AN INTRODUCTION TO

INTERNET GOVERNANCE

Jovan Kurbalija

4th Edition

The history of this book is long, in Internet time. The original text and the overall approach, including the five-basket methodology, were developed in 1997 for a training course on Information and Communications Technology (ICT) Policy for government officials from Commonwealth countries.

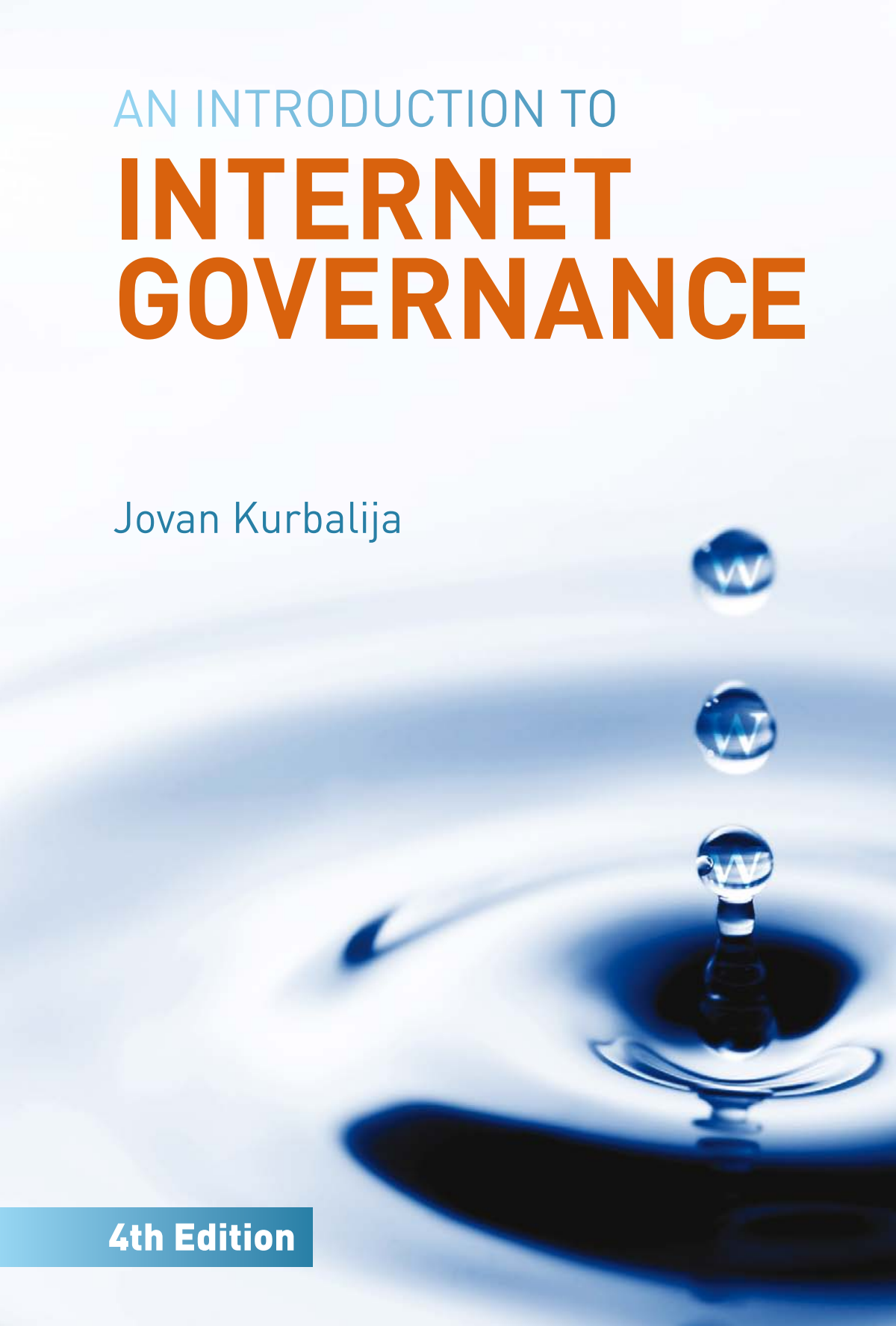
In 2004, Diplo published a print version of its Internet governance materials, in a booklet entitled *Internet Governance – Issues, Actors and Divides*. This booklet formed part of the *Information Society Library*, a Diplo initiative driven by Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija. Special thanks are due to Eduardo Gelbstein, who made substantive contributions to the sections dealing with cybersecurity, spam, and privacy, and to Vladimir Radunovic and Ginger Paque who updated the course materials. Comments and suggestions from other colleagues are acknowledged in the text. Stefano Baldi, Eduardo Gelbstein, and Vladimir Radunovic all contributed significantly to developing the concepts behind the illustrations in the book.

In 2008, a special, revised version of the book, entitled simply *An Introduction to Internet Governance*, was published in cooperation with NIXI-India on the occasion of the Internet Governance Forum 2008 held in Hyderabad, India. In 2009, a revised third edition was published in the cooperation with the Ministry of Communication and Information Technology of Egypt *Internet Governance* is now in its fourth edition (2010), which has been produced with support from the Secretariat of the ACP Group of Countries and the European Union.

AN INTRODUCTION TO

INTERNET GOVERNANCE

Jovan Kurbalija



4th Edition

Published by DiploFoundation (2010)

Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 13, Malta

Switzerland: DiploFoundation
Rue de Lausanne 56
CH-1202 Genève 21, Switzerland

E-mail: diplo@diplomacy.edu

Website: http://www.diplomacy.edu

Cover: the Argument by Design

Editing: Mary Murphy

Illustrations: Zoran Marcetic – Marča & Vladimir Veljašević

Layout & Prepress: the Argument by Design

Printing: Akaprint Nyomdaipari Kft

ISBN: 978-99932-53-23-5

Contents

Foreword

In 2004, when I told my friends what I was doing as a member of WGIG – the Working Group on Internet Governance, they often called on me to fix their printers or install new software. As far as they were concerned, I was doing something related to computers. I remember taking a quick poll of my fellow WGIG members asking them how they explained to their friends, partners, and children what they were doing. Like me, they too were having difficulty. This is one of the reasons I started designing and preparing Diplo's first text and drawings related to Internet governance.

Today, just six years later, the same people who asked me to install their printers are coming back to me with questions about how to protect their privacy on Facebook or how to ensure their children can navigate the Internet safely. Some are even asking whether the apparently fraught relationship between China and Google or the frequent talk of a cyberwar have anything to do with Internet governance. How far we all have come!

Internet governance is moving increasingly into the public eye. The more modern society depends on the Internet, the more relevant Internet governance will be. Far from being the remit of some select few, Internet governance concerns all of us to a lesser or greater extent, whether we are one of the 2 billion using the Internet or a non-user who depends on the facilities it services.

Internet governance is obviously more relevant for those who are deeply integrated in the e-world, whether through e-business or simply networking on Facebook. Yet it has a broad reach. Government officials, military personnel, lawyers, diplomats, and others who are involved in either providing public goods or preserving public stability are also concerned. Internet governance, and in particular the protection of privacy and human rights, is a focal point for civil society activists and non-governmental organisations. For academia and innovators worldwide, Internet governance must ensure that the

Internet remains open for development and innovation. Creative inventors of tomorrow's Google, Skype, Facebook, and Twitter are out there, somewhere, browsing the Net. Their creativity and innovativeness should not be stifled; rather should they be encouraged to develop new, more creative ways to use the Internet. One of the main objectives of Internet governance is to create a pro-development policy environment, which should enable further use of the Internet as an engine of development.

It is my hope that this book provides a clear and accessible introduction to Internet governance. For some of you, it will be your first encounter with the subject. For others, it may serve as a reminder that what you are already doing in your area of specialisation – be it e-health, e-commerce, e-governance, or e-whatever – is part of the broader family of Internet governance issues.

The underlying objective of such a diverse approach is to modestly contribute towards preserving the Internet as an integrated and enabling medium for billions of people worldwide. At the very least, I hope it whets your appetite and encourages you to delve deeper into this remarkable and fluent subject. Stay current. Follow developments on http://www.diplomacy.edu/isl/ig/

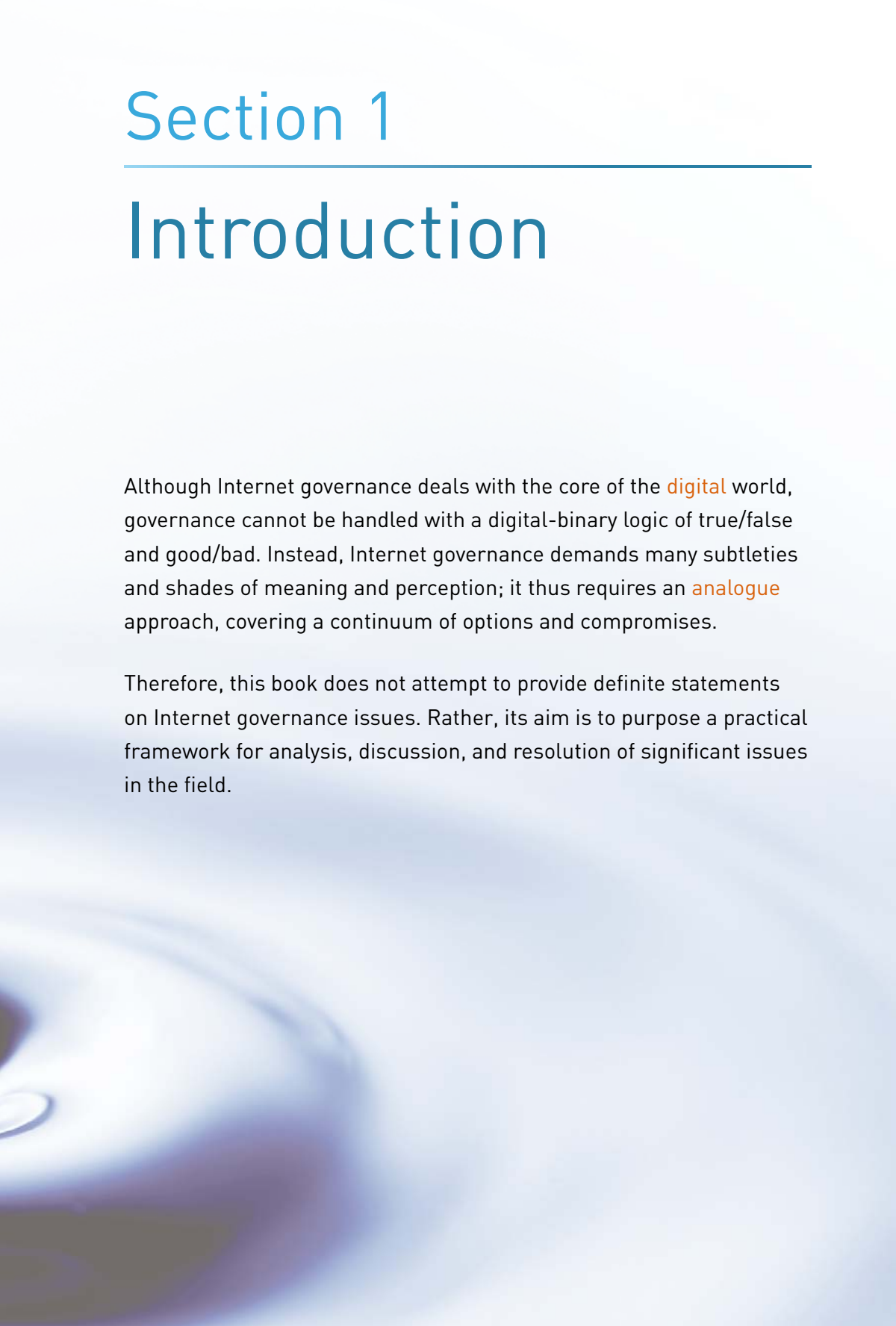
Jovan Kurbalija
DiploFoundation
August 2010

Section 1

Introduction

Although Internet governance deals with the core of the digital world, governance cannot be handled with a digital-binary logic of true/false and good/bad. Instead, Internet governance demands many subtleties and shades of meaning and perception; it thus requires an analogue approach, covering a continuum of options and compromises.

Therefore, this book does not attempt to provide definite statements on Internet governance issues. Rather, its aim is to purpose a practical framework for analysis, discussion, and resolution of significant issues in the field.



Introduction

The controversy surrounding Internet governance starts with its definition. It's not merely linguistic pedantry. Different perspectives of the meaning of Internet governance trigger different policy approaches and expectations. For example, telecommunication specialists see Internet governance through the prism of the development of technical infrastructure. Computer specialists focus on the development of different standards and applications, such as XML (eXtensible Markup Language) or Java. Communication specialists stress the facilitation of communication. Human rights activists view Internet governance from the perspective of freedom of expression, privacy, and other basic human rights. Lawyers concentrate on jurisdiction and dispute resolution. Politicians worldwide usually focus on issues that resonate with their electorates, such as techno-optimism (more computers = more education) and threats (Internet security, child protection). Diplomats are mainly concerned with the process and protection of national interests. The list of potentially conflicting professional perspectives of Internet governance goes on.

What does Internet governance mean?

The World Summit on the Information Society (WSIS)[1] came up with the following working definition of Internet governance:

> *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.*[2]

This, rather broad, working definition does not resolve the question of different interpretations of two key terms: 'Internet' and 'governance'.

'I'nternet or 'i'nternet and diplomatic signalling

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 question of writing Internet/internet with an upper or lowercase 'i' re-emerged at the International Telecommunication Union (ITU) Conference in Antalya (November, 2006) where a political dimension was introduced when the term 'Internet' appeared in the ITU resolution on Internet governance with a lowercase 'i' instead of the usual, uppercase 'I'. David Gross, the US ambassador in charge of Internet governance, expressed concern that the ITU lowercase spelling might signal an intention to treat the Internet like other telecommunication systems internationally governed by ITU. Some interpreted this as a diplomatic signal of ITU's intention to play a more prominent role in Internet governance.[3]

Internet

Some authors argue that 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. The already ubiquitous Internet continues to expand at a rapid rate, not only in terms of the number of users but also in terms of the services that it offers, notably Voice-over Internet Protocol (VoIP), which may displace conventional telephony.

Governance

In the Internet governance debate, especially in the early phase of WSIS-2003, controversy arose over the term 'governance' and its various interpretations. According to one interpretation, governance is synonymous with government. Many national delegations had this initial understanding, leading to the interpretation that Internet governance should be the business of governments and consequently addressed at inter-governmental level with the limited participation of other, mainly non-state, actors.[4] 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, efficacité 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)*.

The evolution of Internet governance

Early Internet governance (1970s–1994)

The Internet started as a government project. In the late 1960s, the US government sponsored the development of the Defense Advanced Research Project Agency Network (DARPA Net), a resilient communication resource. By the mid-1970s, with the invention of TCP/IP (Transmission Control Protocol/Internet Protocol), this network evolved into what is known today as the Internet. One of the key principles of the Internet is its distributed nature: data packets can take different paths through the network, avoiding traditional barriers and control mechanisms. This technological principle was matched by a similar approach to regulating the Internet in its early stages: the Internet Engineering Task Force (IETF), established in 1986, managed the further development of the Internet through a cooperative, consensus-based, decision-making process, involving a wide variety of individuals. There was no central government, no central planning, and no grand design.

This led many people to think that the Internet was somehow unique and that it could offer an alternative to the politics of the modern world. In his famous Declaration of the Independence of Cyberspace, John Perry Barlow said:

> *[the Internet] is inherently extra-national, inherently anti-sovereign and your [states'] sovereignty cannot apply to us. We've got to figure things out ourselves.*[5]

The DNS war (1994–1998)

This decentralised approach to Internet governance soon began to change as governments and the business sector realised the importance of the global

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 commercialisation 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 cybersecurity issues. ITU named its initiative in this field the Global Cybersecurity Agenda. The word virtual rarely appears in international documents. The prefix e- has garnered particular favour in the EU, where it describes various policies related to e-science and e-health. During the WSIS process, e- was introduced at the Pan-European Bucharest Regional Meeting and became predominant in all WSIS texts, including the final documents. WSIS implementation is centred on action lines including e-government, e-business, e-learning, e-health, e-employment, e-agriculture, and e-science.

network. In 1994, the US National Science Foundation, which managed the key infrastructure of the Internet, decided to subcontract the management of the Domain Name System (DNS) to a private US company called Network Solutions Inc. (NSI). This was not well received by the Internet community and led to the so-called 'DNS war'.

This 'war' brought new players into the picture: international organisations and nation states. It ended in 1998 with the establishment of a new organisation, the Internet Corporation for Assigned Names and Numbers (ICANN). Since then, the debate on Internet governance has been characterised by the more intensive involvement of national governments.

