from it.

Of particular mention are the *Internet Corporation for Assigned Names and Numbers* (ICANN), the Internet Governance Forum (IGF), the International Telecommunication Union (ITU), the Internet Society (ISOC), the European Commission, and, at national level, the entities responsible for the management of the *country code top-level domain* (ccTLD)³.

However, it is not possible to understand Internet governance, or the principle on which the Internet should be governed, without first explaining how it came about and developed up to the present, and what is so good about it, which, in our opinion, outweighs its less positive aspects.

Then, we shall attempt to explain that Internet governance is not underpinned by mandatory and imposing actions and policies. Quite the opposite, from the very beginning it has resorted to a participatory model where all players have a say. The balance point is, thus, the compromise that is paramount to the safety and privacy of each individual, and, equally, to a free, open Internet.

¹ Original definition given by the Tunis Agenda for the Information Society, in: <http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf>

² UMIC – Agência para a Sociedade do Conhecimento, IP (Agency for the Knowledge Society) ensures, through its President, Portugal's representation at GAC – Governmental Advisory Committee of ICANN – Internet Corporation for Assigned Names and Numbers, at IGF – Internet Government Forum of The United Nations, as well as , in the European Union, HLIG – High Level Group on Internet Governance.

³ In Portugal, ccTLD.pt is managed by FCCN, within the context of IANA - Internet Assigned Numbers Authority (RFC 1032/3/4 e 159).



2. The technical invention of the Internet

The ideas leading to the origin of the Internet resulted from an applied research project, which began in the 1960s and aimed to connect several computers in the USA armed forces, to ensure the network had high tolerance to flaws. This requirement was brought about by the Cold War political environment and it had the purpose of guaranteeing that, even in case of potential war destroying many of this network's means of communication and computers, the remaining systems would continue to communicate and support military logistic operations, albeit with some limitation of its functions.

Given the poor communication capacity of telecommunication networks at the time, the technology to be developed was expected to work well at low speed connections (compared to now) and use a variety of means of telecommunication, land circuits, and satellite connections.

These objectives were the decisive factors in conceiving this technology, which became the core solution for connecting the main information systems, as well as the communication technology that stands at the basis of the information society at the beginning of the 21st century.

Nevertheless, it was, undoubtedly, the invention of the World Wide Web that gave the Internet the capacity to present information in such a way that it contributed to its expansion to the masses.

It enabled global access to information, which became increasingly presented in digital format, and forced a change in the way individuals and economic agents interact among themselves and with public administration.

3. The year of 1995 and the Internet for the public at large

The year of 1995 marked the beginning of the Internet for the general public. This growth did not take place in a uniform manner in all countries. It first started in the USA and the North of Europe and, subsequently, extended to other world regions.

Right from the outset, there was a perception that the Internet could be very important as a tool for development, which went hand in hand with concerns regarding "who controls the Internet?" There were two types of resources, in particular, that became the focus of concern: domain names and IP addresses (numbers) used by Internet computers.

With regard to domain names (i.e. <http://www.parlamento.pt> or <http://www.cnn.com>), a peculiar situation arose. Whereas domains ending in two letters were the responsibility of each country, corresponding to countries' ISO codes, global domains (.com, .org, .net, .edu) were managed and commercialised, in a monopoly system granted by contract, to an American company, NSI – Network Solutions International. The way domains and other technical aspects of the Internet were managed posed several problems, of which the better known were: i) the need for global and generic domains, called *gTLDs* (Generic Top-Level Domains); ii) cybersquatting, which was the abusive appropriation of domains and the huge difficulty in managing this type of abuse on a global scale; iii) lack of *competitiveness* in the commercialisation of existing *gTLDs* on a world scale; iv) the fact the Internet was dominated by the English language, a



technical reminiscence of the 7 bits *ASCII* code, which did not allow the representation of all the characters in the Portuguese language, but was even much more serious in the case of non-Latin languages; v) the stable system of Internet protocol addresses distribution (IP and other protocol addresses); vi) the technical stability and the safety of the resolution of names and domains support infrastructure.

