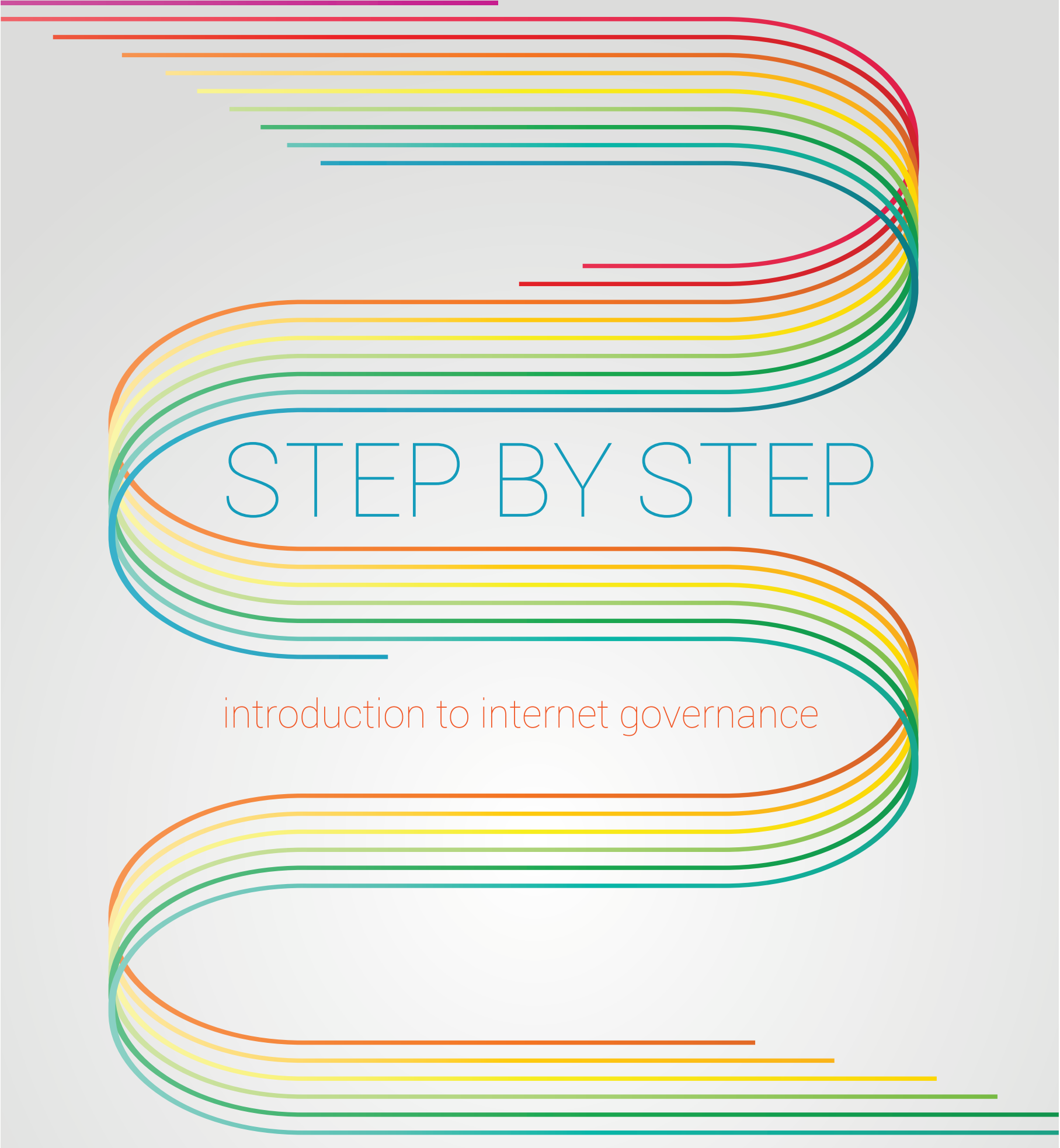