The Word Summit on the Information Society (2003–2005)

WSIS, held in Geneva (2003) and Tunis (2005) officially placed the question of Internet governance on diplomatic agendas. The focus of the Geneva phase of the summit, preceded by a number of Preparatory Committees (PrepComs) and regional meetings, was rather broad, with a range of issues related to information and communication put forward by participants. In fact, during the first preparatory and regional meetings, the term 'Internet', let alone 'Internet governance', was not used.[6] Internet governance was introduced to

the WSIS process during the West Asia regional meeting in February 2003, after the Geneva summit became the key issue of the WSIS negotiations.

After prolonged negotiations and last-minute arrangements, the WSIS Geneva summit agreed to establish the Working Group on Internet Governance (WGIG). WGIG prepared a report which was used as the basis for negotiations at the second WSIS Summit held in Tunis (November, 2005). The WSIS Tunis Agenda for the Information Society elaborated on the question of Internet governance, including adopting a definition, listing Internet governance issues, and establishing the Internet Governance Forum (IGF), a multistakeholder body convoked by the UN Secretary General.

Developments in 2006

After the Tunis Summit, three main developments and events marked the Internet governance debate in 2006. First was the expiration of the existing Memorandum of Understanding (MoU) and the establishment of a new one between ICANN and the US Department of Commerce. Some had hoped that this event would change the relationship between ICANN and the US government and that the former would become a new type of international organisation. However, while the new MoU made the umbilical cord between ICANN and the US government thinner, it maintained the possibility of the eventual internationalisation of ICANN's status.

The second event of 2006 was the IGF in Athens. It was the first such forum and, in many respects, it was an experiment in multilateral diplomacy. The Forum was truly multistakeholder. All players – states, businesses, and civil society – participated on an equal footing. It also had an interesting organisational structure for its main events and workshops. Journalists moderated the discussions and the Forum therefore differed from the usual UN-style meeting format. However, some critics claimed that the Forum was only a 'talk show' without any tangible results in the form of a final document or plan of action.

The third main development in 2006 was the ITU Plenipotentiary Conference held in Antalya, Turkey, in November. A new ITU Secretary-General, Dr Hamadoun Touré, was elected. He announced a stronger focus on cybersecurity and development assistance. It was also expected that he would introduce new modalities to the ITU approach to Internet governance.

Developments in 2007

In 2007, the ICANN discussion focused on .xxx domains (for adult materials), re-opening debates on numerous governance points, including whether ICANN should deal only with technical problems or also with issues having public policy relevance.[7] Interventions by the USA and other governments pertaining to .xxx domains further raised the question of how national governments should become involved in ICANN deliberations. At the second IGF, held in November in Rio de Janeiro, the main development was adding critical Internet resources (names and numbers) to the IGF agenda.

Developments in 2008

The major development of 2008, which will continue to influence Internet governance as well as other policy spheres, was the election of Barack Obama as US President. During his presidential election campaign, he used the Internet and Web 2.0 tools intensively. Some even argue that this was one of the reasons for his success. His advisors include many people from the Internet industry, including the CEO of Google. In addition to his techno-awareness, President Barack Obama supports multilateralism which will inevitably influence discussion on the internationalisation of ICANN and the development of the Internet governance regime.

See Section 2 for further discussion on network neutrality

In 2008, network neutrality[8] emerged as one of the most important Internet governance issues. It was mainly discussed in the USA between two main opposing blocks. It even featured in the US presidential campaign, supported by President Obama. Network neutrality is mainly supported by the so-called Internet industry including companies such as Google, Yahoo! and Facebook. A change in the architecture of the Internet triggered by a breach in network neutrality might endanger their business. On the other side sit telecommunication companies, such as Verizon and AT&T, Internet service providers (ISPs), and the multimedia industry. For different reasons, these industries would like to see some sort of differentiation in packets travelling on the Internet.

Another major development was the fast growth of Facebook and social networking. When it comes to Internet governance, the increased use of Web 2.0 tools opened up the issue of privacy and data protection on Facebook and similar services.

Developments in 2009

The first part of 2009 saw the Washington Belt trying to figure out the implications and future directions of President Obama's Internet-related policy. Obama's appointments to key Internet-related positions did not bring any major surprises. They followed his support for an open Internet. His team also pushed for the implementation of the principle of network neutrality in accordance with promises made during his election campaign.

The highlight of 2009 was the conclusion of the Affirmation of Commitments between ICANN and the US Department of Commerce, which should make ICANN a more independent organisation. While this move solved one problem in Internet governance – the US supervisory role of ICANN – it opened many new issues, such as the international position of ICANN, and the supervision of ICANN's activities. The Affirmation of Commitments provides guidelines, but leaves many issues to be addressed in the forthcoming years.

In November 2009, the fourth IGF was held in Sharm el Sheikh, Egypt. The main theme was the IGF's future in view of the 2010 review of its mandate. In their submissions, stakeholders took a wide range of views on the future of the IGF. While most of them supported its continuation, there were major differences of opinion as to how the future IGF should be organised. China and many developing countries argued for the stronger anchoring of the IGF in the UN system, which would imply a more prominent role for governments. The USA, most developing countries, the business sector, and civil society argued for the preservation of the current IGF model.

Developments in 2010

As of August 2010, the main Internet governance issues are related to the growing importance of social media platforms such as Facebook and Twitter. One of the main questions is the protection of privacy of users of these platforms. In what can be labelled 'Internet geo-politics', the main development was State Secretary Hilary Clinton's speech on the freedom of expression on the Internet, in particular in relation to China.[9] Google and Chinese authorities conflicted over the restricted access to Google-search in China. It led to the closing of Google's search operations in the country.

There were two important developments in the ICANN world. First was the introduction of the first non-ASCII domain names for Arabic and Chinese. By solving the problem of domain names in other languages, ICANN reduced the risk of disintegration of the Internet DNS. Second was ICANN's approval of the .xxx domain (adult materials). With this decision ICANN formally

crossed the Rubicon by officially adopting a decision of high relevance for public policy on the Internet. Previously, ICANN tried to stay, at least formally, within the realm of making only technical decisions.

The IGF review process started in 2010 with the UN Commission on Science and Development adopting the resolution on the continuation of the IGF, which suggests continuation for the next five years, with only minor changes in its organisation and structure. In July 2010, the UN Economic and Social Council (UNECOSOC) endorsed this resolution. The final decision on the continuation of the IGF will be made during the UN General Assembly in the autumn of 2010.

The Internet Governance Cognitive Toolkit

> *Profound truths are recognised by the fact that the opposite is also a profound truth, in contrast to trivialities where opposites are obviously absurd.*
>
> **Niels Bohr, Atomic Physicist (1885–1962)**

The Internet Governance Cognitive Toolkit is a set of tools for developing policy and preparing policy argumentation. It has numerous practical functions for those involved in Internet governance. It helps navigate the vast amount of information, documents, and studies on Internet governance, and also helps in developing policy narrative and understanding of other policy approaches.

Ultimately, the Toolkit improves the quality of negotiations by increasing opportunities for inclusiveness and solutions based on compromise. It deals with the growing Internet governance regime, which is still in the very early stages of its development. Experience from other international regimes (e.g. environment, air transport, arms control) has shown that such regimes first tend to develop a common reference framework, including values, perception of cause-and-effect relationships, modes of reasoning, terminology, vocabulary, jargon, and abbreviations. This reference framework is highly relevant in political life. It shapes how particular issues are framed and what actions are taken.

In many cases, the common reference framework is influenced by the specific professional culture (the patterns of knowledge and behaviour shared by members of the same profession). The existence of such a framework usually helps in facilitating better communication and understanding. It can also be

used to protect one's professional turf and prevent outside influence. To quote American linguist, Jeffrey Mirel, 'All professional language is turf language.'

The Internet governance regime is complex as it involves many issues, actors, mechanisms, procedures, and instruments. The figure above, inspired by the Dutch artist M.C. Escher, demonstrates some of the paradoxical perspectives associated with Internet governance.

The Toolkit reflects the nature of Internet governance, as a so-called 'wicked policy' area, characterised by a broad range of catalysts as well as the difficulty encountered in assigning causation for policy development to one specific reason. In many cases, every problem is a symptom of another one, sometimes creating vicious circles. Certain cognitive approaches, such as linear, mono-causal and either/or thinking, have a very limited utility in the field of Internet governance. Internet governance is too complex to be strapped inside a corset of coherence, non-contradiction, and consistency. Flexibility, and being open and prepared for the unexpected, might be the better part of Internet governance valour.[10]

Like the Internet governance process, the Toolkit is also in flux. Approaches, patterns, guiding principles, and analogies emerge and disappear depending on their current relevance in the policy process.

Approaches and patterns

Internet governance as a whole, as well as specific Internet governance issues, have been a part of policy discussions and academic exchanges for some time. A number of approaches and patterns have gradually emerged, representing points where differences in negotiation positions as well as in professional and national cultures can be identified. Identifying common approaches and patterns may reduce the complexity of negotiations and help to create a common reference framework.

Narrow vs broad approach

A debate on a narrow *vs* broad approach to Internet governance has taken centre stage so far, reflecting different approaches and interests in the process.

The narrow approach focuses on the Internet infrastructure (DNS, IP numbers, and root servers) and on ICANN's position as the key actor in this field. According to the broad approach, Internet governance negotiations should go beyond infrastructural points and address other legal, economic, developmental, and sociocultural issues. This latter approach is adopted in the WGIG Report and the WSIS Concluding Document. It is also used as the underlying principle of IGF architecture.

Distinguishing between these two approaches was particularly important during the WSIS negotiations. However, it was not completely resolved by the end of the WSIS process. The discussions at the IGF in Rio de Janeiro (November, 2007) clearly highlight that the broad approach does not mean that discourse should be vague. The IGF in Rio decided to return to the question of core Internet resources (so-called 'ICANN issues') in the Forum agenda.

Technical and policy coherence

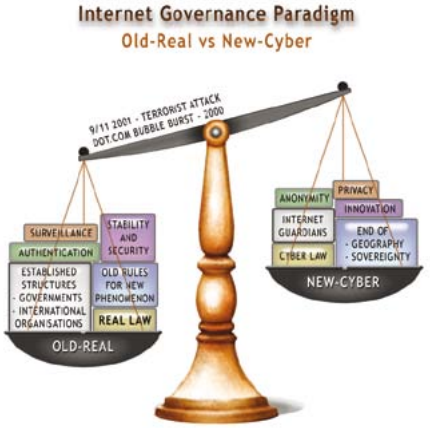
A significant challenge facing the Internet governance process has been the integration of technical and policy aspects, as it is difficult to draw a clear distinction between the two. Technical solutions are not neutral. Ultimately, each technical solution/option promotes certain interests, empowers certain groups, and, to a certain extent, impacts social, political, and economic life.

In the case of the Internet, for a long time both the technical and the policy aspects were governed by just one social group – the early Internet community. With the growth of the Internet and the emergence of new stakeholders in the

1990s – mainly the business sector and governments – there was no longer an integrated coverage of technical and policy issues under one roof by the Internet community. Subsequent reforms, including the creation of ICANN, have tried to re-establish coherence between technical and policy aspects. This issue remains open, and as expected, has shown to be one of the controversial topics at the IGF debate.

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

There are two approaches to almost every Internet governance issue. The 'old-real' approach – think 'new wine in old bottles' – 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. Cyberspace 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.

Decentralised vs centralised structure of Internet governance

According to the decentralised view, the Internet governance structure 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 international organisation, and that decentralised governance is one of the major factors allowing fast Internet growth. This view is mainly supported by the Internet's technical community and developed countries.

The centralised approach, on the other hand, is partly based on the practical difficulty of countries with limited human and financial resources to follow Internet governance discussions in a highly decentralised and multi-institutional setting. Such countries find it difficult to attend meetings in the main diplomatic centres (Geneva, New York), let alone to follow the activities of other institutions, such as ICANN, W3C (World Wide Web Consortium), and IETF. These mainly developing countries argue for a one-stop shop, preferably within the framework of an international organisation.

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.

See Section 2 for further discussion on network neutrality

Geography and the Internet

One of the early assumptions regarding the Internet was that it overcame national borders and eroded the principle of sovereignty. With Internet communication easily transcending national borders and user anonymity embedded in the very design of the Internet, it seemed to many, to quote the famous Declaration of the Independence of Cyberspace,[11] that governments had 'no moral right to rule us [users]' nor 'any methods of enforcement we have true reason to fear'.

Technological developments of the recent past, however, including more sophisticated geo-location software, increasingly challenge the view of the end of geography in the Internet era. Today, it is still difficult to identify exactly who is behind the screen but it is fairly straightforward to identify through which ISP the Internet is accessed.

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

Policy uncertainty

The Internet governance debate is conducted in the context of high uncertainty regarding the future technical development of the Internet, and this uncertainty has affected the Internet governance agenda. For example, in 2002 when the WSIS process started,[12] Google was just one of many search engines. At the end of the process in November 2005, Google was established as the primary company shaping Internet use. In 2002, the use of blogs was in its infancy. Today, bloggers sway governments, push the limits of freedom of expression, and have considerable influence on social and economic life. The list of technological developments with relevance for Internet governance includes Facebook, Skype, YouTube, Twitter, and Wiki.

Today, many think that the traditional core Internet governance issues (ICANN-related issues) are gradually losing relevance in comparison to questions regarding network neutrality, the convergence of different technologies (e.g. telephony, TV, and the Internet), and governance issues regarding social networking (Facebook and Twitter) as well as the role of Google and Wikipedia as gatekeepers of digitalised knowledge and information.

Policy balancing acts

Balance is probably the most appropriate graphical illustration of Internet governance and policy debates. 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

Policy balancing acts in history

Back in 1875, the International Telegraph Union (predecessor of today's ITU) held a conference in St Petersburg, which influenced the future development of the telegraph. One of the most controversial issues was the control of the content of telegraph communication. While the conference participants from the USA and the UK promoted the principle of privacy of telegraph correspondence, Russia and Germany insisted on limiting this privacy in order to protect state security, public order, and public morality. A compromise was reached through an age-old diplomatic technique – diplomatic ambiguity. While Article 2 of the St Petersburg Convention guaranteed the privacy of telegraph communication, Article 7 limited this privacy and introduced the possibility of state censorship. The USA refused to sign the Convention because of the censorship article.

Rights has been extended to the Internet. It is very often discussed in the context of content control and censorship on the Internet.

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

See Section 2 for further discussion on cybersecurity

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

See Section 3 for further discussion on intellectual property

Many criticise these 'balancing pairs' considering them false dilemmas. For example, there are strong arguments that more cybersecurity does not necessarily mean less privacy. There are approaches towards enhancing both cybersecurity and privacy. While these views are strongly held, the reality of Internet governance policy is that it is shaped by the aforementioned 'binary' policy options.

Guiding principles

Guiding principles represent certain values and interests that are central to the emerging Internet governance regime. Some of those principles have been

adopted by WSIS, such as transparency and inclusiveness. Other principles have been introduced, mainly tacitly, through discussions on Internet governance.

Don't re-invent the wheel

Any initiative in the field of Internet governance should start from existing regulations, which can be divided into three broad groups:

1. those invented for the Internet (e.g. ICANN);
2. those that require considerable adjustment in order to address Internet-related issues (e.g. trademark protection, e-taxation); and
3. those that can be applied to the Internet without significant adjustments (e.g. protection of freedom of expression).

The use of existing rules would significantly increase legal stability and reduce the complexity of the development of the Internet governance regime.

If it ain't broke, don't fix it

Internet governance must maintain the current functionality and robustness of the Internet, yet remain flexible enough to adopt changes leading towards increased functionality and higher legitimacy. General consensus recognises that the stability and functionality of the Internet should be one of the guiding principles of Internet governance. The stability of the Internet should be preserved through the early Internet approach of 'running code', which involves the gradual introduction of well-tested changes in the technical infrastructure.

However, some actors are concerned that the use of the slogan 'if it ain't broke, don't fix it' will provide blanket immunity from any changes in the current Internet governance, including changes not necessarily related to technical infrastructure. One solution is to use this principle as a criterion for the evaluation of specified Internet-governance-related decisions (e.g. the introduction of new protocols and changes in decision-making mechanisms).

Promotion of a holistic approach and prioritisation

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

While maintaining a holistic approach to Internet governance negotiations, stakeholders should identify priority issues depending on their particular interests. Neither developing nor developed countries are homogenous groups. Among developing countries there are considerable differences in priorities, level of development, and IT-readiness (e.g. between ICT-advanced countries, such as India, China, and Brazil, and some least-developed countries in sub-Saharan Africa).

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

The principle of technological neutrality

According to the principle of technological neutrality, policy should not be designed for specific technological or technical devices. For example, regulations for the protection of privacy should specify what should be protected (e.g. personal data, health records), not how it should be protected (e.g. access to databases, crypto-protection). The use of the principle of technological neutrality makes a few privacy and data protection instruments, such as the Organisation for Economic Co-operation and Development (OECD) Guidelines from 1980, as relevant today as they were in 1980.

Technological neutrality provides many governance advantages. It ensures the continuing relevance of governance regardless of future technological developments and likely convergence of the main technologies (telecommunication, media, the Internet, etc.). Technological neutrality is different from network neutrality: the former indicates that particular policy is independent of the technology which it regulates; the latter focuses mainly on the neutrality of Internet traffic.