The European Union was aware of the economic and social importance of the Internet, and started contacts and negotiations with the USA government, which, during the Clinton administration, triggered off a series of political moves aiming to create a new era in the way the Internet was managed. The initial concerns, predominantly of a technical nature, were followed by a series of measures we shall now analyse.

4. The setting up of the ICANN

The *ICANN*⁴ (*Internet Corporation for Assigned Names and Numbers*) was set up following a few failed attempts to create procedures appropriate to the expansion of the Internet, supported by mechanisms ensuring its geographic and cultural diversity, democraticity, technical stability, and independence from economic interests.

On 25 November 1998, the Department of Commerce of the USA, on behalf of the American Government, signed a *Memorandum of Understanding (MoU)* with the recently founded *ICANN*. Basically, this *MoU* had a fundamental objective: to carry out the transfer of the management of the Domain Names System (DNS) to the private sector, that is, a not-for profit corporation, thus freeing it from alleged ties to the USA government.

After a series of addenda to this *MoU*, the *Joint Project Agreement (JPA)* was only signed in 2006. In practice, it reaffirmed *ICANN*'s responsibilities regarding a set of goals established in the beginning, the most important being the effort to establish competition in the services registering domain names for *gTLDs* (*Generic Top Level Domain System*), including the implementation of new *TLDs* (*Top Level Domains*), the development of a policy to resolve dispute and conflict in the registration of *TLDs* (*Uniform Domain Name Dispute Resolution Policy*), the establishment of formal agreements with entities responsible for the management of distinct *TLDs*, the implementation of a financial strategy capable of ensuring the sustainability of the actual organization and, particularly, the technical management of the *DNS*, where *ICANN* operated together with *IANA* (*Internet Assigned Numbers Authority*).

On 5 June 2008, Viviane Reding, then European Commissioner for the Information Society and the Media, contended that: "The Internet Corporation for Assigned Names and Numbers is reaching an historical milestone in its development. Will it become a fully independent and responsible organisation for the Internet's world community? This is what the European expects and this is what we shall defend. I invite the United States to work with the European Union to attain this goal".

Eleven years after the process started, the Affirmation of Commitments (AoC) was signed on 30 September 2009, a date considered historical in Internet governance. Several principles were agreed: the management of the Internet shall be carry out by a not-forprofit private organisation, in a bottom-up manner, and the multi-stakeholder

⁴ <http://www.icann.org/>



structure will be open, transparent, and independent. This set of prerogatives was explicitly and unquestionably conferred to *ICANN*.

Nowadays, *ICANN* stands as an institution turned to the future and able to take on the challenges formalised by the AoC. It represents public and private organisations, governments and governmental agencies, companies, the Internet technical community, Internet services suppliers, registrars, registries, registrants, and the civil society itself.

ICANN, thus, relies on a governance model that is networked, global, and open, and aims to balance the various interests involved in the management of the several technical aspects connected to Internet management.

ICANN is based on the group of entities that form it, of which the most important are: the Board and its president, several supporting organizations (SO), and a *CEO* responsible for its operational structure. The members of the Board are elected according to geographical regions for one, two, or three-year mandates, with the aim of ensuring widespread representation and diversity. The geographic regions are: Africa, North America, Latin America and Caribbean, Asia, and Europe.

Although it is acknowledged that many Internet-related issues are of public interest, *ICANN* deals with the role of governments in a particular and innovative manner, with all the controversy associated to it. There is an advisory body called *Government Advisory Committee (GAC)* that prepared the guidelines and opinions that are taken into consideration by the Board in its decision-making process. These reports are written by own initiative or at the request of the of *ICANN's* president. The role of GAC was amply strengthened in the AoC in terms of decision-making processes of a political and strategic nature, and also in the actual technical coordination of DNS.