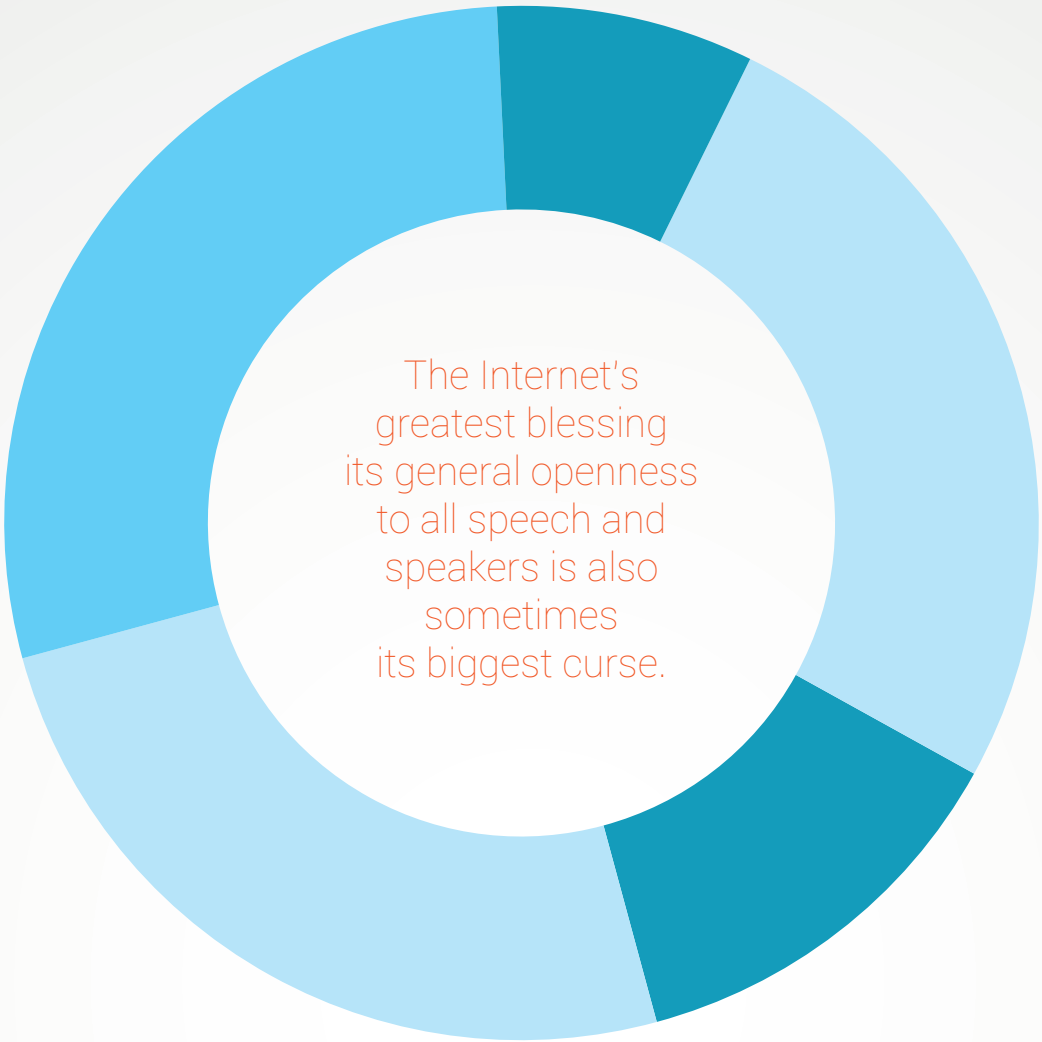