See Section 2 for further discussion on network neutrality

Make tacit technological solutions explicit policy principles

It is a view commonly held within the Internet community that certain social values, such as free communication, are facilitated by the way in which the Internet is technologically designed. For instance, the principle of network neutrality, according to which the network should merely transmit data between two endpoints rather than introduce intermediaries, is often acclaimed as a guarantee of free speech on the Internet. This view could lead to the erroneous conclusion that technological solutions are sufficient for promoting and protecting social values. The latest developments in the Internet, such as the use of firewall technologies for restricting the flow of information, prove that technology can be used in many, seemingly contradictory, ways. Whenever possible, principles such as free communication should be clearly stated at policy level, not tacitly presumed at technical level. Technological solutions should strengthen policy principles, but should not be the only way to promote them.

Avoid the risk of running society through programmers' code

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

Analogies

Though analogy is often misleading,
it is the least misleading thing we have.
Samuel Butler, British Poet (1835–1902)

Analogy helps us to understand new developments in terms of what is already known. Drawing parallels between past and current examples, despite its risks, is one of the key cognitive processes in law and politics. Most legal cases concerning the Internet are solved through analogies, especially in the Anglo-Saxon precedent law system.

The use of analogies in Internet governance has a few important limitations. First, 'Internet' is a broad term, which encompasses a variety of services, including e-mail (analogous to telephony), web services (analogous to broadcasting services – television), and databases (analogous to libraries). An analogy to any particular aspect of the Internet may over-simplify the understanding of the Internet.

Second, with the increasing convergence of different telecommunication and media services, the traditional differences between the various services are blurring. For example, with the introduction of VoIP, it is increasingly difficult to make a clear distinction between the Internet and telephony.

In spite of these limiting factors, analogies are still powerful; they are still the main cognitive tool for solving legal cases and developing an Internet governance regime.

Internet – telephony

Similarities: In the early Internet days, this analogy was influenced by the fact that the telephone was used for dial-up access to the Internet. In addition, a functional analogy holds between the telephone and the Internet (e-mail and chat), both being means for direct and personal communication.

Differences: The Internet uses packets instead of circuits (the telephone). Unlike telephony, the Internet cannot guarantee services; it can only guarantee a 'best effort'. The analogy highlights only one aspect of the Internet: communication via e-mail or chat. Other major Internet applications, such as the World Wide Web, interactive services, etc., do not share common elements with telephony.

The postal system and ICANN

Paul Twomy, former CEO of ICANN, used the following analogy between the postal system and ICANN's function: *If you think of the Internet as a post office or a postal system, domain name and IP addressing are essentially ensuring that the addresses on the front of an envelope work. They are not about what you put inside the envelope, who sends the envelope, who's allowed to read the envelope, how long it takes for the envelope to get there, what is the price of the envelope. None of those issues are important for ICANN's functions. The function is focusing on just ensuring that the address works.*

Used by: This analogy is used by those who oppose the regulation of Internet content (mainly in the United States). If the Internet were analogous to the telephone, the content of Internet communication could not be controlled, as is the case with the telephone. It is also used by those who argue that the Internet should be governed like other communication systems (e.g. telephony, post), by national authorities with a coordinating role of international organisations, such as ITU. According to this analogy, the Internet DNS should be organised and managed like the telephony numbering system.[13]

Internet – mail/post

Similarities: There is an analogy in function, namely the delivery of messages. The name itself, e-mail, highlights this similarity.

Differences: This analogy covers only one Internet service: e-mail. Moreover, the postal service has a much more elaborate intermediary structure between the sender and recipient than the e-mail system, where the active intermediary function is performed by ISPs or an e-mail service provider like Yahoo! or Hotmail.

Used by: The Universal Postal Convention draws this analogy between mail and e-mail: 'Electronic mail is a postal service which uses telecommunications for transmitting.' This analogy can have consequences concerning the delivery of official documents. For instance, receiving a court decision via e-mail would be considered an official delivery.

The families of US soldiers who died in Iraq have also attempted to make use of the analogy between mail (letters) and e-mail in order to gain access to their loved ones' private e-mail and blogs, arguing that they should be allowed to inherit e-mail and blogs as they would letters and diaries.

ISPs have found it difficult to deal with this highly emotional problem. Instead of going along with the analogy between letters and e-mail, most ISPs have denied access based on the privacy agreement they had signed with their users.

Internet – television

Similarities: The initial analogy was related to the physical similarity between computers and television screens. A more sophisticated analogy draws on the use of both media – web and TV – for broadcasting.

Differences: The Internet is a broader medium than television. Aside from the similarity between a computer screen and a TV screen, there are major structural differences between them. Television is a one-to-many medium for broadcasting to viewers, while the Internet facilitates many different types of communication (one-to-one, one-to-many, many-to-many).

Used by: This analogy is used by those who want to introduce stricter content control to the Internet. In their view, due to its power as a mass media tool similar to television, the Internet should be strictly controlled. The US government attempted to use this analogy in the seminal Reno *vs* ACLU case. This case was prompted by the Communication Decency Act passed by Congress, which stipulates strict content control in order to prevent children from being exposed to pornographic materials via the Internet. The court refused to recognise the television analogy.

Internet – library

Similarities: The Internet is sometimes seen as a vast repository of information and the term 'library' is often used to describe it: for example, 'huge digital library', 'cyberlibrary', 'Alexandrian Library of the twenty-first century', etc.

Differences: The storage of information and data is only one aspect of the Internet, and there are considerable differences between libraries and the Internet:

- Traditional libraries aim to serve individuals living in a particular place (city, country, etc.), whereas the Internet is global.
- Books, articles, and journals are published using procedures to ensure quality (editors). The Internet does not always have editors.
- Libraries are organised according to specific classification schemes, allowing users to locate the books in their collections. There is no such classification scheme for information on the Internet.

- Apart from keyword descriptions, the contents of a library (text in books and articles) are not accessible until the user borrows a particular book or journal. The content of the Internet is immediately accessible via search engines.

Used by: This analogy is used by various projects that aim to create a comprehensive system of information and knowledge on particular issues (portals, databases, etc.). Recently, the library analogy has been used in the context of a Google book project with the objective of digitalising all printed books.

Internet – VCR, photocopier

Similarities: This analogy focuses on the reproduction and dissemination of content (e.g. texts and books). Computers have simplified reproduction through the process of 'copy and paste'. This, in turn, has made the dissemination of information via the Internet much simpler.

Differences: The computer has a much broader function than the copying of materials, although copying itself is much simpler on the Internet than with a VCR or photocopier.

Used by: This analogy was used in the context of the US Digital Millennium Copyright Act (DMCA), which penalises institutions that contribute to the infringement of copyright (developing software for breaking copyright protection, etc.). The counterargument in such cases was that software developers, like VCR and photocopier manufacturers, cannot predict whether their products will be used illegally.

Highways and the Internet

Hamadoun Touré, ITU Secretary General, used an analogy between highways and the Internet by relating highways to telecommunications and the Internet traffic to trucks or cars: *I was giving a simple example, comparing Internet and telecommunications to trucks or cars and highways. It is not because you own the highways that you are going to own all the trucks or cars running on them, and certainly not the goods that they are transporting, or vice versa. It's a simple analogy. But in order to run your traffic smoothly, you need to know, when you are building your roads, the weight, the height and the speed of the trucks, so that you build the bridges accordingly. Otherwise, the system will not flow. For me, that's the relationship between the Internet and the telecommunications world. And they are condemned to work together.*[14]

This analogy was used in cases against the developers of Napster-style software for peer-to-peer (P2P) sharing of files, such as Grokster and StreamCast.

Internet – highway

Similarities: This analogy is linked to America's fascination with discovering new frontiers. Railroads and highways are usually part of this process. The Internet, as a frontier in the virtual world, corresponds metaphorically to highways in the real world.

Differences: Aside from the transportation aspect of the Internet, there are no other similarities between the Internet and highways. The Internet moves intangible materials (data), while highways facilitate the transportation of goods and people.

Used by: The highway analogy was used extensively in the mid-1990s, after Al Gore allegedly coined the term 'information superhighway'. The term 'highway' was also used by the German government in order to justify the introduction of a stricter Internet content control law in June 1997:

> *It's a liberal law that has nothing to do with censorship but clearly sets the conditions for what a provider can and cannot do. The Internet is a means of transporting and distributing knowledge… just as with highways, there need to be guidelines for both kinds of traffic.*[15]

Internet – high seas

Similarities: Initially, this analogy was driven by the fact that like the high seas, the Internet seems to be beyond any national jurisdiction. Nowadays, it is clear that most of the Internet lies within some national jurisdiction. The technical infrastructure through which Internet traffic is channelled is owned by private and state companies, typically telecommunication operators. The closest analogy to the Internet would be a shipping company's transport containers.

Differences: Sea transport is regulated by a wide array of international conventions, starting with the Convention on the Law of the Sea and branching out into numerous International Maritime Organization conventions relating to issues such as safety or the protection of the environment. These conventions regulate activities beyond national jurisdiction, such as on the high seas. There is nothing analogous in the field of Internet telecommunication.

Used by: This analogy is used by those who argue for the international regulation of the Internet. Concretely speaking, this analogy suggests the use of the old Roman law concept of *res communis omnium* (i.e. space as a common heritage for humankind to be regulated and garnered by all nations) on the Internet as it is used for regulating the high seas.

Classification of Internet governance issues

Internet governance is a complex new field requiring an initial conceptual mapping and classification. Its complexity is related to its multidisciplinary nature, encompassing a variety of aspects, including technology, socio-economics, development, law, and politics.

The practical need for classification was clearly demonstrated during the WSIS process. In the first phase, during the lead-up to the Geneva Summit (2003), many players, including nation states, had difficulty grasping the complexity of Internet governance. A conceptual mapping, provided by various academic inputs and the WGIG Report, contributed towards more efficient negotiations within the context of the WSIS process. The WGIG Report (2004) identified four main areas:

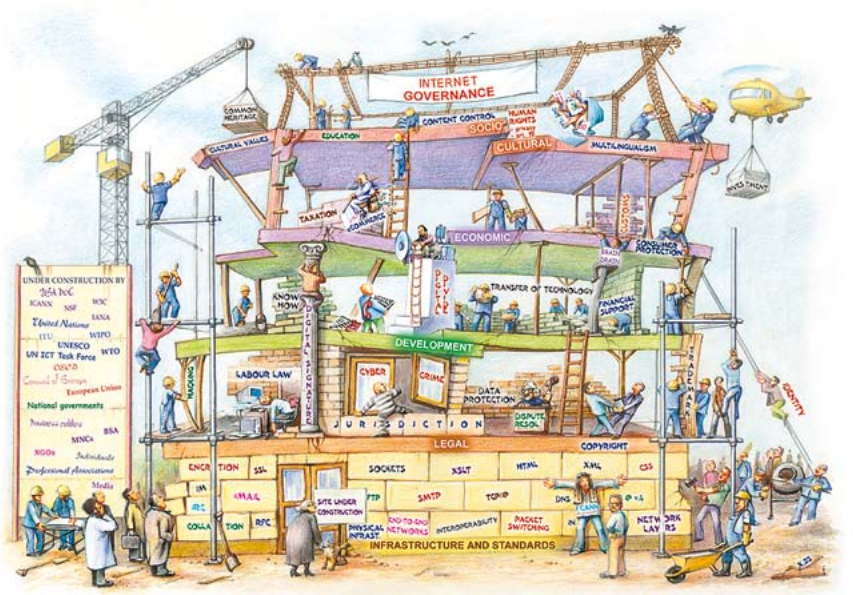
1. Issues related to infrastructure and the management of critical Internet resources.
2. Issues related to the use of the Internet, including spam, network security, and cybercrime.
3. Issues relevant to the Internet but have an impact much wider than the Internet and for which existing organisations are responsible, such as intellectual property rights (IPR) or international trade.
4. Issues related to the developmental aspects of Internet governance, in particular capacity building in developing countries.

The agenda for the first IGF held in Athens (2006) was built around the following thematic areas:

1. Access
2. Security
3. Openness
4. Diversity

At the second IGF in Rio de Janeiro (2007), the fifth thematic area was added to the agenda.

5. Managing Critical Internet Resources



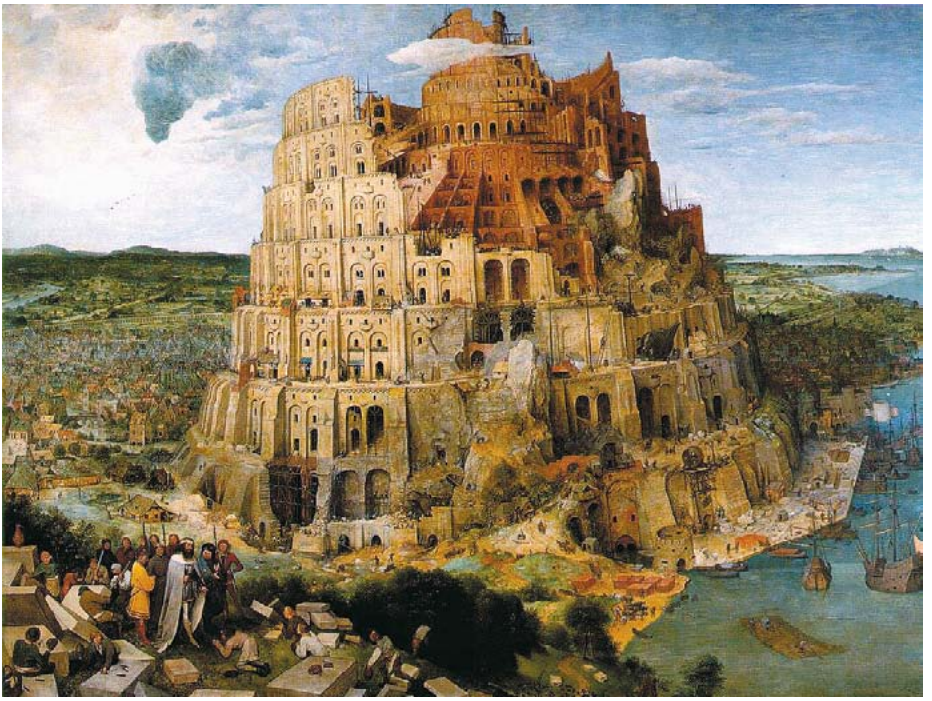
Although the classification changes, Internet governance addresses more or less the same set of 40–50 specific issues, with the relevance of particular issues changing. For example, while spam featured prominently in the WGIG classification in 2004, its policy relevance diminished at the IGF meetings, where it became one of the less prominent themes within the Security thematic area.

Diplo's classification of Internet governance groups the main 40–50 issues into the following five baskets:[16]

1. Infrastructure and standardisation
2. Legal
3. Economic
4. Development
5. Sociocultural

This classification reflects both the aforementioned (WGIG, IGF) policy approaches as well as academic research in this field. The classification has been developed since 1997 with constant adjustment based on feedback from students (alumni of 850 students as of 2010), research results, and insights from the policy process.

The five-basket classification of Internet governance is metaphorically presented through the image of a building under construction (see above) developed by Diplo researchers.



Building under construction: Are we building the twenty-first-century Tower of Babel?

A painting by Pieter Brueghel the Elder (1563), displayed in the Kunsthistorisches Museum in Vienna, shows the construction of the Tower of Babel (see above). Another, smaller, painting of the same year and on the same subject is in the Boijmans Van Beuningen Museum in Rotterdam. The Bible's *Book of Genesis* (11.7) refers to the construction of the Tower of Babel:

> *Let us go… and confuse their language so that one will not understand each other's language, each will not understand their fellow.*

The analogy of the construction of the Tower of Babel seems appropriate when looking at the challenges posed by the Internet and prompted us to consider another building under construction – one not aimed at reaching the heavens but at least at reaching everyone on the planet. Diplo has developed a framework for the discussion of Internet governance, illustrated on the previous page. Each floor in this building is discussed in the sections that follow. It is important to realise that all of the floors are linked, and that construction is ongoing and never-ending.

Endnotes

1 The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005. The objective of the first phase was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. More than 19 000 participants from 174 countries attended the Summit and related events. (Source: **http://www.itu.int/wsis/basic/about.html**)

2 The WGIG definition follows the pattern of frequently used definitions in the regime theory. The founder of regime theory, Stephen D. Krasner, notes that: *Regimes can be defined as sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations. Principles are beliefs of fact, causation, and rectitude. Norms are standards of behaviour defined in terms of rights and obligations. Rules are specific prescriptions or proscriptions for action. Decision-making procedures are prevailing practices for making and implementing collective choice*. Krasner S (1983) Introduction, in *International Regimes.* Krasner SD (ed.), Cornell University Press: Ithaca, NY, USA.

3 Shannon V (2006) What's in an 'i'? *International Herald Tribune,* 3 December 2006. Available at: **http://www.iht.com/articles/2006/12/03/technology/btitu.php**

4 The terminological confusion was highlighted by the way the term 'governance' was used by some international organisations. For example, the term 'good governance' has been used by the World Bank to promote the reform of states by introducing more transparency, reducing corruption, and increasing the efficiency of administration. In this context, the term 'governance' is directly related to core government functions.