There are several supporting organisations: *ccNSO (Country Code Name Supporting Organisation)*, *GNSO (Global Names Supporting Organisation)*, *ASO (Address Supporting Organisation)* and *At-Large*. *At-Large* is the name given to those who aim to represent Internet individual users worldwide and wish to contribute to *ICANN's* political orientations.

ICANN's agenda, the result of contributions by its several supporting organizations, is currently focused on Internet safety and stability – *DNSSEC* and *eCrime* -, on the launching of new *gTLDs*; on *IDNs* for *ccTLDs* and *gTLDs*; on the transition from *IPv4* to *IPv6*, and on issues regarding the *WHOIS* system.

ICANN has been acting on several fronts but has pursued a set of stronger measures, of which the following stand out: internationalisation of the management and technical operations of the Internet, representation equity of all geographic areas, and the safety and stability of the Internet's core infrastructure.

5. Global challenges

The years between 1995 and 2000 confirmed the importance of the Internet as a tool for development. There was also a perception that, besides the global technical aspects that *ICANN* had started to address, there were many others that needed to be debated, in a world that was becoming increasingly global.



WSIS – World Summit on the Information Society – is a United Nations initiative organised around two conferences that took place in 2003 (Geneva), and in 2005 (Tunis). The conferences aimed to overcome the digital divide between rich and poor countries and discuss how the information society can be a core tool for development, improved life standards, and sustained development.

The *Declaration of the Principles of Geneva* and the *Action Plan* (ITU website) were the first documents that identified the major guidelines the world community saw as being of relevance. The documents approved in Tunis – *The Tunis Compromise* – and, particularly, the *Tunis Agenda for the Information Society*, defined a series of objectives and ways to attain them. It is not possible, in the present paper, to describe the diversity and scope of the identified objectives, given the cultural nature and diversity of the communities involved. Some of them ended up as statements of good will, rather than concrete measures that can be followed up on a global scale.

However, we would like to stress that there is a general awareness that we have entered the age of the Information Society, and that this fact brings huge opportunities, particularly for developing countries. It also brings to the foreground a series of older challenges that need to be overcome, especially those related to communication infrastructures and the training of individuals to fight the digital divide. Particular emphasis is being given to the effort that needs to be made to include traditionally excluded groups whenever there are paradigm breaks, such as women, the elderly, migrants, the disabled, particularly because there is a perception that these groups may benefit the most from the Information Society.

Among the *Key Principles of the Tunis Agenda*, the following stand out: investment in a multi-stakeholder model for the development of the Information Society; acknowledgement of the major role played by the private sector in making infrastructures available and of the role of the media in a knowledge-based society; raising awareness of the need for increased cooperation between public and private bodies to address the fact that safety issues are global and critical to ensure users trust the use of the Internet and information technologies.

This multi-stakeholder model relies on the collaboration, involvement, and sharing of responsibility among governments, the private sector in its distinct forms, the civil society where NGOs play a decisive role, and citizens.

Some of the numerous examples stipulated in the *Tunis Agenda* as factors in development include access to information and knowledge, enabling people to benefit from the information society, creation of safe and trustworthy environments, protection of intellectual property rights, the need to invest in research and development, the possibility of using *ICT* in new sectors such as health, even at a distance, maintaining the Internet's multicultural facet and using it to preserve cultural heritage.

After 2005, the *Tunis Agenda* has been followed up on a yearly basis by annual meetings of the *Internet Governance Forum – IGF*⁵. So far meetings have taken place in Athens (2006), Rio de Janeiro (2007), Hyderabad (2008), Sharm-el-Sheik (2009), and Vilnius (2010). Although *IGF's* mandate comes to an end this year, it may continue its agenda up to 2015, a decision the UN will make at the end of the year. However, the work and reflections already carried out in, for instance, cybercrime, privacy, freedom

⁵ <http://www.intgovforum.org/cms/>



of speech, and the most critical resources in the Internet must be underlined. Another vital issue for many regions in the globe is access to the Information Society. Either due to cost or lack of infrastructures, there are still millions of individuals worldwide who are deprived from access to it. Accordingly, one of the areas where a lot of effort has been made, but which is also one of the most difficult to resolve, is that involving access to communication structures, which is closely connected to the next steps: access to equipments (computers or similar) and digital world literacy.