STEP BY STEP
introduction to internet governance

Back in 2003,
The Economist magazine started writing Internet with a lowercase 'i'.

This change in editorial policy was inspired by the fact that the Internet had become an everyday item, no longer unique and special enough to warrant an initial capital.

The word 'Internet' followed the linguistic destiny of (t)elegraph, (t)elephone, (r)adio, and (t)elevison, and other such inventions.


The Internet's
greatest blessing
its general openness
to all speech and
speakers is also
sometimes
its biggest curse.

What is Internet governance and why is it important?

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.

Still what are internet and governance doing together?

Internet

The term 'Internet' does not cover all of the existing aspects of global digital developments. Two other terms – information society and information and communication technology (ICT) – are usually put forward as more comprehensive. They include areas that are outside the Internet domain, such as mobile telephony. The argument for the use of the term 'Internet', however, is enhanced by the rapid transition of global communication towards the use of Internet protocol (IP) as the main communications technical standard.

Governance

In the Internet governance debate, controversy arose over the term 'governance' and its various interpretations. According to one interpretation, governance is synonymous with government.

This interpretation clashed with a broader meaning of the term 'governance', which includes the governance of affairs of any institution, including non-governmental ones.

This was the meaning accepted by Internet communities, since it describes the way in which the Internet has been governed since its early days.

The terminological confusion was further complicated by the translation of the term 'governance' into other languages. In Spanish, the term refers primarily to public activities or government (gestión pública, gestión del sector público, and función de gobierno). The reference to public activities or government also appears in French (gestion des affaires publiques, e cacité de l'administration, qualité de l'administration, and mode de gouvernement). Portuguese follows a similar pattern when referring to the public sector and government (gestão pública and administração pública).

 # Old-real' vs 'new-cyber' approach

There are two approaches to almost every Internet governance issue. The 'old-real' approach argues that the Internet has not introduced anything new to the field of governance. It is just another new device, from the governance perspective, no different from its predecessors: the telegraph, the telephone, and the radio.

For example, in legal discussions, this approach argues that existing laws can be applied to the Internet with only minor adjustments. In the economic field, this approach argues that there is no difference between regular commerce and e-commerce. Consequently there is no need for special legal treatment of e-commerce.

The 'new-cyber' approach argues that the Internet is a fundamentally different communication system from all previous ones. The main premise of the cyber approach is that the Internet has managed to de-link our social and political reality from the (geographically separated) world of sovereign states. Cyberspac e is different from real space and it requires a different form of governance. In the legal field, the cyber school of thought argues that existing laws on jurisdiction, cybercrime, and contracts cannot be applied to the Internet and that new laws must be created. Increasingly, the old-real approach is becoming more prominent in both regulatory work and policy field.

Decentralized vs centralized structure of Internet governance

According to the decentralized view, Internet governance should reflect the very nature of the Internet: a network of networks. This view underlines that the Internet is so complex it cannot be placed under a single governance umbrella, such as an inter-governmental organization, and that decentralized governance is one of the major factors allowing fast Internet growth. This view is mainly supported by the Internet's technical community and by developed countries.

The centralized approach, on the other hand, argues that there should be one inter-governmental organization for Internet governance. Some countries are motivated for this approach due to the limited human and financial resources available to follow highly decentralized Internet governance processes.

 # Protection of public interests on the Internet

One of the main strengths of the Internet is its public nature, which has enabled its rapid growth and also fosters creativity and inclusiveness. How to protect the public nature of the Internet will remain one of the core issues of the Internet governance debate. This problem is especially complicated given that a substantial part of the core Internet infrastructure – *from transcontinental backbones to local area networks* – is privately owned.

Whether or not private owners can be requested to manage this property in the public interest and which parts of the Internet can be considered a global public good are some of the difficult questions that need to be addressed. Most recently, the question of the public nature of the Internet has been re-opened through the debate on network neutrality.

Prefixes: e- / virtual / cyber / digital

The prefixes *e- / virtual / cyber / digital* are used to describe various ICT/Internet developments. Their use originates in the 1990s and implies different social, economic, and political influences in the development of the Internet. For example, the prefix e- is usually associated with e-commerce and the commercialization of the Internet in the late 1990s. Academics and Internet pioneers used both cyber and virtual to highlight the novelty of the Internet and the emergence of a brave new world. Digital came into use primarily in technical fields and received prominence in the context of the digital divide discussion. In the international arena, the prefix cyber was used by the Council of Europe for the Convention on Cybercrime (2001). More recently, it has been used to describe cyber security issues.

 # Policy balancing acts

On many Internet governance issues, balance has to be established between various interests and approaches. Establishing this balance is very often the basis for compromise. Areas of policy balancing include:

Freedom of expression vs protection of public order: the well-known debate between Article 19 (freedom of expression) and Article 27 (protection of public order) of the Universal Declaration on Human Rights has been extended to the Internet. It is very often discussed in the context of content control and censorship on the Internet.

Cyber security vs privacy: like security in real life, cyber security may endanger some human rights, such as the right to privacy. The balance between cyber security and privacy is in constant flux, depending on the overall global political situation. After 09/11 with the securitization of the global agenda, the balance shifted towards cyber security.

Intellectual property – protection of authors' rights vs fair use of materials: another 'real' law dilemma which has taken a new perspective in the online world.

IGF - Internet Governance Forum

In the Tunis Agenda (2005) of the UN World Summit on the Information Society (WSIS) heads of states decided to invite the UN Secretary General to convene a "Internet Governance Forum" (IGF) for a multi stakeholder policy dialogue on Internet issues.