5 Barlow JP (1996) *A declaration of the independence of cyberspace.* Available at: **https://projects.eff.org/~barlow/Declaration-Final.html**

6 For the evolution of the use of the word 'Internet' in the preparation for the Geneva summit consult, see: DiploFoundation (2003) *The Emerging Language of ICT Diplomacy – Key Words.* Available at: **http://www.diplomacy.edu/IS/Language/html/words.htm**

7 In June 2010, ICANN approved the .xxx top level domain name for adult material.

8 Network neutrality is a principle proposed for user access networks participating in the Internet that advocates no restrictions by Internet Service Providers and governments on content, sites, platforms, on the kinds of equipment that may be attached, and no restrictions on the modes of communication allowed. The principle states that if a given user pays for a certain level of Internet access, and another user pays for the same level of access, then the two users should be able to connect to each other at the subscribed level of access (Source: Wikipedia).

9 Available at: **http://www.state.gov/secretary/rm/2010/01/135519.htm**

10 This section could not have been completed without discussions with Aldo Matteucci, Diplo's senior fellow, whose 'contrarian' views on modern governance issues are a constant reality check in Diplo's teaching and research activities.

11 Barlow (1996) *op. cit.*

[12] The WSIS process started with the first preparatory meeting held in July 2002 in Geneva. The first summit was held in Geneva (December, 2003) and the second summit in Tunisia (November, 2003).

[13] Volker Kitz provides an argument for the analogy between administration of telephony systems and Internet names and numbers. Kitz V (2004) *ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called 'uniqueness' of the Internet.* Available at: **http://smu.edu/stlr/articles/2004/Winter/Kitz.pdf**

[14] Excerpts from the Secretary General's speech delivered at the ICANN meeting in Cairo (6 November 2008). Available at: **https://cai.icann.org/files/meetings/cairo2008/toure-speech-06nov08.txt**

[15] Quoted in Mock K, Armony L (1998) *Hate on the Internet.*Available at: **http://www.media-awareness.ca/english/resources/articles/online_hate/hate_on_internet.cfm**

[16] The term 'basket' was introduced into diplomatic practice during the Organization on Security and Cooperation in Europe (OSCE) negotiations

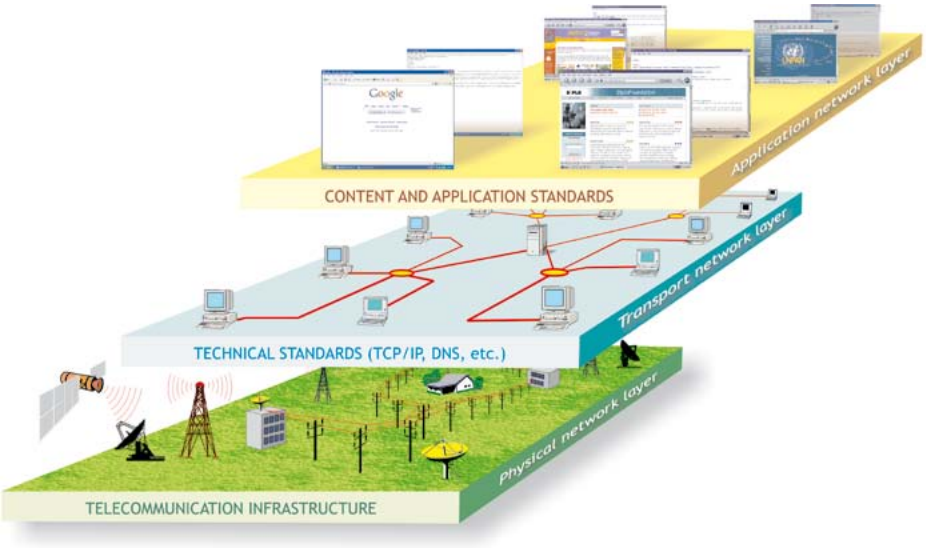
Section 2

The infrastructure and standardisation basket

The infrastructure and standardisation basket

The infrastructure and standardisation basket includes the basic, mainly technical, issues related to the running of the Internet. The main criterion for classifying an issue in this basket is its relevance to the basic functionality of the Internet. There are two groups of issues here.

The first group includes the essential issues without which the Internet and the World Wide Web could not exist.[1] These issues are grouped into three layers:



1. The telecommunication infrastructure, through which all Internet traffic flows.
2. The Internet technical standards and services, the infrastructure that makes the Internet work (e.g. TCP/IP: Transmission Control Protocol/ Internet Protocol; DNS: Domain Name Services; SSL: Secure Sockets Layer).
3. The content and applications standards (e.g. HTML: HyperText Markup Language; XML: eXtensible Markup Language).

The second group consists of issues related to safeguarding the secure and stable operation of the Internet infrastructure, and includes cybersecurity, encryption, and spam.

The telecommunication infrastructure

The current situation

Internet data can travel over a diverse range of communication media: telephone wires, fibre-optic cables, satellites, microwaves, and wireless links. Even the basic electric grid can be used to relay Internet traffic utilising powerline technology.[2]

Because the telecommunication layer carries Internet traffic, any new regulations linked to telecommunication will inevitably affect the Internet, too. The telecommunication infrastructure is regulated at both national and international level by a variety of public and private organisations. The key international organisations involved in the regulation of telecommunication include the International Telecommunication Union (ITU), which developed elaborate rules for covering the relationship between national operators, the allocation of the radio spectrum, and the management of satellite positioning, and the World Trade Organization (WTO), which played a key role in the liberalisation of telecommunication markets worldwide.[3]

ITU International Regulation

The 1988 ITU International Regulation (ITR) facilitated the international liberalisation of pricing and services and allowed a more innovative use of basic services in the Internet field, such as international leased lines, in the Internet field. It provided one of the infrastructural bases for the rapid growth of the Internet in the 1990s.

The roles of WTO and ITU are quite different. ITU sets detailed voluntary technical standards, telecommunication-specific international regulations, and provides assistance to developing countries. WTO provides a framework for general market rules.[4]

The liberalisation of national telecommunication markets has provided large telecommunication companies, such as AT&T, Cable and Wireless, France Telecom, Sprint, and WorldCom, with the opportunity of globally extending their market coverage. Since most Internet traffic is carried over these companies' telecommunication infrastructures, they have an important influence on Internet developments.

The issues

The 'local loop' or 'last mile'

The 'local loop' (or 'last mile') is the name given to the connection between Internet service providers (ISPs) and their individual customers. Problems with local loops are an obstacle to the more widespread use of the Internet in many, mainly developing, countries. Wireless communication is one possible, low-cost solution to the local loop problem. Apart from increasingly available technological options, the solution to the local loop problem also depends on the liberalisation of this segment of the telecommunication market.

The liberalisation of telecommunication markets

A considerable number of countries have liberalised their telecommunication markets. Many developing countries, however, are faced with a hard choice: to liberalise and make the telecommunication market more efficient, or to preserve an important budgetary income from existing telecommunication monopolies.[5] Foreign assistance, gradual transition, and linking the liberalisation process to the protection of the public interest might be ways out of this conundrum.

The establishment of technical infrastructure standards

Technical standards are increasingly being set by private and professional institutions. For example, the WiFi standard, IEEE 802.11b, was developed by the Institute of Electrical and Electronic Engineers. The certification of WiFi-compatible equipment is carried out by the WiFi Alliance. The very function of setting or implementing standards in such a fast-developing market affords these institutions considerable influence.

Transport Control Protocol/Internet Protocol (TCP/IP)

The current situation

TCP/IP is the Internet's main technical standard, specifying how data is moved through it; it is based on three principles: packet-switching, end-to-end networking, and robustness. Internet governance, as it relates to TCP/IP, has two important aspects: the introduction of a new standards and the distribution of IP numbers.

TCP/IP standards are set by the Internet Engineering Task Force (IETF). Given the core relevance of these protocols to the Internet, they are carefully guarded by IETF. Any changes to TCP/IP require extensive prior discussion and proof that they are an efficient solution (the 'running code' principle).

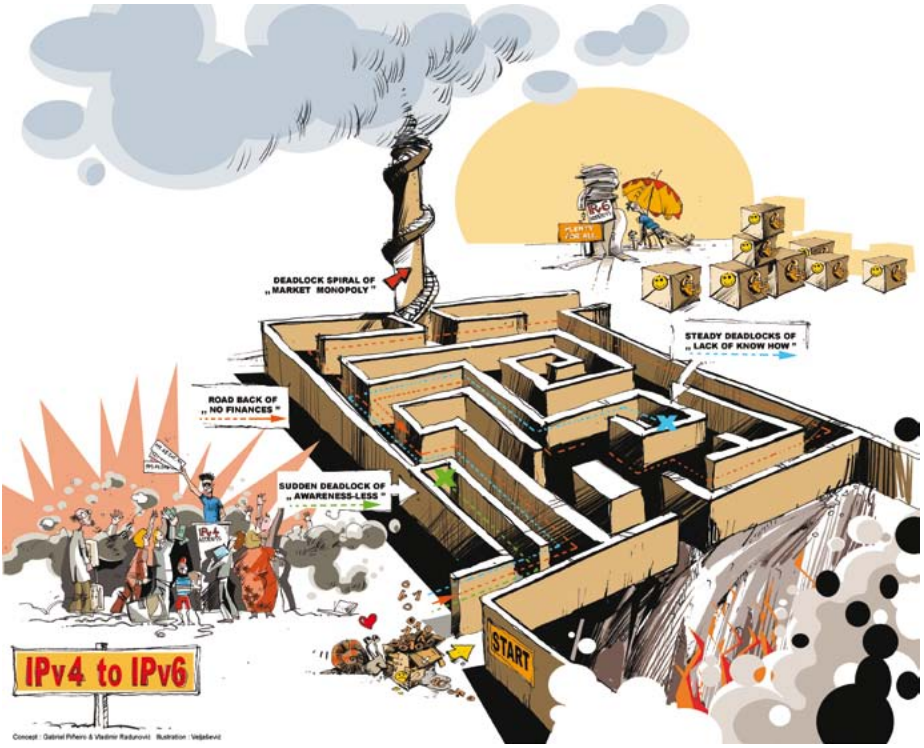
IP numbers are unique numeric addresses that all computers connected to the Internet must have. No two computers connected to the Internet have the same IP number, which makes them a potentially scarce resource. The system for the distribution of IP numbers is hierarchically organised. At the top is IANA (Internet Assigned Numbers Authority – a subsidiary of ICANN – Internet Corporation for Assigned Names and Numbers), which distributes blocks of IP numbers to the five regional Internet registries (RIRs).[6] RIRs distribute IP numbers to local Internet registries (LIRs) and national Internet registries (NIRs) which in turn distribute IP numbers to smaller ISPs, companies, and individuals further down the ladder.

The issues

How to deal with the limitation of IP numbers (Transition to IPv6)

The current pool of IP numbers under IPv4 (Internet Protocol, version 4) contains some four billion numbers and could reach depletion in the next few years with the introduction of Internet-enabled devices, such as mobile phones, personal organisers, game consoles, and home appliances. The concern that IP numbers might run out and eventually inhibit the further development of the Internet has led the technical community to take the following major actions:

- Rationalise the use of the existing pool of IP numbers through the introduction of Network Address Translation (NAT).
- Address the wasteful address allocation algorithms used by RIRs by introducing Classless Inter-Domain Routing (CIDR).



- Introduce a new version of the TCP/IP protocol – IPv6 – which provides a much bigger pool of IP numbers (340,000,000,000,000,000,000).

The response from the Internet technical community to the problem of a potential shortage of IP numbers is an example of prompt and proactive management. While both NAT and CIDR provided a quick fix for the problem, a proper long-term solution is the transition to IPv6. Although IPv6 was introduced back in 1996, its deployment has been very slow. With the approaching depletion of the pool of IPv4 numbers, this slow deployment is acquiring elements of a crisis in the making.

One of the main challenges facing the deployment of IPv6 is the lack of backward compatibility between IPv6 and IPv4. Networks using IPv6 cannot communicate directly to those, still dominant today, using IPv4. Since it is very likely that networks using IPv4 and IPv6 will coexist during the forthcoming period, it is important to ensure that new – IPv6-based – networks do not remain islands. A technical solution will involve special tunnelling between the two types of networks, which will cause more complex routing on the Internet and a few other 'collateral problems'.

The deployment has also been delayed by the low interest on the part of ISPs and users. Although they are aware of the risk of depletion of IP numbers, they prefer 'wait-and-see' tactics. For example, a recent survey in Japan showed that while more than 70% of ISPs are aware of the risk of depletion of IPv4, only 30% are preparing for transition to IPv6. In such a situation, when market motivation cannot provide the solution, there is increasing pressure on governments and other public authorities to play a more prominent role in championing the transition towards IPv6 through increasing awareness of the risks of the depletion of IPv4, giving financial support for the transition to IPv6, and using IPv6 for government networks.

Given the complexity of the transition to IPv6, developing countries, mainly in Africa, may benefit from the delayed start and the possibility of introducing IPv6-based networks from the beginning. In this process, developing countries will need technical assistance.[7]

Apart from the problem of transition, the policy framework for IPv6 distribution will require a proper distribution of IP numbers, demanding the introduction of open and competitive mechanisms to address the needs of end-users in the most optimal way.

Changes in TCP/IP and cybersecurity

Security was not a major issue for the original developers of the Internet, as, at that time, it consisted of a closed network of research institutions. With the expansion of the Internet to 2 billion users, and its growing importance as a commercial tool, the question of security is high on the list of Internet governance issues.

Because the Internet architecture was not designed with security in mind, incorporating intrinsic cybersecurity will require substantial changes to the very foundation of the Internet: TCP/IP. The new IPv6 protocol provides some security improvements, but still falls short of a comprehensive solution. Such protection will require considerable modifications to TCP/IP.[8]

Changes in TCP/IP and the problem of limited bandwidth

To facilitate the delivery of multimedia content (e.g. Internet telephony, video on demand) it is necessary to provide a Quality of Service (QoS) capable of guaranteeing a minimum level of performance. QoS is particularly important in delay-sensitive applications, such as live event broadcasting, and is often difficult to achieve due to bandwidth constraints. The introduction of QoS may require changes in the IP, including a potential challenge for the principle of network neutrality.

Technology, standards, and politics

The debate over network protocols illustrates how standards can be politics by other means. Whereas other government intervention into business and technology (such as safety regulations and anti-trust actions) are readily seen as having political and social significance, technical standards are generally assumed to be socially neutral and therefore of little historical interest. But technical decisions can have far-reaching economic and social consequences, altering the balance of power between competing businesses or nations and constraining the freedom of users. Efforts to create formal standards bring system builders' private technical decisions into the public realm; in this way, standards battles can bring to light unspoken assumptions and conflicts of interest. The very passion with which stakeholders contest standards decisions should alert us to the deeper meaning beneath the nuts and bolts.[9]

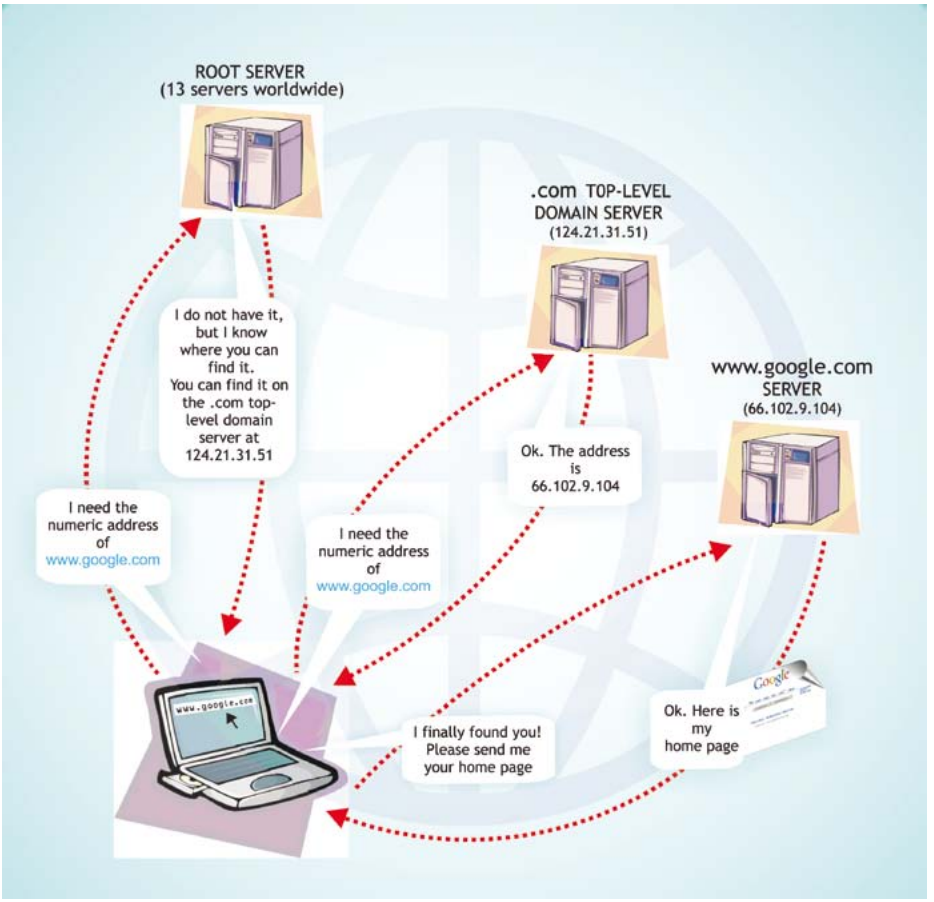
The Domain Name System (DNS)

The current situation

DNS handles Internet addresses (such as **www.google.com**) and converts them to IP numbers (a simplified scheme of this process is presented in in the graphic over the page). DNS consists of root servers, top-level domain (TLD) servers, and a large number of DNS servers located around the world. The management of DNS has been a hot issue in the Internet governance debate. One of the main controversies involves the ultimate authority of the US government (via the Department of Commerce) over root servers, the top tier of the hierarchically organised DNS. It is further aggravated by the fact that 10 out of 13 existing root servers are located in the United States (with three more in Europe and Asia). To address this problem and to enhance the scalability of the root server system, the 'Anycast' scheme was developed, which now includes about a hundred servers all over the world and in all continents.