On a European level, increased attention is being paid to the problems regarding Internet governance. Europe is probably the region in the world where we find more structured thoughts on the topic. *EuroDIG*⁶ (*European Dialogue on Internet Governance*), which is a forum for debating these issues, was created to discuss the current and future challenges the Internet is bringing into the agenda of the European society.

6. Legal issues of the global network

Awareness of the power and growth of the Internet led to the alleged need for its governance. When talking about governance, the law is the first ruling instrument, followed by crime police bodies and, in the last instance, the courts. On this issue, there are two opposing views. One that defends that Internet governance is a safety imperative, and that safety can only be guaranteed if there is regulation and sanctions' control. The other position defends that governance is anti-natural and that, in its most radical stance, it represents a tool for Internet censorship.

Among us, the prevailing view is for minimum governance combining individual freedom with the necessary privacy, safety, and respect for rights, liberties, and guarantees of each individual and people in general.

The protection of personal data, the defence of intellectual property and associated rights, the fight against cybercrime, the protection of minors, who are considered to be particularly vulnerable in their daily use of Web resources, particularly social networks, the rights of consumers in general, the potential constraints in commercial access to Internet services and corresponding regulation by the competent authorities in each country, constitute a few of the touchstones when referring about the legal aspects of the Internet.

Within the Internet, the borders become blurred or simply disappear, and international law not always has the answers to the issues that arise. In addition, at a national level, there is either no specific law or, when it exists; there may be doubts as to its enforcement.

With regard to protection of personal data⁷, the National Committee for Data Protection, as the national entity for control of personal information, has launched several awareness-raising campaigns to draw people's attention to the dangers of circulation of personal data on the Internet. The applicable legal system restrains the

⁶ <http://www.eurodig.org>

⁷ Law no 67/98 of 26 October – the Law for the Protection of Personal Data defines personal data as follows: any type of information, regardless of its nature and form it is presented, including sound and image, pertaining to an identified or identifiable person («data holder»); anyone who can be directly or indirectly identified, namely through reference to an identification number or one or more specific aspects of his physical, physiological, psychic, economic, cultural or social features is considered to be identifiable;



possibility of data processing to two specific situations: those resulting from the law, and those stemming from the express free and informed consent of each individual. Apart from these two situations, we have a muddy field that deserves and awaits legal regulation. This is where vagueness arises, when, for instance, the applicable legal system is that of a country where simply there may not be a law regulating personal data protection. This is the case in the USA, for example, where the accountability model prevails, in detriment of personal data protection, which we have in countries like Portugal or Germany.

In 1991, the *Computer Crime Law (LCI)* was approved as per Law no. 109/91 of 17 August. This law followed the Recommendation 89/9 of the European Council and adopted the non-compulsory list of crimes listed in the Recommendation, such as: computer fraud; damage regarding data or computer programmes; computer sabotage; illegal access; illegal interception and reproduction of protected programmes. The penalties for basic crimes ranged from imprisonment up to 3 years, except in the case of qualified crimes, when sentences could be up to 10 years imprisonment (in the case of informatics sabotage). The Computer Crime Law also foresaw the criminal responsibility of companies practising this type of crime (as well as several accessory crimes), with managers and the actual companies being considered responsible. The national legal system went even further, and the *Criminal Code* established the legal system regarding computer fraud where, contrary to what happens with the LCI, companies are not considered to be accountable.