The Internet Governance Forum (IGF) is a multi-stakeholder forum for policy dialogue on issues of internet governance. It brings together all stakeholders in the internet governance debate, whether they represent governments, the private sector or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process.
The Internet Governance Forum is the place where all these stakeholders can meet and talk. It is, essentially, global assemblage of internet users of which will lead to new ideas that will improve the operation. The Forum is not a decision making body but a prospect for dialogue on issues relating Internet governance.

The mandate of the IGF is:
Discuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet.

Facilitate discourse between bodies dealing with different cross-cutting international public policies regarding the Internet and discuss issues that do not fall ithin the scope of any existing body;

Interface with appropriate inter-governmental organizations and other institutions on matters under their purview;

Facilitate the exchange of information and best practices, and in this regard make full use of the expertise of the academic, scientific and technical communities;
Advise all stakeholders in proposing ways and means to accelerate the availability and affordability of the Internet in the developing world;

• Strengthen and enhance the engagement of stakeholders in existing and/or future Internet governance mechanisms, particularly those from developing countries;

• Identify emerging issues, liing them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations;

• Contribute to capacity building for Internet governance in developing countries, drawing fully on local sources of knowledge and expertise;

• Promote and assess, on an ongoing basis, the embodiment of WSIS principles in Internet governance processes;

• Discuss, inter alia, issues relating to critical Internet resources;

• Help to find solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users;All six IGF conferences (Athens 2006, Rio de Janeiro 2007, Hyderabat 2008 Sharm el Sheikh 2009, Vilnius 2010, Nairobi 2011 and Baku 2012) demonstrated the need and usefulness of the creation of innovative discussion platform which allow various stakeholders to contribute to a global bottom up policy development process on Internet issues.
The five main subjects of the IGF agenda, as agreed by the IGF Multistakeholder Advisory Group (MAG), are access, openness, diversity, security and critical Internet resources.The five global Internet issues are also important on the national and regional level. European stakeholders, including European institutions like the European Parliament and the Council of Europe, supported the idea, to launch a "European Dialogue on Internet Governance" (EuroDIG) to enable European governments, parliaments, organizations, private sector and civil society groups, the technical and academic community etc. to contribute to Internet Governance policy development in Europe and to bring European experiences to the global IGF-debate.

EuroDIG

The Pan-European dialogue on Internet governance (EuroDIG) is an open platform for informal and inclusive discussion and exchange on public policy issues related to Internet Governance (IG) between stakeholders from all over Europe. It was created in 2008 by a number of key stakeholders representing various European stakeholder groups working in the field of IG. EuroDIG is a network which is open to all European stakeholders that are interested in contributing to an open and interactive discussion on IG issues.

The stakeholders participating in the EuroDIG programme network comprise a considerable number of representatives from civil society, the business sector, the technical and academic community as well as European governments, institutions and organizations including the EU-presidency, the European Commission, the European Parliament, the Council of Europe and the European Broadcasting Union.

The purpose of EuroDIG is twofold: first to help European stakeholders to exchange their views and best practices on the issues to be discussed at global IGF meetings and to identify common ground which is shared by all European stakeholders as well as highlighting the diversity of experience of the different European stakeholders; second to raise awareness in Europe and among European stakeholders about the relevance of the issues discussed in the IGF context and also to raise awareness of the value of the new multi stakeholder discussion format developed by and around the IGF.

DIGITAL RIGHTS

The term digital rights describes the human rights that allow individuals to access, use, create, and publish digital media or to access and use computers, other electronic devices, or communications networks. The term is particularly related to the protection and realization of existing rights, such as the right to privacy or freedom of expression, in the context of new digital technologies, especially the Internet. Internet access is recognized as a right by the laws of several countries.

A number of human rights have been identified as relevant with regard to the Internet. These include: freedom of expression, data protection and privacy and freedom of association. Furthermore the right to education and multilingualism, consumer rights, and capacity building in the context of the right to development have also been identified. Human rights have been termed the "missing link" between the technology oriented and the value oriented approaches to the Internet.

 # 10 Internet Rights & Principles

The Internet offers unprecedented opportunities for the realization of human rights, and plays an increasingly important role in our everyday lives. It is therefore essential that all actors, both public and private, respect and protect human rights on the Internet. Steps must also be taken to ensure that the Internet operates and evolves in ways that fulfill human rights to the greatest extent possible.