DNS includes three types of top-level domains: generic (gTLD), country code (ccTLD), and sponsored (sTLD). gTLDs include domains that could be obtained by anyone (.com, .info, .net and .org). sTLDs are limited to specific group. For example, the sTLD '.aero' is open for registration only for air-transport industry. ccTLDs are limited to specific country (.uk, .cn, .in).

For each gTLD there is one registry that maintains an address list. For example, the .com gTLD is managed by VeriSign. The 'salesman' function is performed by registrars. ICANN provides overall coordination of DNS by



concluding agreements and accrediting registries and registrars. It also sets the wholesale price at which the registry (VeriSign) 'rents' domain names to registrars, and places certain conditions on the services offered by the registry and by the registrars. That is to say, ICANN acts as the economic and legal regulator of the domain name business for gTLDs.

An important part of DNS management is the protection of trademarks and dispute resolution. The 'first come first served' principle of domain name allocation used in the early days of the Internet triggered the phenomenon known as 'cybersquatting', the practice of registering domain names that could be resold later on. The Uniform Domain-Name Dispute-Resolution Policy (UDRP) developed by ICANN and the World Intellectual Property Organization (WIPO) was aimed at reducing cybersquatting.

Another important element in the survey of the current organisation of DNS governance is the management of ccTLDs. Currently, some country codes

are still managed by a variety of institutions or individuals that received accreditation in the early days of the Internet, when some governments were not all that interested in such matters.

The issues

The creation of new generic domain names

Technically, the creation of new TLDs is almost unlimited. However, the introduction of new gTLDs has been very slow, with a number of new gTLDs introduced only recently. Currently 20 gTLDs are active and three more are under consideration.[10] The main opposition to the creation of new gTLDs originates from the trademark lobby, whose concern is that increasing the number of domains would make the protection of their trademarks difficult and increase cybersquatting.

Under pressure to introduce new gTLDs, ICANN initiated consultations to design a new policy in this field which would address the resolution of competing claims for gTLDs, the risk of cybersquatting, questions of public morality, and registration fees, among others.

Content-related generic domain names

Another ICANN policy issue is deciding on the creation of new domains, which could involve linking domain names to content.[11] The most illustrative situation is the proposal to introduce the .xxx domain for adult materials. The ICANN Board rejected this proposal in March 2007. The main criticism of this decision was that ICANN made it under pressure from the US government, which strongly opposed its introduction.[12] Interestingly, many other governments supported the US government, including those who are usually critical of the US position in Internet governance, such as Brazil and China. The issue was revisited in June 2010 at the ICANN meeting in Brussels where the ICANN Board positively reviewed the application for the .xxx domain and initiated negotiations for its introduction. This decision also re-opened the discussion about ICANN's role in public policy issues.

Generic domain names for cultural and linguistic communities

In 2003, ICANN introduced a new .cat domain for the Catalan language. This is the first domain introduced for a language.[13] The Spanish government did not oppose this decision.

At the time it was introduced, it triggered many concerns that it could be used as precedent for other languages, or even more controversially for language

and cultural communities that may have aspirations towards nationhood. With hindsight, we see that this has not happened.

The management of country domains

The management of ccTLDs involves three important issues. The first concerns the often politically controversial decision as to exactly which country codes should be registered when dealing with countries and entities with unclear or contested international status (e.g. newly independent countries and resistance movements). One controversial issue was the allocation of a Palestinian Authority domain name. In justifying its decision to assign the .ps TLD, IANA reiterated the principle of allocating domain names in accordance with the ISO 3166 standard, as was proposed by Jon Postel, one of the Internet's founding fathers.[14]

The second issue concerns who should manage ccTLDs. Many countries have been trying to gain control over their country domains, which are considered national resources. National governments have chosen a wide variety of policy approaches.[15] Transition ('re-delegation') to a new institution managing the ccTLD ('delegee') within each country is approved by ICANN only if consensus exists within the country, reached by all interested stakeholders. Given the importance of this issue and the wide variety of approaches, there were two important international-level initiatives to introduce a certain level of harmonisation. The first was the GAC Principles, adopted by the ICANN Government Advisory Committee (GAC), which proposed policy and specified procedures for the re-delegation of ccTLD administration.[16] The second was Best Practices, proposed by the World Wide Alliance of Top Level Domains (June, 2001).

The third issue is related to the reluctance of many country domain operators to become part of the ICANN system. So far, ICANN has not managed to gather country domain operators under its umbrella. Country domain operators are organised at regional level (Europe – CENTR, Africa – AFTLD, Asia – APTLD, North America – NATLD, and South America – LACTLD). At global level, the main forum is the World Wide Alliance of Top Level Domains. ICANN is developing Accountability Frameworks as a less formal way of developing links with the country domain operators.

Internationalised domain names

The Internet was originally a predominately English-language medium. Through rapid growth, it has become a global communication facility with an increasing number of non-English-speaking users. For a long time, the lack

of multilingual features in the Internet infrastructure was one of the main limitations of its future development.

In May 2010, after a long testing period and political uncertainties, ICANN started approving new domain names in a wide variety of scripts, including Chinese, Arabic, and Cyrillic. The introduction of internationalised domain names (IDNs) is considered to be one of the main successes of the Internet governance regime.

Root servers

At the top of the DNS hierarchical structure, root servers attract a lot of attention. They are a part of most policy and academic debates on Internet governance issues.

The current situation

The function and robustness of DNS can be illustrated by analysing the concern that the Internet would collapse if the root servers were ever disabled. First, there are 13 root servers distributed around the world (10 in the USA and one each in Sweden, the Netherlands and Japan; of the 10 in the USA, several are operated by US government agencies), which is the maximum number technically possible. If one server crashes, the remaining 12 would continue to function. Even if all 13 root servers went down simultaneously, the resolution of domain names (the main function of root servers) would continue on other domain name servers, distributed hierarchically throughout the Internet.[17]

Therefore, thousands of domain name servers contain copies of the root zone file and an immediate and catastrophic collapse of the Internet could not occur. It would take some time before any serious functional consequences would be noticed, during which time it would be possible to reactivate the original servers or to create new ones.

In addition, the system of root servers is considerably strengthened by the Anycast scheme, which replicates root servers throughout the world. This provides many advantages, including an increased robustness in DNS and faster resolution of Internet addresses (with the Anycast scheme, the resolving servers are closer to the end-users).

The 13 root servers are managed by a diversity of organisations: academic/public institutions, commercial companies, and government institutions. Institutions managing root servers receive a root zone file proposed by IANA (ICANN) and approved by the US Government (Department of Commerce). Once the content is approved by the Department of Commerce, it is entered into the master root server operated by VeriSign under contract to the Department.

The file in the master root server is then automatically replicated in all the other root servers. Thus, it is theoretically possible for the US government to introduce unilateral changes to the entire DNS. This is a source of concern to many governments.

The issues

Internationalisation of the control of root servers

Many countries have expressed concern about the current arrangement in which the ultimate decision-making with regard to the content of root servers remains the responsibility of one country (the United States). There were various proposals in the Internet governance process, including adopting a Root Convention, which would put the international community in charge of policy supervision of the root servers or, at least, grant nation states rights over their own national domain names. New possibilities have been opened with the Affirmation of Commitments,[18] which addresses the question of the institutional independence of ICANN from the US Department of Commerce, including ICANN's future internationalisation. The IANA arrangement will be re-negotiated in 2011. Some elements of a solution-in-the-making would consist of two steps:

1. The reform of ICANN, initiated by the Affirmation of Commitments, leading to the creation of a *sui generis* international organisation, which would be an acceptable institutional framework for all countries.
2. The transfer of control of root servers from the US Department of Commerce to ICANN, as was initially envisaged.

Alternative root servers – feasibility and risks

Creating an alternative root server is technically straightforward. The main question is how many followers an alternative server would have, or, more precisely, how many computers on the Internet would point to it, when it came to resolving domain names. Without users, any alternative DNS becomes useless. A few attempts to create an alternative DNS have been

made: Open NIC, New.net, and Name.space. Most of them were unsuccessful, accounting for only a few percent of Internet users.

The US role in the management of root servers – the paradox of power

Since the adoption of the Affirmation of Commitments, the question of US power over root servers could gradually become history. The potential power of removing a country from the Internet (by deleting the country's domain name) can hardly be qualified as a power, since it has no effective use. The key element of power is forcing the other side to act in the way the holder of power wants. The use of US power over the Internet infrastructure could create unintended consequences, including countries and regions establishing their own Internets. In such a scenario, the Internet might disintegrate and US interests could be endangered (predominance of US values on the Internet, English as the Internet's lingua franca, and predominance of US-based companies in the field of e-commerce). Based on the first policy initiatives in Internet governance (e.g. Affirmation of Commitments) it seems that the Obama administration is aware of this paradox of power. It is a promising sign for the future development of the global Internet governance regime.

Network neutrality[19]

What would have happened if the competition had restricted access to Google in its early days? Or if telecom operators had slowed down Skype's introduction of Internet telephony? Or if the US government had had Internet access to enemy countries?[20] Most likely, we would have a computer network that was an extension of 1980s logic with, for instance, X25 network protocol instead of TCP/IP, exchanging data between national computer networks at borders between countries.

The Internet's success lies in its design, which is based on the principle of network neutrality. All data traffic on the Internet at that time, whether coming from start-ups or big companies, was treated without discrimination. New companies and innovators did not need permission or market power to innovate on the Internet.

The importance of network neutrality to the success of the Internet, so far, has been key. This is why the debate has attracted a wide range of actors: from the President of the United States to human right grassroots activists. Network neutrality is one of the highest priorities on President Obama's technology agenda and has been debated in many political bodies, including

the US Congress. From the start, network neutrality was a US-based debate; but with new developments, network neutrality is increasingly being discussed worldwide.

Why is network neutrality so topical now?

There is no conspiracy. The Internet has become a victim of its own success. With 2 billion users and the increasing shift of our daily economic and social reality to the Internet, the stakes are becoming very high. The Internet has great commercial and development potential. For some of these commercial developments, especially those related to the delivery of video and multimedia services, network neutrality could create an obstacle.

The current situation

Paradoxically, network neutrality has never been strictly applied. Since the early days of dial-up modem connections, there has been rivalry between available bandwidth and the users' needs. In order to address this challenge and provide quality service, Internet operators (telecom companies and ISPs) have used various network management techniques to prioritise certain traffic. For example, Internet traffic carrying voice conversation over Skype should have priority over traffic carrying a simple e-mail: while we can hear delays in Skype voice chat, we won't notice minor delays in an e-mail exchange. The need for network management is especially important today with the extended pool of users of high-demand services such as downloads, HD video stamps, Internet telephony, online games, etc.

Growing demand for bandwidth

In 2009, as an illustration of the growing demand for bandwidth, YouTube viewers were watching some 1.2 billion videos per day,[21] and uploaded almost 20 hours of video every minute! [22]

Network management is becoming increasingly sophisticated in routing Internet traffic in the most optimal way for providing quality service: preventing congestion, and eliminating latency and jitter. The first discord in the interpretation of the principle of network neutrality focuses on whether any network management at all should be allowed. Network neutrality purists argue that 'all bits are created equal' and that all Internet traffic must be equally treated. Telecoms and ISPs challenge this view arguing that it is users who should have equal access to Internet services and if this is to happen, Internet traffic cannot be treated equally. If both video and e-mail traffic are treated equally, users won't have good video-stream reception, yet they wouldn't notice a few seconds delay in receiving an e-mail. Even network neutrality purists cannot question this

rationale. Their concern is that any compromise on network neutrality can open a Pandora's box, raising the problem of distinguishing between justified network management and possible manipulation.

The issues

In the network neutrality debate, there is an emerging consensus that there is a need for *appropriate* network management. The main question is how to interpret the adjective 'appropriate'. There are three areas besides technical concerns – economic, legal, and human rights issues – where the debate on network management and network neutrality is particularly heated.

Economic issues

During the past few decades, many significant network operators – including both telecoms and ISPs – have extended their business to offer services as well: besides selling Internet connections of various bandwidths to households and businesses, they have introduced their own VoIP (Voice-over Internet Protocol; telephone via Internet) or IP TV (television via Internet) services, video on demand (akin to renting movies), music or video download portals, etc. They are now competing not only with their counterparts for cheaper, faster, and better quality connections, but also with service and content providers – such as Skype, Google, and Apple.

Network management – something available to operators but not to others – may be an important tool when competing in service and content provision by prioritising packages according to business-driven preferences. For instance, an operator may decide to slow down or fully ban the flow of data packages from a competing company (such as Skype or Google Voice) to end-users through its network, while giving priority to data packages of its own in-house service (such as the IP telephony or Internet-television it offers to customers).[23]

Legal issues

Another grey area in network management is the right of Internet operators to block materials that may infringe on copyright. Do ISPs have the right and obligation to stop traffic, for example, on peer-to-peer (P2P) networks which are usually used for sharing copyright-protected materials? Do they have the prerogative of juridical and administrative bodies?

Some of these questions have been the focus of the case between the Federal Communication Commission (FCC) and Internet operator Comcast. In 2007, two public advocacy groups filed a complaint with FCC, the US regulatory authority, claiming that Comcast, the operator, violated network

neutrality by significantly slowing down the BitTorrent application (P2P software for downloading files – usually music, video and games, though not only these) for its users.[24]

Political issues

The ability to manage network traffic based on origin or destination, service or content, can give governments the opportunity to impose such practices on inland carriers and thereby effectively introduce traffic filters for objectionable or sensitive content in relation to the country's political, ideological, religious, cultural or other values. This brings risks of misuse of network management for censorship, especially in countries with authoritarian regimes.

The risks

If network management goes beyond an *appropriate* level aimed at providing equal service to all Internet users, the principle of network neutrality will be endangered. It could lead towards creating a tiered Internet. According to user groups like Save the Internet[25] and the Internet Governance Caucus,[26] the Internet could become a set of commercial packages offered by ISPs in which users would be able to access only certain online services and content within a certain chosen package[27] – much like cable TV.

Accordingly, they warn that if carriers start charging the content or application providers, it will kill the competition for the operators' own services, and endanger small businesses[28] and non-commercial offers, such as applications for people with disabilities that commonly require high bandwidth.

Who are the main players and what are their arguments?

The position of the main players is in constant flux. For example, the latest indications that Google may sign a special agreement with Verizon for a mid-way approach to network neutrality would change the positioning of the main players.[29] Till now, Google has been considered one of the main proponents of network neutrality; others include consumer advocates, online companies, some technology companies, many major Internet application companies including Yahoo!, Vonage, Ebay, Amazon, EarthLink, and software companies like Microsoft.

Opponents of network neutrality include the main telecom companies, ISPs, producers of networking equipment and hardware, and producers of video and multimedia materials. Their arguments are market-centered, starting from the need to offer what consumers want.

There are four main arguments in the network neutrality debate.