Meanwhile, on 23 November 2001, Portugal joined the *Cybercrime Convention*, whose main goal was to standardise the national legal systems of member states of the European Union with regard this type of crime, as well as to make international cooperation and crime investigation easier.

On 15 September 2009, Law no. 109/2009, also known as *Cybercrime Law*, was published. This new law set out the material and procedural penal dispositions, and those on international cooperation on crime matters, regarding cybercrime and the collection of evidence in electronic format. It transposed into the Portuguese legal system the Council Framework Decision no. 2005/222/JHA on attacks on information systems, adapting internal law to the *Convention on Cybercrime of the Council of Europe*. The *Computer Crime Law*, which had been in force for a long time, was, thus, revoked. On the same day the *Cybercrime Law* was published, the Convention on Cybercrime was also approved and ratified (eight years later), as well as the Additional Protocol to *The Convention on Cybercrime Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems*, adopted in Strasbourg on 28 January 2003. This law implemented what Portugal committed to do as part of the Cybercrime convention. It is an instrument for international cooperation as it allows over 40 countries to adopt a similar legal system regarding Cybercrime and electronic collection of evidence on matters of attack against information systems.

This new law brings a new element, in that it sets out types of new crimes that aim to deal with new Internet paradigms, such as the crime of phishing. Now, the mere propagation of computer viruses is punished. Even in the absence of computer damages, Courts may rule the handing over of objects, equipments or devices to the State, if they were used for the practice of crimes listed. This is a law applicable to computers crimes, crimes committed by electronic means, or illicit acts whose evidence is kept electronically. To further stress the points made in this paper, this law



underlines and formalises, explicitly and unequivocally, the role of international cooperation. This is set out over six articles that establish the ways and means the competent national authorities cooperate with their international counterparts. It further contemplates the preservation and quick release of computer data for purposes of criminal investigation, with rigorous deadlines for their safekeeping. On this matter, cooperation extends beyond law enforcement officers and includes providers of electronic communications services. Lastly, as part of the general law applicable, whenever it does not oppose the Cybercrime Law, crimes, procedural measures, and cooperation shall be ruled by dispositions set out in the *Criminal Code*, the *Criminal Procedural Code* and Law no. 144/99, of 31 August. The fact that treatment of personal data must be regulated by the dispositions contained in Law 67/98, of 26 October, is further strengthened.

In short, to state that the legislative body has its back turned on the Internet, is to ignore current legal legislation. However, the slow pace of law enforcement continues to be a major challenge.

As it is not possible to mention extensively the entire legal framework in this paper, we shall mention just a few dispositions of the Fundamental Law: the Portuguese Constitution. Examples include Article 35, no. 6, which states: "access to public computer networks is open to everyone (...)". Article 37 establishes freedom of expression and of information, and its wording states that everyone can freely express his/her thoughts by any means without impediments or discrimination.

Given that, in general, legal norms may not prevail over the fundamental principles of the democratic Rule of Law protected by the Constitution, the dichotomy safety/freedom is easy to understand, as well as the need to balance out these values when referring to Internet governance.

We have referred to the role of particular bodies regarding Internet governance, stressing the importance of national registries in the management of each country's ccTLDs. We shall now briefly assess what has been done in Portugal on this matter.

Between 1991 and 1996, the registration of names under the domain .pt was based exclusively on technical grounds. With the increase in the number of registrations, the first rules on registration of .pt domains came about in 1996, still quite incipient and adapted to the needs of the time, when the main concern was fighting cybersquatting.

The Resolution of the Council of Ministers no. 69/97 of 5 May clarified, within the Portuguese legal system, the spread, and the terms of the responsibility and role of FCNN, and conferred to the Ministry of Science and Technology the competences "to settle all potential divergences between FCNN and those requesting or benefiting from all Portuguese specific domains or sub-domains."