Internet Rights and Principles Dynamic Coalition (IRP), an open network of individuals and organizations working to uphold human rights in the Internet environment has complied ten key rights and principles that must form the basis of Internet governance.

To help realize this vision of a rights-based Internet environment, the 10 Rights and Principles are:

1) Universality and Equality

All humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.

2) Rights and Social Justice

The Internet is a space for the promotion, protection and fulfilment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment.

3) Accessibility

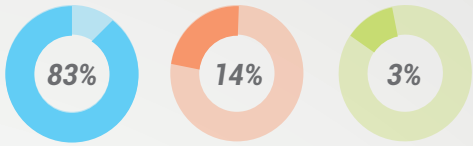
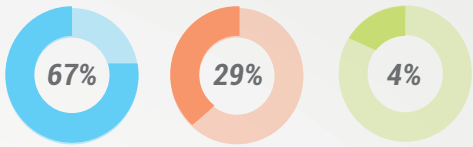
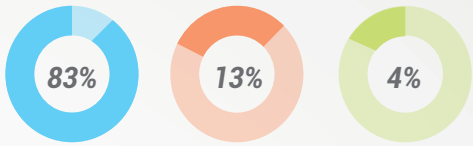
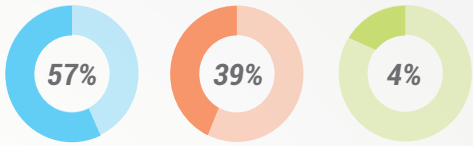
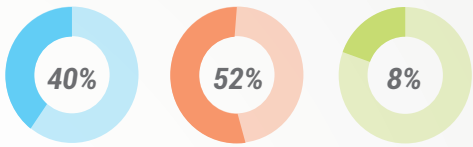
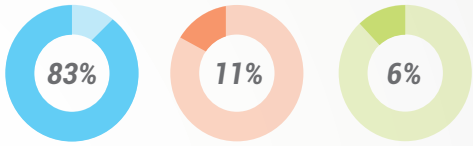
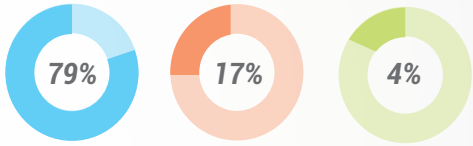
Everyone has an equal right to access and use a secure and open Internet.

4) Expression and Association

Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural or other purposes.

5) Privacy and Data Protection

Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.

Question	No. of Responses	Responses
Access to the Internet should be considered a basic human right.	*10,789*	
Each individual country has the right to govern the Internet the way they see fit.	*10,789*	
The Internet does more to help society than it does to hurt it.	*10,789*	
Increased government control of the Internet would make me use the Internet less.	*9,717*	
Increased government control of the Internet would increase the number of users.	*9,717*	
Governments need to place a higher priority on expanding the Internet and its benefits in my country.	*10,789*	
For the Internet to reach its full potential in my country people need to be able to access the Internet without data and content restrictions.	*10,789*	

somewhat or strongly agree

somewhat or strongly disagree

don't know / not applicable

In July and August 2012 the Internet Society conducted online interviews of more than 10,000 Internet users in 20 countries. Some of the results relevant to Digital rights and Internet access are summarized above.
https://www.internetsociety.org/sites/default/files/GIUS2012-GlobalData-Table-20121120_0.pdf

6) Life, Liberty and Security

The rights to life, liberty, and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

7) Diversity

Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.

8) Network Equality

Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritization, filtering or traffic control on commercial, political or other grounds.

9) Standards and Regulation

The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all.

10) Governance

Human rights and social justice must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability.

Digital literacy

Digital literacy is the ability to effectively and critically navigate, evaluate and create information using a range of digital technologies. It requires one "to recognize and use that power, to manipulate and transform digital media, to distribute pervasively, and to easily adapt them to new forms". Digital literacy does not replace traditional forms of literacy. It builds upon the foundation of traditional forms of literacy. Digital literacy is the marrying of the two terms digital and literacy; however, it is much more than a combination of the two terms.
Digital information is a symbolic representation of data, and literacy refers to the ability to read for knowledge, write coherently, and think critically about the written word.

There are five types of literacies that are encompassed in the umbrella term that is digital literacy:

(1) Photo-visual literacy is the ability to read and deduce information from visuals.

(2) Reproduction literacy is the ability to use digital technology to create a new piece of work or combine existing pieces of work together to make it your own.

(3) Branching literacy is the ability to successfully navigate in the non-linear medium of digital space.