	Proponents	Opponents
Argument about the future	Network neutrality will preserve the Internet architecture that has enabled the fast and innovative development of the Internet so far. Most proponents are new Internet companies who have developed thanks to the Internet's open architecture.	Online companies must have an opportunity to further develop the Internet and offer services which customers will be interested in. This may involve faster Internet traffic.
Economic argument	Without network neutrality, the Internet will look like cable TV. A handful of massive companies would control access and distribution of content, deciding what users get to see and how much it costs. While it would benefit a few, it would damage many and ultimately ruin the economic future of the Internet.	If there isn't a possibility to offer new services and economic models, this will reduce economic interest in the Internet, stop investment, and ultimately even endanger the Internet infrastructure.
Ethics argument	The Internet is the result of developments of many volunteers over decades. They invested time and creativity in developing the core of the Internet from technical protocols to content. It is not justifiable to have such a huge investment harvested by a few companies who will lock the Internet in constrained business models by breaching network neutrality. The Internet was developed openly and publicly. The public's interests must be ensured. Network neutrality is one of the ways to do it.	Network neutrality is ethically questionable because Internet operators have to invest in maintaining the Internet infrastructure; most benefits are reaped by Internet 'content' companies such as Google, Facebook, and Amazon. Internet and telecom operators argue that the cake should be shared more equally.
Regulation argument	Network neutrality must be imposed by government. Any form of self-regulation will leave it open for Internet and telecom operators and cable companies to breach the principle of network neutrality.	The Internet has developed because of very light or no regulation. Heavy government regulation can stifle creativity and regulation on network neutrality can stifle the future development of the Internet

The basic principles

In recent years, some regulators – such as those in Norway, the USA or the EU – have stepped in and formulated key principles for network neutrality based on ongoing discussions:[30]

- **Transparency:** Internet operators must provide complete and accurate information on their network managing practices, capacity, and the quality of their service to customers.
- **Access**: Users should be able to have [equal] access to any [legal] content, service or application [with minimum quality of service guaranteed, as prescribed by the regulator] or to connect any hardware that does not harm the network [regardless of their financial capacities or social status].
- **(Non)discrimination:** Internet operators should make no discrimination [or reasonable discrimination] of traffic based on:
  - Origin of sender or receiver.
  - Type of content type of application and service [with fair competition – no discrimination against undesired competitors].
  - Where 'reasonable' could be any practice for public benefit (assuring quality of service, security and resilience of network, innovations and further investments, lowering costs, etc.).

Other principles most frequently debated in international forums such as the IGF meetings and the EuroDIG dialogue[31] include:

- Preserving freedom of expression, access to information and choice.
- Assuring quality of service and security and resilience of the network.
- Preserving incentives for investments.
- Stimulating innovations [including opportunities for new business models and innovative businesses]. Defining rights, roles, and accountability of all parties involved (providers, regulators, users) including the right to appeal and redress.
- Preventing anti-competitive practices.
- Creating a market environment that would allow users to easily choose and change their network operator.
- Protecting the interests of the disadvantaged, such as people with disabilities and users and businesses in the developing world.
- Maintaining diversity of content and services.

Users or customers?

The network neutrality debate also creates linguistic discourse. Proponents of network neutrality focus on Internet 'users', while the others – mainly commercial players – describe them as 'customers'. Internet users are more than simply customers; the term 'user' implies active participation in the development of the Internet through social networks, blogging, and other tools and the important role they have in deciding the future of the Internet. Customers, on the other hand, like any other customers, can decide whether or not to purchase the services on offer. Their status on the Internet is based on a contract with the ISP and customer protection rules. Beyond that, customers are not supposed to have any role in deciding how the Internet is run.

Policy approaches

With the network neutrality debate, another question has come to the fore: what is the role of the regulators in broadband policy and operator practices?

Developed countries

In response to the Comcast case, the US FCC adopted the Guidelines on Network Neutrality as an update to its 2005 policy paper,[32] which reflect the need for access to and choice of content and devices, and addressed the issues of discrimination and transparency. Japan's Ministry of Internal Affairs and Communications' working group reported on choice and access as well as discrimination, but additionally tackled fairness in network cost-sharing and network use.[33] The Swedish Post and Telecom Agency (PTS) outlines that openness – promoted by non-discrimination and competition – is a prerequisite for innovation but also that it should be balanced against investments and security of the network.[34] The regulatory framework on electronic communications of EU targets protecting freedom of expression, users' choice, and access rights, along with the transparency principle; yet it also stresses the need for investments, fair competition with no discrimination, and opportunities for new business models including innovative business.[35]

The most praised model comes from the Norwegian Post and Telecommunications Authority (NPT), seeking to ensure: transparency of business offers and practices, user choice and access to content, services and hardware, and non-discrimination based on application, service, content, sender or receiver.[36] It is not, however, only the content that stands out but also the process of reaching consensus on these guidelines: taking a broad multistakeholder-based approach to designing soft co-regulations based on reaching consensus of all parties over a binding agreements; in that way NPT re-assured consumers and business that the market can be regulated without hard law.[37]

In some countries, however, there is a practice not to prevent business-driven discrimation. Proponents of net neutrality label them 'anti-neutrality islands' where, arguably, one can see what the perspectives of a 'non-neutral Internet' are.

Developing countries

Due to limited infrastructure and bandwidth, regulators of developing countries put more focus on fair usage policy – affordable prices and fair access for all. Some raise concerns over cross-border non-discrimination, saying that the traffic from all countries should be treated the same way with no preferences based on termination costs. Also, certain countries have more sensitivity to internal cultural, political, or ethical aspects, thereby understanding '(in) appropriate use' and management differently than some others. Concerns have been raised that the innovative models of the developed world might hamper developing markets: by prioritising the services of big global companies; the emerging business and competition would be additionally downsized, threatening diversity and innovation. No major formal policies or regulatory practices on network neutrality, however, have yet come from the developing world.

International organisations and NGOs

Many international organisations and user groups have also developed policy positions with regards to network neutrality. The Council of Europe emphasises the fundamental rights to freedom of expression and information; ISOC promotes its user-centric approach which dominantly tackles the issues of access, choice, and transparency through the 'Open Inter-networking' debate rather than the one on network neutrality.[38] The Trans Atlantic Consumer Dialogue (TACD), a forum of US and EU consumer organisations additionally emphasises requests for carrier non-discriminatory behaviour, calling upon the USA and the EU to entitle regulators to act as safeguards of users' rights.[39] Many NGOs are especially concerned about the future of non-commercial and non-competing online content and services, requesting these to be broadcasted through any carrier network equal to the commercial ones. They emphasise the rights of marginalised groups – especially people with disabilities – to use content, services, and applications (including high-bandwidth-demand ones) of their needs without any limits whatsoever.

Open issues

There are a number of open issues on the network neutrality debate agenda:

- Where should the balance be between public good effects of the Internet and user (and human) rights on the one hand, and the rights of Internet operators to innovate within the networks they own on the other?

- Would an unregulated market with open competition, as advocated by the carriers, provide unlimited (or sufficient) choice for users? Or should the regulators inevitably be empowered as safeguards, and with what authority?
- How would different regulatory approaches impact the broadband market and further investment and innovation?
- What are the implications of network (non)neutrality for the developing world?
- Will the need for network management for technical (quality) reasons be outdated in future, due to advancements in carrier technology?
- What are the implications of a tiered Internet for competition, innovation, investment, and human rights?
- How will the cloud computing era and the growing dependence on clouds influence the debate on network neutrality, and vice versa?
- Should the debate be extended from traffic management on a carrier level to content and application management on content and application provider level, such as Google, Apple, or Facebook?
- Will consumer protection continue to be intrinsically linked to network neutrality? If network neutrality is 'defeated', what principles will support consumer protection in future?

Internet service providers (ISPs)

Since ISPs connect end-users to the Internet, they provide the most direct and straightforward option for the enforcement of legal rules on the Internet. With the Internet's growing commercial relevance and increasing cybersecurity concerns, many states have started concentrating their law enforcement efforts on ISPs.

The issues

See Section 5 for further discussion on the digital divide

Telecommunication monopolies and ISPs

It is common in countries with telecommunication monopolies for those monopolies to also provide Internet access. Monopolies preclude other ISPs from entering this market and inhibiting competition. This results in higher prices, often a lower quality of service, and fails to reduce the digital divide. In some cases, telecommunication monopolies tolerate the existence of other ISPs, but interfere at operational level (e.g. by providing lower bandwidths or causing disruptions in services).

ISPs responsibility for copyright

Common to all legal systems is the principle that an ISP cannot be held responsible for hosting materials that breach copyright law if the ISP is not aware of the violation. The main difference lies in the legal action taken after the ISP is informed that the material it is hosting is in breach of copyright.

US and EU law employs the Notice-Take-Down procedure, which requires ISPs to remove such material in order to avoid being prosecuted. Japanese law takes a more balanced approach, through the Notice-Notice-Take-Down procedure, which provides the user of the material with the right to complain about the request for removal.

The approach of placing limited liability on ISPs has been generally supported by jurisprudence. Some of the most important cases where ISPs were freed of responsibility for hosting materials in breach of copyright law are: the Scientology case (the Netherlands), RIAA *vs* Verizon (United States), SOCAN *vs* CAIP (Canada), and Sabam *vs* Tiscali (Belgium).

The role of ISPs in content policy

Under growing public pressure, ISPs are gradually, albeit reluctantly, becoming involved with content policy. In doing so, they might have to follow two possible routes. The first is to enforce government regulation. The second, based on self-regulation, is for ISPs to decide themselves what is appropriate content. This runs the risk of privatising content control, with ISPs taking over governments' responsibilities.

The role of ISPs in anti-spam policy

ISPs are commonly seen as the primary institutions involved with anti-spam initiatives. Usually, ISPs have their own initiatives for reducing spam, through either technical filtering or the introduction of anti-spam policy. The ITU report on spam states that ISPs should be liable for spam and proposes an anti-spam code of conduct, which should include two main provisions: an ISP must prohibit its users from spamming and it must not peer with other ISPs that do not accept a similar code of conduct.[40]

The spam problem exposes ISPs to new difficulties. For instance, Verizon's anti-spam filtering led to a court case as it also blocked legitimate messages causing inconvenience for users who did not receive their legitimate e-mail.[41]

Internet bandwidth providers (IBPs)

The Internet access architecture consists of three tiers. ISPs that connect end-users constitute Tier 3. Tiers 1 and 2 consist of IBPs. Tier 1 carriers are the major IBPs. They usually have peering arrangements with other Tier 1 IBPs.[42] The main difference between Tier 1 and Tier 2 IBPs is that Tier 1 IBPs exchange traffic through peering, while Tier 2 IBPs have to pay transit fees to Tier 1 providers.[43]

Tier 1 is usually run by large companies, such as MCI, AT&T, Cable Wireless, and France Telecom.

The issues

Should the Internet infrastructure be a public service?

Internet data can flow over any telecommunication medium. In practice, facilities such as Tier 1 backbones (i.e. principal data routes between large, strategically interconnected networks and core routers in the Internet), commonly having optical cables or satellite links, have become critical to the operation of the Internet. Their pivotal position within the Internet network grants their owners the market power to impose prices and conditions for providing their services. Ultimately, the functioning of the Internet could depend on the decisions taken by the owners of central backbones. Is it possible for the global Internet community to request assurances and guarantees for the reliable functioning of the critical Internet infrastructure from major telecommunication operators? The trend in discussion is on imposing certain public requirements on private Internet infrastructure operators.

IBPs and critical infrastructure

In early 2008, a disruption occurred with one of the main Internet cables in the Mediterranean, near Egypt. This incident endangered access to the Internet in a broad region extending to India. Two similar incidents happened in 2007 (disruptions in the Internet cable near Taiwan and the main Internet cable for Pakistan) clearly showing that the Internet infrastructure is part of national and global critical infrastructure. Disruption of Internet services can affect the overall economy and social life of a region. The possibility of such a disruption leads to a number of questions.

- Are the main Internet cables properly protected?
- What are the respective roles of national governments, international

organisations, and private companies in the protection of Internet cables?

- How can we manage the risks associated with potential disruption of the main Internet cables?

Telecommunication liberalisation and the role of ISPs and IBPs

There are opposing views about the extent to which ISPs and IBPs should be subjected to existing international instruments. Developed countries argue that the liberalised rules granted by WTO to telecommunication operators can also be extended to ISPs. A restrictive interpretation highlights the fact that the WTO telecommunication regime applies only to the telecommunication market. The regulation of the ISP market requires new WTO rules.

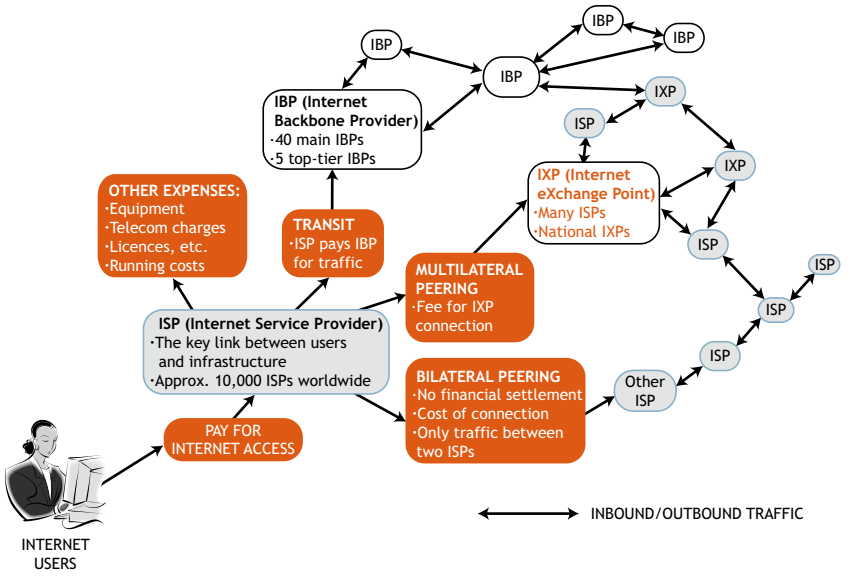
An economic model of Internet interconnectivity

> *We know how to route packets,*
> *what we don't know how to do is route dollars.*
>
> **David Clark**

The current situation

Often, any discussion of governance-related issues ends up with an analysis of the distribution of money.[44] Who pays for the Internet? A number of financial transactions occur between the many parties involved with the Internet. Individual subscribers and companies pay ISPs for Internet access and services. How is this money distributed to others in the various chains of Internet service provision or, in other words, how does the Internet dollar flow?[45] Expenses that should be covered from the fees collected by ISPs include those that:

- ISPs pay to telecommunication operators and for Internet bandwidth;
- ISPs pay to RIRs or LIRs, from whom the pools of IP addresses are obtained for further allocation;
- ISPs pay to vendors for equipment, software, and maintenance (including diagnostic tools as well as support for the staff to operate their facilities, help desks, and administrative services);
- parties registering a domain name with a registrar pay to the registrar and to IANA for its services; and
- telecommunication operators pay to cable and satellite manufacturers and telecommunication service providers to supply them with the necessary links. (As these operators are often in debt, they in turn pay interest to various banks and consortia.)



The list continues and the truth is, 'there ain't no such thing as a free lunch'. Ultimately, Internet end-users, whether individuals or institutions, pay the costs in this chain.

The issues

Does the economics of Internet connectivity need reform?

One of the Internet's legacies is its current economic policy and practice, which has been developed through a number of iterations. Internet economic practice is presently considered efficient, because of the Internet's smooth functionality and, in general, its affordable cost. The primary criticisms of the current economic policies focus on two aspects:

1. It does not avoid a monopoly of the main players in the field of Internet connectivity and thus a potential distortion of the market is possible.
2. It does not allocate a fair share of both income and costs among all those involved in Internet economics.

In academic circles, numerous attempts have been made to provide proper economic policies for the Internet. Nguyen and Armitrage argue that the Internet should have an optimal balance between three elements: technical efficiency, economic efficiency, and social effects.[46] Others highlight the challenges of replacing the existing, simple, flat-rate pricing structure with a more complex one, such as accounting based on the traffic of packets. With

regard to practical changes, some believe that changing the current Internet economic policies could open a Pandora's box.

Preventing possible monopolies in the Internet resources market

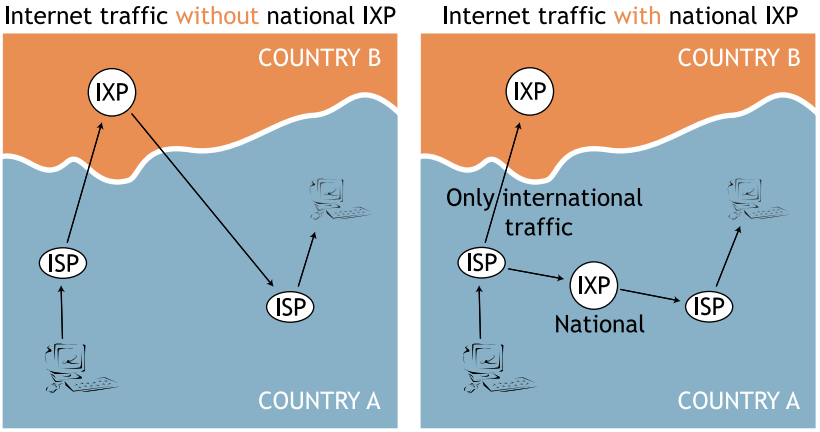
It is possible that through take-overs, a few monopolies could dominate the entire Internet traffic market.[47] This problem exists in both developed and developing countries. Some hope that the process of the liberalisation of telecommunication markets will solve the problem of monopolies (especially involving incumbent operators). However, liberalisation could lead to the replacement of a public monopoly by a private monopoly. Geoff Huston argues that establishing monopolies and losing the diverse market of Internet resources would inevitably affect the price and quality of Internet services.[48]

Who should cover the cost of links between developing and developed countries?