The *DNS Advisory Council of .pt* was subsequently created, as a consultative body formed by renowned entities in the areas of the Internet, intellectual and industrial property, and telecommunications, which are asked to propose and give opinions on any changes to the applicable regulations. This model is an example of what nowadays is regarded as the basis of "good" Internet governance, as it has a multi-stakeholder composition where entities such as INPI – *Instituto Nacional da Propriedade Industrial/National Institute for Industrial Property*, *Associação Portuguesa para a Defesa do Consumidor* – *DECO/Portuguese Association for the Protection of*



Consumers; ANACOM – Autoridade Nacional de Comunicações/National Authority for Telecommunications, Direcção Geral do Consumidor/Consumers Directorate-General, APREGI – Associação de Prestadores de Registos de Domínios e Alojamento/Association of Domains and Accommodation Sites Providers/APREGI are represented, as well as highly reputable bodies in the field of the Internet.

When the impact of the Internet and the legal and economic value of domain names became fully acknowledged at the end of the 1990s, FCCN, as a *.pt Registry*, published a new regulation with the purpose of facilitating and accommodating *.pt* registrations according to their activity and target audience. As a result, the following classifiers were created: *.org.pt*, *.publ.pt*, *.gov.pt*, *.net.pt*, *.name.pt*, *.int.pt*, *.edu.pt*, *.com.pt* (the latter had no registration restrictions, which made access to domain name registration easier, which in fact did happen, making it the first choice in name registration, immediately after the registration *.pt*).

The rules on *.pt* domain name registration were reviewed again in 2003. The most important change was the introduction of an arbitration system for the resolution of conflict in domain names, the abolition of some prohibitions, and a reduction on the price of submitting and maintaining domains. These measures fostered an increase in the number of registrations under TLD.PT. A new alteration in 2006 consolidated a set of principles: the pursuit of a policy that aims to prevent speculative and abusive registration of *.pt* domain names, in conformity with best practice, including *World Intellectual Property Organization – WIPO* recommendations, resorting to an extra-judicial litigation solving policy – arbitration process; the possibility of registering domains/sub-domains with special characters of the Portuguese alphabet; the correct configuration and operation of the prime server of the zone DNS PT, and the priority assumption of safety in that operation, with the implementation of DNSSEC extensions. The new regulation for the registrations of *.pt* domains has been in force since 1 July 2010, characterised by increased flexibility of the sub-domains *.com.pt* and *.org.pt*, increased safety for *.pt*, and the formal adoption of the arbitration centre *ARBITRARE*⁸ for resolution of conflicts in this field.

Final Notes

The dissemination of the digital society is one of flags of the *Strategy Europe 2010*, launched in March by the European Commission, which, on 19 May 2010, published a Digital Agenda with one hundred measures and a calendar for implementation up to 2015. The Agenda is divided in seven priority areas, including the creation of a single digital market, increased interoperability, and reinforcement of trust in the Internet and its safety, and much quicker access to the Internet for all citizens.

The growing role the Internet is playing in our society has led to increasing involvement of governments in the distinct areas of this network. Whereas some governments express their concern regarding the economic and social impact of the network, and defend its use as a tool for development and democraticity, others attempt to control it to impair its use for political purposes that oppose their own interests. It is within this huge and diverse world that Internet governance moves about, aiming to follow

⁸ <http://www.arbitrare.pt>. *ARBITRARE* is an institutional arbitration centre with authority to solve conflicts on industrial property, companies and pt. domains denominations and names.



innovative approaches that ensure a growing use of the network amidst safety, stability, and universal span.

List of Acronyms

ICANN – Internet Corporation for Assigned Names and Numbers

gTLD – Generic Top-Level Domain

ccTLD – Country Code Top-Level Domain

ITU – International Telecommunications Union

ISOC – Internet Society

IGF – Internet Governance Forum

EuroDIG – European Dialogue on Internet Governance

IPv4 – Internet Protocol Version 4

IPv6 – Internet Protocol Version 6