(4) Information literacy is the ability to search, locate, assess and critically evaluate information found on the web.

(5) Lastly, socio-emotional literacy refers to the social and emotional aspects of being present online, whether it may be through socializing, and collaborating, or simply consuming content.

European Youth Forum in its Policy paper on New media and Internet Governance states:

"A new threat of social exclusion and discrimination is emerging where equal access to digital media literacy is not ensured for all young people. This calls for policies aimed at equipping young people with adequate skills and securing informed access to the internet and new media for them. It is important that digital media literacy is mainstreamed at all levels of formal and non-formal education, including a lifelong learning approach.

Digital skills showcase the importance of the right mix of generic competences and technical skills, ranging from informally acquired functional digital skills to specialist skills. Digital and media literacy will therefore be crucial both for private and professional life and, although it is almost universally true that any job will require some level of e-skills, the aim should be digital fluency. "

Privacy and data protection

Privacy and data protection are two interrelated Internet governance issues.
Data protection is a legal mechanism that ensures privacy. Yet, what is privacy?

It is usually defined as the right of any citizen to control their own personal information and to decide about it (to disclose information or not). Privacy is a fundamental human right.

National cultures and the way of life influence the practice of privacy. Although this issue is important in Western societies, it may have lesser importance in other cultures. Modern practices of privacy focus on communication privacy (no surveillance of communication) and information privacy (no handling of information about individuals). Privacy issues, which used to focus on governmental activities, have been extended and now include the business sector.

 # Online privacy

When you go online, you often entrust vital personal information, such as your name, address, and credit card number, to your Internet Service Provider and to the website you are using. What happens to this data? Could it fall into the wrong hands? What rights do you have regarding your personal information? European Commission has developed policies and directives in order to protect users online.

Common EU rules have been established to ensure that your personal data enjoys a high standard of protection everywhere in the EU. Since 2009, new requirements have been introduced and are being implemented by the Commission.

Under the EU Data Protection Directive, personal data can only be gathered under strict conditions and for a legitimate purpose. Organizations that collect and manage your personal information must also protect it from misuse and respect certain rights. In 2012, the European Commission proposed a major reform of the EU legal framework on the protection of personal data. The new proposals will strengthen individual rights and tackle the challenges of globalisation and new technologies.

In particular, new requirements were introduced on data such as "cookies" and on personal data breaches:

Informed consent for "cookies" and other devices: the new rules require Member States to ensure users have given their consent when data such as cookies (small text files stored by a user's web browser) is stored and accessed in their computer, smartphone or other device connected to the Internet.

Personal data breaches: telecoms operators and Internet Service Providers normally hold a range of data about their customers. In general, providers are required to keep this data confidential and secure. However, sometimes the data can be stolen or lost, or someone could gain unauthorized access to it. Under the new rules, the provider has to report such "personal data breaches"

to the national authority and inform the subscriber or individual directly if there is a risk to personal data or privacy.

 # Recommendations: what steps can I take to protect my privacy online?

The internet offers many opportunities and have a lot of useful information and resources that are available at your fingertips. Use these precautions to make your web surfing experience a safe and enjoyable one.

Before you enter personally identifying information like your name, email address, credit card info, and other similar sensitive information, check to see if the website has a privacy policy page. If it is missing a privacy page, leave the site and find a similar site or service that has a policy protecting your personal information. Don't take the risk of identity theft or worse with untrusted or shady sites. If they didn't bother to formulate and enforce a privacy policy, they aren't worth trusting with your sensitive information.

Do not leave personal information that you aren't comfortable disclosing. If you feel the information being requested is way too intrusive or personal or irrelevant to the service or content you're trying to get from the site, leave the website and try to find a similar website that asks fewer prying questions.

When using social networking sites or forums or chat sites, make sure to put some thought into what you're posting. Search engines are extremely powerful and can dig up random posts and messages on the internet. If you don't want your identity know when posting to public forums or publicly accessible areas, use a newly created email address and account with no personally identifying information.

If you're using an "always on" network connection, make sure to install and maintain a firewall. Firewall software prevents your computer from hacking and remote attacks.

Manage your passwords responsibly. Do not use the same password among all websites you join. Make sure that the password you use for encrypted or secure sites are different from less secure sites you visit. Don't use the same password you

use for your credit cards or bank accounts for your online accounts and vice versa.