> *When an end-user in Kenya sends e-mail to a correspondent in the USA, it is the Kenyan Internet service provider (ISP) who is bearing the cost of international connectivity from Kenya to the USA. Conversely, when an American end-user sends e-mail to Kenya, it is still the Kenyan ISP who is bearing the cost of International connectivity, and ultimately the Kenyan end-user who bears the brunt by paying higher subscriptions.*[49]

Currently, developing countries cover the cost of links between developing and developed countries.[50, 51] Compared to the traditional telephony system, where two countries share the price of each international call, the Internet model puts the entire burden on one side: that of developing countries. These countries must bear the costs for connecting to backbones located mainly in developed countries. As a result, small and poor countries subsidise the Internet in rich countries.

The main argument in discussions about changes to the current system of Internet charges uses the analogy of the telephone financial settlement system, which shares the cost and income between communication endpoints. However, Geoff Huston argues that this analogy is not sustainable. In the telephony system, only one clearly identifiable commodity – a phone call establishing human conversation between two telephone sets – has a price.[52] The Internet does not have an equivalent, single 'commodity', only packets, which take different routes through the network. This fundamental difference makes this analogy inappropriate. It is also the main reason why the telephone financial settlement model is difficult to apply to the Internet.



ITU initiated discussions on possible improvements to the current system for the settlement of Internet expenses, in order to have a more balanced distribution of costs for Internet access. Due to opposition from developed countries and telecom operators, the adopted ITU Resolution, D. 50, is practically ineffective.[53] Unsuccessful attempts were also made to introduce this issue during WTO negotiations. The need for adjustments in interconnection charges was reiterated in the Word Summit on the Information Society (WSIS) Final Documents and in the Working Group on Internet Governance (WGIG) Report.

Web standards

By the late 1980s, the battle over network standards had ended. TCP/IP gradually became the main network protocol, marginalising other standards, such as the ITU-supported X25 and many proprietary standards, such as IBM's SNA. While the Internet facilitated normal communication between various networks via TCP/IP, the system still lacked common applications standards.

A solution was developed by Tim Berners-Lee and his colleagues at CERN (the European Organization for Nuclear Research) in Geneva, consisting of a new standard for sharing information over the Internet, called HTML (really just a simplification of an existing ISO standard called SGML – Standard Generalized Markup Language). Content displayed on the Internet first had to be organised according to HTML standards. HTML, as the basis of the World Wide Web, paved the way for the Internet's exponential growth.

Since its first version, HTML has been constantly upgraded with new features. The growing relevance of the Internet has put the question of the standardisation of HTML into focus. This was particularly relevant during the 'Browser Wars' between Netscape and Microsoft, when each company tried to strengthen its market position by influencing HTML standards. While basic HTML only handled text and photos, new Internet applications required more sophisticated standards for managing databases, video, and animation. Such a variety of applications required considerable standardisation efforts in order to ensure that Internet content could be properly viewed by the majority of Internet browsers.

Application standardisation entered a new phase with the emergence of XML, which provided greater flexibility in the setting of standards for Internet content. New sets of XML standards have also been introduced. For example, the standard for the distribution of wireless content is called Wireless Markup Language (WML).

Application standardisation is carried out mainly within the framework of the World Wide Web Consortium (W3C), headed by Tim Berners-Lee. It is interesting to note that in spite of its high relevance to the Internet, so far W3C has not attracted much attention in the debate on Internet governance.

Cloud computing

The term 'cloud computing' is used to describe a recent trend in the computer industry based on the use of computer applications as services delivered from huge server farms (a collection of computer servers maintained by an enterprise to accomplish server needs far beyond the capability of one machine). The first glimpse of cloud computing is already available with the move of e-mail from our hard disks to mail servers (Gmail, Hotmail, Yahoo!) and the use of online word processors (Wiki, Google services). Social networking applications such as Facebook and blogs have further accelerated the trend towards cloud computing. More and more of our digital assets are moving from our hard disk to the cloud. The main players in cloud computing are Google, Microsoft, Apple, Amazon, and Facebook; all either already have or plan to develop big server farms.

In the early days, there were powerful mainframe computers and dumb workstations. The power was in the centre. After that, for a long time, with PCs and Windows applications, computer power moved to the periphery.

Will cloud computing close the circle? Are we going to have a few big central computers/server farms and billions of dumb units in the form of notebooks, monitors, and mobile phones? The answer to this and other questions will take time. Currently, we can identify a few Internet governance issues which are very likely to emerge in parallel with the development of cloud computing.

1. With more services delivered online, modern society will increase its dependence on the Internet. In the past, when the Internet went down we weren't able to send e-mail or browse the Net. In the era of cloud computing we may not even be able to write text or do calculations. This higher dependence on the Internet will imply higher pressure on its robustness and reliability. It will inevitably lead towards a stronger Internet governance regime and greater involvement of governments.
2. With more of our personal data stored in clouds, the question of privacy and data protection will become central. Will we have control of our text files, e-mails, and other data? Could cloud operators use them without our permission? Who will have access to our data?
3. With a growing volume of social assets going digital, countries may become uncomfortable with having national assets outside national 'borders'. They may try to create national or regional clouds or make sure that existing clouds are managed with some international supervision. Nationalisation of clouds could be further accelerated by the fact that all main operators in this field are based in the United States. Some argue that the current ICANN-centred debate may be replaced by an Internet governance debate on the regulation of cloud computing.
4. With diverse operators of cloud computing, the question of standards is becoming very important. The adoption of common standards will ensure a smooth transfer of data among different clouds (e.g. from Google to Apple). One possibility that is being discussed is the adoption of open standards by the main players in cloud computing.

See Section 6 for further discussion on the Safe Harbor Agreement

When it comes to cloud computing there are more questions than answers. The Internet governance of cloud computing is likely to emerge through the interplay of various actors and bodies. For example, the EU is concerned with privacy and data protection. The Safe Harbor Agreement, which was supposed to solve the problem of different privacy regimes in the USA and the EU does not work well. With more digital data crossing the Atlantic Ocean, the EU and the USA will have to address the question of protection of privacy according to EU standards by US companies, the main operators in cloud computing. When it comes to standards, it is very likely that the main companies will

agree among themselves. Google has already started a strong push towards open standards by establishing the Data Liberation Front aimed at ensuring a smooth transition of data between different clouds. These are the first building blocks that will address the question of the Internet governance of cloud computing. Others are likely to emerge as a solution for concrete policy problems.

Convergence: Internet – telecommunication – multimedia

Historically, telecommunication, broadcasting, and other related areas were separate industry segments; they used different technologies and were governed by different regulations. The broad and prevailing use of IP has started their convergence. Today, we can make telephone calls, watch TV, and share music on our computers via the Internet. Only a few years ago they would have been handled by different systems.

In the field of traditional telecommunication, the main point of convergence is VoIP. The growing popularity of VoIP systems such as Skype is based on lower price, the possibility of integrating data and voice communication lines, and the use of advanced PC-based tools. With YouTube and similar services, the Internet is also converging with traditional multimedia and entertainment services. While technical convergence is going ahead at a rapid pace, its economic and legal consequences will require some time to evolve.

The issues

The economic implications of convergence

At an economic level, convergence has started to reshape traditional markets by putting companies that previously operated in separate domains into direct competition. Companies use different strategies. The most frequent approach is merger and acquisition. For example, the merger of America Online and Time Warner was aimed at combining telecommunication with media/entertainment. Now, AOL/Time Warner has gathered ISPs, television, music, and software development under one corporate umbrella.

The need for a legal framework

The legal system was the slowest to adjust to the changes caused by technological and economic convergence. Each segment – telecommunication, broadcasting, and information delivery – has its own special regulatory framework.

This convergence opens up several governance and regulatory questions:

- What is going to happen to the existing national and international regimes in such fields as telephony and broadcasting?
- Will new regimes be developed that focus mainly on the Internet?
- Should the regulation of convergence be carried out by public authorities (states and international organisations) or through self-regulation?

Some countries, like Malaysia and Switzerland, as well as the EU, have started providing answers to these questions. Malaysia adopted the Communications and Multimedia Act in 1998, establishing a general framework for the regulation of convergence. The new EU framework directives, now being transposed into national laws, are also a step in this direction, as are the Swiss telecommunication laws and regulations.

The risk of convergence: merger of cable operators and ISPs

In many countries, broadband Internet has been introduced via cable networks. This is especially true in the USA, where cable Internet is much more prevalent than ADSL (asymmetric digital subscriber line), the other main Internet broadband option. What are the risks associated with this convergence?

Some parties argue that the cable operators' buffering between users and the Internet could challenge the network neutrality principle.

The main difference between ADSL and cable is that cable is not regulated by so-called 'common carrier' rules. These rules, applicable to the telephony system, specify that access should be non-discriminatory. Cable operators are not subject to these rules, and so have complete control over their subscribers' Internet access. They can block the use of certain applications and control access to certain materials. Surveillance possibilities and consequently the ability to violate privacy are much greater with the cable Internet since access is controlled through a system similar to local area networks, which provides a high level of direct control of users.

In a paper on this issue, the American Civil Liberties Union provides the following example of the risks of cable Internet monopolies:

> *This is like the phone company being allowed to own restaurants and then provide good service and clear signals to customers who call Domino's and frequent busy signals, disconnects and static for those calling Pizza Hut.*[54]

This convergence problem will be solved when a decision is made on whether the cable Internet is an 'information service' or a 'telecommunication service'. If the latter, it will have to be regulated through common carrier rules.

Cybersecurity

The current situation

The Internet was originally designed for use by a closed circle, mainly of academics without security concerns. They communicated openly and addressed possible security problems informally.

Cybersecurity came into sharper focus with the rapid expansion of the Internet user base. The Internet reiterated the old truism that technology can be both enabling and threatening. What can be used to the advantage of society can also be used to its disadvantage.

One side effect of the rapid integration of the Internet in almost all aspects of human activity is the increased vulnerability of modern society. The Internet is a part of the critical global infrastructure. Other core services of modern society, such as electric grids, transport systems, and health services, are increasingly dependent on the Internet. They are frequent targets of cyberattacks.

Cybersecurity issues can be classified according to three criteria:

1. **Type of action.** Classification based on type of action may include data interception, data interference, illegal access, spyware, data corruption, sabotage, denial-of-service, and identity theft.
2. **Type of perpetrator.** Possible perpetrators might include hackers, cybercriminals, cyberwarriors, and cyberterrorists.
3. **Type of target.** Potential targets are numerous, ranging from individuals, private companies, and public institutions to critical infrastructures, governments, and military assets.

Cybersecurity policy initiatives

Many national, regional, and global initiatives focus on cybersecurity. At national level, a growing volume of legislation and jurisprudence deals with cybersecurity. The most prominent legal initiatives are those in the United States linked to the fight against terrorism where the Department of Homeland Security is the main institution dealing with questions of

cybersecurity. It is difficult to find any developed countries without some initiative focusing on cybersecurity.

At international level, ITU is the most active organisation; it has produced a large number of security frameworks, architectures, and standards, including X.509, which provides the basis for the public key infrastructure (PKI), used, for example, in the secure version of HTTP(S) (HyperText Transfer Protocol (Secure)). Recently, ITU moved beyond strictly technical aspects and launched the ITU Global Cybersecurity Agenda.[55] This initiative encompasses legal measures, policy cooperation, and capacity building.

The G8 also has a few initiatives in the field of cybersecurity designed to improve cooperation between law enforcement agencies. It formed a Subgroup on High Tech Crime to address the establishment of 24/7 communication between the cybersecurity centres of member states, the training of staff, and the improvement of state-based legal systems to combat cybercrime and promote cooperation between the ICT industry and law enforcement agencies.

The United Nations General Assembly has passed several resolutions on a yearly basis on 'developments in the field of information and telecommunications in the context of international security', specifically resolutions 53/70 (1998), 54/49 (1999), 55/28 (2000), 56/19 (2001), 57/239 (2002) and 58/199 (2003). Since 1998, all subsequent resolutions have included similar content, without any significant improvements. Apart from these routine resolutions, the main breakthrough was in the recent set of recommendations for negotiations of the cybersecurity treaty, which were submitted to the UN Secretary General by 15 member states, including all permanent members of the UN Security Council.

See Section 3 for further discussion on cybercrime

A major international legal instrument related to cybersecurity is the Council of Europe's Convention on Cybercrime, which entered into force on 1 July 2004.[56] Some countries have established bilateral arrangements; for example, the United States has bilateral agreements on legal cooperation in criminal matters with more than 20 other countries.[57] These agreements also apply in cases of cybercrime.

One attempt by academics and non-state actors to draft an international agreement is the Stanford Draft Convention on Protection from Cyber Crime and Terrorism. This draft recommends the establishment of an international body: the Agency for Information Infrastructure Protection (AIIP).

The issues

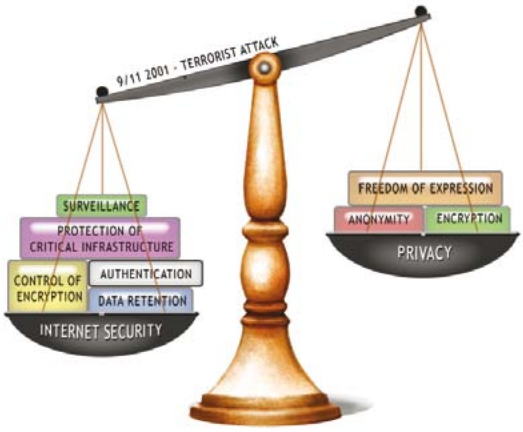
Influence of Internet architecture on cybersecurity

The very nature of how the Internet is organised affects its security. Should we continue with the current approach of building security on a pre-existing non-secure foundation or modify the basis of the Internet's infrastructure? How would such a change affect other features of the Internet, especially its openness and transparency? Most of the past development of Internet standards aimed at improving performance or introducing new applications; security was not a priority.

It is unclear whether IETF will be able to change e-mail standards to provide proper authentication and, ultimately, reduce the misuse of the Internet (e.g. spam, cybercrime). Given the controversy surrounding any changes to basic Internet standards, it is likely that security-related improvements in basic Internet protocol will be gradual and slow.

Future development of e-commerce demands a high level of cybersecurity

Cybersecurity is often mentioned as one of the preconditions for the rapid growth of e-commerce. Without a secure and reliable Internet, customers will be reluctant to provide confidential information online, such as credit card numbers. The same applies to online banking and the use of electronic money. If general cybersecurity only improves slowly (with, for example, a lack of standards), it is likely that the business sector will push for faster developments. It may lead towards further challenges for the principle of network neutrality and the development of 'a new Internet', which would, among other things, facilitate more secure Internet communication.



Cybersecurity and privacy

Another debated issue is the relationship between security and privacy. Will additional cybersecurity measures imply some loss of privacy? What regulation should apply to encryption software, which can be used both for the legitimate protection of communication privacy and for the protection of communication by terrorists and criminals? The answers to these and other questions depend on the constantly shifting balance between cybersecurity and privacy.

See Section 6 for further discussion on freedom of expression

In the aftermath of the terrorist attack in New York in September 2001, security became a priority, which was reflected in the adoption of various national acts specifying, among other things, higher levels of Internet surveillance. The reaction of civil society focused on the dangers to privacy and to the concept of freedom of expression.

At international level, the question of balancing cybersecurity with protection of privacy has been the focus of discussions regarding the extension of the Council of Europe Convention on Cybercrime to global level. The main objection from human rights activists is that the Convention addresses cybersecurity issues at the expense of the protection of privacy and other human rights.

Encryption

One of the central points of discussion on Internet security is encryption, which deals with tools that can be used for the protection of data communications.

Encryption software scrambles electronic communication (e-mail, images) into unreadable text by using mathematical algorithms. The balance between the need to keep some information confidential and the need for governments to monitor potential criminal and terrorist activity remains an issue.

The international aspects of encryption policy are relevant to the discussion of Internet governance inasmuch as the regulation of encryption should be global, or at least, involve those countries capable of producing encryption tools.

For example, the US policy of export control of encryption software was not very successful because it could not control its international distribution. US software companies initiated a strong lobbying campaign arguing that export controls do not increase national security but rather undermine US business interests.

International regimes for encryption tools

Encryption has been tackled in two contexts: the Wassenaar Arrangement and the OECD. The Wassenaar Arrangement is an international regime adopted by 33 industrialised countries to restrict the export of conventional weapons and 'dual use' technologies to countries at war or considered to be 'pariah states'. The arrangement established a secretariat in Vienna. US lobbying, with the Wassenaar Group, was aimed at extending the 'Clipper approach'[58] internationally, by controlling encryption software through a key escrow. This was resisted by many countries, especially Japan and the Scandinavian countries.