The purpose of this website is to provide you with simple and clear information on how cookie technology helps both website users and website owners to enjoy all the opportunities the Internet offers. We would like to hear from you and your feedback on how we can improve this website and provide better information to all our visitors. Please click here to submit your feedback on this site.

 # What other steps can I take to protect my privacy online?

The internet is a powerful tool that used correctly is safe, easy and fast. So let your fingers do the hard work while you sit back and browse through a virtual library or high street from the comfort of your keyboard. But do be mindful and take a few basic precautions.

Before entering any personal data such as email address, credit card details, check the privacy policy of the site you are visiting. If there is no privacy policy, go elsewhere.

Do not provide more personal data than you are comfortable with. If you feel the questions are too intrusive, go elsewhere.

Think before putting your personal details on a public site such as a bulletin board or chat room. Set up a different email address for such uses.

Where you are permanently connected to the internet use a firewall to protect your computer and personal information from online attacks.

Be Smart with passwords. Don't use the same password on an unsecured site that is used on a secured site. Don't use the same password for voice mail at work or at home. Don't use credit or debit card PIN number as a password.

Human rights online

A basic set of Internet-related human rights includes privacy; freedom of expression; the right to receive information; various rights protecting cultural, linguistic and minority diversity; and the right to education. It is not surprising that human-rights-related issues have very often been debated. While human rights are usually explicitly addressed, they are also involved in cross-cutting issues appearing when dealing with net neutrality (right to access, freedom of expression, anonymity), cyber security (observing human rights while carrying out cyber security and protection activities), content control, etc.

 # Activities of the Council of Europe on human rights and the Internet

One of the main players in the field of human rights and the Internet is the CoE. The CoE is the core institution dealing with pan-European human rights, with the Convention for the Protection of Human Rights and Fundamental Freedoms as its main instrument. Since 2003, the CoE has adopted several declarations highlighting the importance of human rights on the Internet.

The CoE is also the depository of the Convention on Cybercrime as the main global instrument in this field. This may position it as one of the key institutions in finding the right balance between human rights and cybersecurity considerations in the future development of the Internet.

The Council of Europe is promoting an Internet based on its core values and objectives, namely human rights, pluralist democracy and the rule of law; developing Europe's cultural identity and diversity; finding common solutions to the challenges facing European society; and consolidating democratic stability in Europe.

Human rights, democracy and the rule of law on the Internet: a Council of Europe priority

1. The Internet has become an essential tool for many people in their everyday vlives. It is imperative that people can use the Internet with freedom and confidence. The most effective way to achieve this is through the promotion and respect of the Council of Europe's core values on the Internet with regard to its use and governance.

2. An open, inclusive, safe and enabling environment must go hand in hand with a maximum of rights and services subject to a minimum of restrictions and a level of security which users are entitled to expect. Freedom of expression and information regardless of frontiers is an overarching requirement because it acts as a catalyst for the exercise of other rights, as is the need to address threats to the rule of law, security and dignity.

3. The Council of Europe fully supports the multi-stakeholder model of Internet governance which ensures that the Internet remains universal, open and innovative, and continues to serve the interests of users throughout the world.

Right to access the Internet

Finland is the first country to legally guarantee the right to access the Internet. As of July 2010 all citizens in Finland have the right to a one-megabit broadband connection.2 Yet the right to Internet access is argued more in relation to the freedom of expression and information than the actual speed of Internet connection. And opinions are still nuanced regarding a firm worldwide recognition of the access to Internet as a human right, since access involves different valences – from access to infrastructure to access to content.

Still, there are reluctant opinions to considering broadband as a basic human right, when there are people still fighting for clean water, medical attention, and food.

Hate speech online

Definition of hate speech:

The term hate speech shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin, but not restricted to this.

Hate speech targets

There are a lot of groups that are targets of hate speech on-line – mainly on social media, but also on forums or in the comment sections of on-line newspapers. Some groups that are affected the most by hate speech on-line are: ethnic minorities (for example Roma people), sexual minorities (LGBTIQ), immigrants, religious groups, violence victims, people with diffabilities (different abilities) and people with fewer opportunities.

Causes for hate speech on line

Main causes for hate speech online are: lack of education (people that don't have enough knowledge about certain issues tend to discriminate the groups that they have a wrong image of), prejudices and stereotypes, bad economic situation (in times of crisis people tend to look for people that can be blamed for the bad economic conditions), cultural background (all of us are brought up in a different way and they inherit thinking patterns of their families).

Scale of the problem

With the growth of the internet and social media the problem of hate speech is growing very fast. Internet is a place where people can share their opinions freely – that is why sometimes, feeling anonymous, they post things that are offensive and harassing for others.
For more information check: http://www.nohatespeechmovement.org/

How to be active online?

In the modern age, technology is the backbone of any activist. Well-designed tools will make people be more active online and share information easily and efficiently, make well-informed decisions, and easily expand as they try to approach their audience.

The tools that online activists are using are part of electronic communication technologies such as social media, especially Twitter and Facebook, YouTube, e-mail, and podcasts for various forms of activism to enable faster communications by citizen movements and the delivery of local information to a large audience. Internet technologies are used for cause-related fundraising, community building, lobbying, and organizing. But being active online all the time and running a campaign is one of the most challenging and exhausting activities possible. Running a typical campaign will mean more long work days for several days or months. For one person is nearly impossible so Organizations and NGO must have supporters and people that have faith in the cause of the large campaigns. The ideal system is one that can manage all your campaign needs, from accounting, to tracking volunteers, calendaring events, to generating detailed financial reports.

There are a lot of theories and practices how to be more active online or to run a successfully campaign. The right strategy of the smaller campaign is to focus. According to experts there are some steps that an online activist must follow.

Steps:

Setting your goals is the first step. Why you want to be active online or who your audience is.

Knowledge and becoming an expert is the next one. Detailed information, facts, figures about the cause of the campaign.

Create resource pool. Find people who want to help you with the campaign, online or offline. People that can offer advice or recourses. People that often want to be more active online often recruit advocates and allies to help to promote their cause.

There are a lot of ways when your online to get our message across – sometimes it's the simplest ideas that will make the most impact.
Effectively communicating any campaign message is the most effective thing that active online user can do to achieve the goals.
Whatever is the cause of a campaign, no matter of its scale, team running it must have faith and to be truly active online in order to succeed in the goal

European Youth Forum in its Policy paper on New media and Internet Governance states:

"A new threat of social exclusion and discrimination is emerging where equal access to digital media literacy is not ensured for all young people. This calls for policies aimed at equipping young people with adequate skills and securing informed access to the internet and new media for them. It is important that digital media literacy is mainstreamed at all levels of formal and non-formal education, including a lifelong learning approach.

Digital skills showcase the importance of the right mix of generic competences and technical skills, ranging from informally acquired functional digital skills to specialist skills. Digital and media literacy will therefore be crucial both for private and professional life and, although it is almost universally true that any job will require some level of e-skills, the aim should be digital fluency. "

Guidelines for good behavior online:

There is no space for curses, insults, humiliation or discrimination on the internet.
Linking your own status or profile picture is same as calling yourself on your mobile phone.
TYPING WITH CAPITAL LETTERS IS THE SAME AS YOU SHOUT AT SOMEONE'S FACE. Keep calm and underline someting if it is that important.
Internet is not a "fight platform". You are a coward if you use anonymous profile or humiliate.
Posting wise quotes every 2 minutes on your profile does not make you wiser.
Behave as you do in real life.
Try using proper grammar when it comes to language. Not everyone can un derstand your slang.
Do not face abusive users by joining the argue. Avoid direct confrontation – re port, ignore or argument wisely.
Social networks are not a diary. It has no locker and everyone can read it to anyone at any time.
Respect and you will gain respect.

Sources:

http://www.diplomacy.edu/IGBook
https://www.internetsociety.org/sites/default/files/GIUS2012-GlobalData-Table-20121120_0.pdf
http://ec.europa.eu/digital-agenda/en/online-privacy
www.wikipedia.org
https://www.internetsociety.org/sites/default/files/GIUS2012-GlobalData-Table-20121120_0.pdf

This Manual has been developed
as part of New Media Summer School 2013

"WEB OF/FOR PEACE - YOUNG PEOPLE'S SAY IN INTERNET GOVERNANCE"

held in Lisbon, Portugal as youth event prior to EuroDIG.

SUPPORTED BY: European Youth Foundation www.eyf.coe.int

Google www.google.com

PARTNER ORGANIZATIONS:
Youth for Exchange and Understanding / www.yeu-international.org
European Students Forum - AEGEE / www.aegee.org
Federation of Young European Greens / www.fyeg.org
Young European Federalists / www.jef.org
European Youth Forum / www.youthforum.org