A compromise was reached in 1998 through the introduction of cryptography guidelines, which included dual-use control list hardware and software cryptography products above 56 bits. This extension included Internet tools, such as web-browsers and e-mail. It is interesting to note that this arrangement does not cover 'intangible' transfers, such as downloading. The failure to introduce an international version of Clipper contributed to the withdrawal of this proposal internally in the USA itself. In this example of the link between national and international arenas, international developments had a decisive impact on national ones.

The OECD is another forum for international cooperation in the field of encryption. Although the OECD does not produce legally binding documents, its guidelines on various issues are highly respected. They are the result of an expert approach and a consensus-based decision-making process. Most of its guidelines are eventually incorporated into national laws. The question of encryption was a highly controversial topic in OECD activities. It was initiated in 1996 with a US proposal for the adoption of a key escrow as an international standard. Similarly to Wassenaar, negotiations on the US proposal to adopt a key escrow with international standards were strongly opposed by Japan and the Scandinavian countries. The result was a compromise specification of the main encryption policy elements.

A few attempts to develop an international regime for encryption, mainly within the context of the Wassenaar Arrangement, did not result in the development of an effective international regime. It is still possible to obtain powerful encryption software on the Internet.

Spam

The current situation

Spam is usually defined as unsolicited e-mail, which is sent to a wide number of Internet users. While mainly used for commercial promotion, its other uses include social activism, political campaigning, and the distribution of pornographic materials. Spam is classified in the infrastructure basket because it affects the normal functioning of the Internet by impeding one of the Internet's core applications: e-mail. It is one of the Internet governance issues that affect almost everyone who connects to the Internet. According to the statistics from 2009, 81% of e-mail traffic is spam. The volume of spam between 2008 and 2009 increased 24%. Besides the fact that it is annoying for users, spam also causes considerable economic loss, both in terms of bandwidth used and time lost checking/deleting it.

Spam can be combated through both technical and legal means. On the technical side, many applications for filtering messages and detecting spam are available. The main problem with filtering systems is that they are known to delete non-spam messages, too. The anti-spam industry is a growing sector, with increasingly sophisticated applications capable of distinguishing spam from regular messages. Technical methods have only a limited effect and require complementary legal measures.

On the legal side, many nation states have reacted by introducing new anti-spam laws. In the USA, the Can-Spam law involves a delicate balance between allowing e-mail-based promotion and preventing spam.[59] Although the law prescribes severe sentences for distributing spam, including prison terms of up to five years, some of its provisions, according to critics, tolerate or might even encourage spam activity. The starting, default, position set out in the law is that spam is allowed until the receiver of spam messages says 'stop', i.e. uses an opt-out clause. Since the law was adopted in December 2003, spam statistics have not evidenced a decrease in the number of spam messages.

In July 2003, the EU introduced its own anti-spam law as part of its directive on privacy and electronic communications. The EU law encourages self-regulation and private sector initiatives that would lead to a reduction in spam.[60] In

Spam and 'policy fashion'

Spam is an illustrative example of the trends and, sometimes, the fashion in global policy. In 2005, spam was listed as a significant Internet governance issue in the WGIG Report. Spam was discussed at WSIS Tunis and at numerous international meetings. It was also frequently covered in the media.

Since 2005, the volume of spam has increased six times, according to conservative estimates (2005: 30 billion messages per day; 2010: 183 billion messages per day). The policy relevance of spam does not follow this trend. Spam now has a very low visibility in global policy processes. At the 2009 IGF at Sharm El Sheikh, there wasn't one workshop or session discussing spam. The global policy relevance of spam has obviously yet to be discovered.

November 2006, the European Commission adopted its Communication on fighting spam, spyware, and malicious software. The Communication identifies a number of actions to promote the implementation and enforcement of the existing legislation outlined above, as the lack of enforcement is seen as the main problem.[61]

The international response

Both of the anti-spam laws adopted in the USA and in the EU have one weakness: a lack of provision for preventing cross-border spam. This issue is particularly relevant to some countries, such as Canada, which, according to the latest statistics, receives 19 out of 20 of its spam messages from abroad. The Canadian Industry Minister, Lucienne Robillard, stated that the problem cannot be solved on a 'country by country' basis. A global solution is required, implemented through an international treaty or some similar mechanism.

A Memorandum of Understanding (MoU) signed by Australia, Korea, and the UK is one of the first examples of international cooperation in the anti-spam campaign.

The OECD established a task force on spam and prepared an anti-spam toolkit. ITU has also been proactive by organising the Thematic Meeting on Countering Spam (2004) for considering various possibilities of establishing a global MoU on combating spam. At regional level, the EU established the Network of Anti-Spam Enforcement Agencies and APEC (Asia-Pacific Economic Cooperation) prepared a set of consumer guidelines.

Another possible anti-spam approach was undertaken by the leading Internet companies that host e-mail accounts: America Online, British Telecom, Comcast, EarthLink, Microsoft, and Yahoo! They established the Anti-Spam Technical Alliance (ASTA) with the main task of coordinating technical and policy-related anti-spam activities.

The issues

Different definitions of spam

Different understandings of spam affect the anti-spam campaign. In the USA, a general concern about the protection of the freedom of speech and the First Amendment also affect the anti-spam campaign. US legislators consider spam to be only 'unsolicited commercial e-mail' leaving out other types of spam, including political activism and pornography. In most other countries, spam is considered to be any 'unsolicited bulk e-mail' regardless of its content. Since most spam is generated from the USA, this difference in definitions seriously limits any possibility of introducing an effective international anti-spam mechanism.

Spam and e-mail authentication

One of the structural enablers of spam is the possibility of sending e-mail messages with a fake sender's address. There is a possible technical solution to this problem, which would require changes in existing Internet e-mail standards. IETF is working on introducing changes to the e-mail protocol, which would ensure the authentication of e-mail. This is an example of how technical issues (standards) can affect policy. A possible trade-off that the introduction of e-mail authentication would bring is the restriction of anonymity on the Internet.

The need for global action

Most spam originates from outside a given country. It is a global problem requiring a global solution. There are various initiatives that could lead towards improved global cooperation. Some of them, such as bilateral MoUs, have already been mentioned. Others include such actions as capacity building and information exchange. A more comprehensive solution would involve some sort of global anti-spam instrument. So far, developed countries prefer the strengthening of national legislations coupled with bilateral or regional anti-spam campaigns. Given their disadvantaged position of receiving a 'global public bad' originating mainly from developed countries, most developing countries are interested in shaping a global response to the spam problem.

Endnotes

1 The terms 'Internet' and 'World Wide Web' are sometimes used interchangeably; however, there is a difference. The Internet is a vast network of networks; it covers a number of different services. Sometimes, the term 'Internet' is used to encompass everything, including infrastructure, applications (e-mail, ftp, Web), and content. The World Wide Web is just one of many Internet applications, a system of interlinked documents connected with the help of HyperText Transfer Protocol (HTTP).

2 Internet transfer via an electric grid is called powerline communication (PLC). The use of the power grid would make the Internet more accessible to many users. For a technical and organisational review of this facility, see: Internet Society (2003) *Addressing the digital divide with IPv6-enabled broadband power line communications.* ISOC Member Briefing No. 13. Available at: **http://www.isoc.org/briefings/013/**

3 The liberalisation of telecommunication markets of WTO members was formalised in 1998 in the Basic Telecommunication Agreement (BTA). Following the adoption of the BTA, more than 100 countries began the liberalisation process, characterised by the privatisation of national telecommunication monopolies, the introduction of competition, and the establishment of national regulators. The agreement is formally called The Fourth Protocol to the General Agreement on Trade in Services (adopted on 30 April 1996 and entered into force on 5 February 1998). Available at: **http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm**

4 For more information about WTO's role in the field of telecommunication, see: **http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm**

5 The common opinion is that states may collect more revenue from the market monopoly of the national operators; opponents argue that with the liberalisation of market, the overall market value rises, thus bringing more income to the state than in the case of monopoly.

6 The current RIRs are: ARIN (the American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Caribbean IP Address Regional Registry), RIPE NCC (Reseaux IP Européens Network Coordination Centre – covering Europe and the Middle East) and AFRINIC (the African Network Information Centre). A detailed explanation of the RIR system is available at: **https://www.ripe.net/info/resource-admin/rir-system.html**

7 For a detailed discussion on IPv6, see: Kissangou JP, Guthrie M, Njiraini M (2005) *IP allocation and IPv6*, part of the 2005 Internet Governance Capacity Building Programme. Available at: **http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84**

8 For a comprehensive and highly technical survey of TCP/IP security, see: Chambers C, Dolske J, Iyer J (ND) *TCP/IP Security, Department of Computer and Information Science,* Ohio State University: Columbus, OH, USA. Available at: **http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html**

9 Abbate J (1999) *Inventing the Internet*. MIT Press: Cambridge, MA, USA.

10 An overview of the gTLDs with a link to the list of all TLDs is available at: **http://www.icann.org/registries/about.htm**

[11] One previous example of content-related domains is kids.us domain. The US Congress adopted a law introducing the domain reserved for child-friendly content. The main difficulty with this proposal is deciding what constitutes child-friendly content. Controversial conceptual and practical problems related to content control could ensue. So far, the 'kids' domain has only been used as part of the US country domain.

[12] The US government did not follow the ICANN decision-making procedures during discussions on the.xxx domain. US opposition was voiced through a letter sent by the US Department of Commerce to the Chairman of ICANN.

[13] The application form for the registration of the .cat domain is available at: **http://www.icann.org/tlds/stld-apps-19mar04/cat.htm**

[14] The IANA Report on the ccTLD for Palestine is available at: **http://www.iana.org/reports/ps-report-22mar00.htm**

[15] For example, South Africa used its sovereign rights as an argument in winning back control of its country domain. A newly enacted law specifies that the use of the country domain outside the parameters prescribed by the South African government will be considered a crime. The Brazilian model of the management of country domains is usually cited as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains is open to all key players, including government authorities, the business sector, and civil society. Cambodia's transfer of country domain management from non-governmental to governmental control is often cited as an example of an unsuccessful transition. The government reduced the quality of services and introduced higher fees, which have made the registration of Cambodian domains much more difficult. For more information, see: Alfonso CA (2004) *BR: CCTLD* An asset of the commons, in *Internet Governance: A grand collaboration*. MacLean D (ed.). UNICT Task Force: New York, NY, USA, pp. 291–299; Klein N (2004) Internet governance: Perspectives from Cambodia, in *Internet Governance: A grand collaboration*. *op. cit.*

[16] ICANN (2000) *Principles for the Delegation and Administration of Country Code Top-Level Domains,* currently being redrafted. Available at: **http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm**

[17] The list of root zone servers, their nodes and positions, and managing organisations is available at: **http://www.root-servers.org/**

[18] ICANN (2009) Available at: **http://www.icann.org/en/announcements/announcement-30sep09-en.htm**

[19] The section on network neutrality is based on the writings of Vladimir Radunovic, Coordinator of DiploFoundation's Internet governance project.

[20] In the long history of the Internet, the United States has never block ed access to another country, including countries in conflict. In some cases, like the 1999 Kosovo war, the UN sanctions regime provided the United States with the legal possibility of cutting telecommunication links to Serbia. It did not use this legal possibility and Serbia had access to the Internet throughout the conflict.

[21] Arrington M (2009) YouTube video streams top 1.2 billion/day. TechCrunch. Available at: **http://techcrunch.com/2009/06/09/youtube-video-streams-top-1-billionday/**

[22] Broadcasting Ourselves. The office YouTube Blog (2009) Zoinks! 20 hours of video uploaded every minute! Available at: **http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.html**

[23] America insists on net neutrality: the rights of bits. *The Economist* 24 September 2009.

[24] The case had several turn-overs. For more information on the case background, see: Broache A (2008) FCC wants to know: Is degrading P2P traffic 'reasonable'? Cnet News Blog. Available at: **http://news.cnet.com/8301-10784_3-9850611-7.html?tag=mncol;txt**.

The most recent update was the decision of the court against the previous FCC ruling. See: Kang C (2010) Court rules for Comcast over FCC in 'net neutrality' case. *The Washington Post*, 7 April. Available at: **http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html**

[25] Save the Internet is particularly active in advocating network neutrality as preserving the free and open Internet. Available at: **http://www.savetheinternet.com/**

[26] The Internet Governance Caucus (IGC) was originally created by individual and organisational civil society actors who came together in the context of the WSIS to promote global public interest objectives in Internet governance policy-making. Available at: **www.igcaucus.org**

[27] John Herrman illustrates the package offers often used by network neutrality proponents. Available at: **http://gizmodo.com/5391712/net-neutrality-worst-case**

[28] *La Quadrature du Net*, an advocacy group that promotes the rights and freedoms of citizens on the Internet, states within its open letter to the European Parliament on Network Neutrality: *everyone around the globe has access to the same Internet, and even the smallest entrepreneurs are on equal footing with the leading global enterprises*. Available at: **http://www.laquadrature.net/en/we-must-protect-net-neutrality-in-europe-open-letter-to-the-european-parliament#**

[29] Ogg E (2010) *Report: Google, Verizon reach Net neutrality deal*. CNet 4 August. Available at: **http://news.cnet.com/8301-31021_3-20012703-260.html?tag=mncol;mlt_related**

[30] Those elements that are still controversial and to be negotiated about in future are in square brackets.

[31] Reports from these meetings, as well as other relevant related materials on network neutrality, are available at: **www.diplomacy.edu/ig/nn**

[32] FCC (2005) Policy paper on network management and neutrality. Available at: **http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf**

[33] Ministry of Internal Affairs and Communications, Japan (2007) *Report on Network Neutrality*. Available at: **www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf**

[34] PTS (2009) *Open Networks and Services.* Available at: **http://www.pts.se/en-gb/Documents/Reports/Internet/2009/Open-Networks-and-Services---PTS-ER-200932/**

[35] Kroes N (2010) *Net neutrality in Europe*. Speech given by Vice President of the European Commission Commissioner for the Digital Agenda. Available at: **http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/153&format=HTML&aged=0&language=EN&guiLanguage=en**

[36] NPT (2009) *Net neutrality: Guidelines for Internet neutrality.* Available at: **http://www.npt.no/ikbViewer/Content/109604/Guidelines%20for%20network%20neutrality.pdf**

[37] Anderson N (2009) Norway gets net neutrality – voluntary, but broadly supported. *Ars Technica.* Available at: **http://arstechnica.com/tech-policy/news/2009/02/norway-gets-voluntary-net-neutrality.ars**

[38] ISOC considers the concept of network neutrality as rather ill-defined, and instead discusses the continued open inter-networking. Available at: **http://www.isoc.org/pubpolpillar/usercentricity/openinternetworking.shtml**. Its 16 May 2010 Public consultation on Net Neutrality states: *Rather than focusing simply on the range of possible Network Neutrality definitions, the Internet Society believes it is more appropriate to concentrate more broadly on the imperative of preserving the open, user-centric Internet model that has been so successful to date*. Available at: **http://www.isoc.org/regions/europe/docs/netneutrality_20100516_en.pdf**

[39] *TACD calls for Net Neutrality.* Available at: **http://tacd.org/index.php?option=com_content&task=view&id=162&Itemid=43**

[40] Williams F (2006) ISPs should be liable for spam, says UN report. *Financial Times,* 8 November. Available at: **http://www.qlinks.net/quicklinks/spam.htm**

[41] Shannon V (2006) The end user: Junk payout in spam case. *International Herald Tribune,* 13 April. Available at: **http://www.iht.com/articles/2006/04/12/business/PTEND13.php**

[42] Peering is 'a bi-lateral agreement made by network operators to guarantee access to each others' customers at no cost to either party', as defined by HSC Group (**www.hscgroup.co.uk**). The peering arrangement is a mutual benefit, and is also common among ISPs, as well as telecom operators.

[43] Tier 2 IBPs are usually called ICP (Internet connection points) or Internet gateways.

[44] Andrew Odlyzko views the question of pricing and architecture on the Internet from a historical perspective. Identifying the thread in the pricing policy from the pricing of transportation systems in the ancient world, he links with the current Internet pricing policy. Odlyzko A (2004) *Pricing and architecture of the Internet: Historical perspectives from telecommunications and transportation.* University of Minnesota: Minneapolis, MN, USA. Available at: **http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf**

[45] Shawn O'Donnell, in the article *An economic map of the Internet*, provides an analysis of how the Internet dollar flows, explaining where the consumer's ISP dollar goes. Available at: **http://ebusiness.mit.edu/research/papers/162_ODonnell_Map.pdf**

[46] Nguyen TT, Armitage GJ (2005) Evaluating Internet pricing schemes: A three-dimensional visual model. *ETRI Journal* **27**: 64–74.

[47] The bandwidth market website is an online market of Internet resources, offering bandwidth, Internet access, and other Internet resources. Available at: **http://www.bandwidthmarket.net/**

[48] Huston G (2005) Where's the money? – Internet interconnection and financial settlements. The ISP Column, Internet Society. Available at: **http://ispcolumn.isoc.org/2005-01/interconns.pdf**

[49] AfrISPA (2002) The halfway proposition: Background paper on reverse subsidy of G8 countries by African ISPs, presented at the Conference of African Ministers of Finance, Planning and Economic Development, Johannesburg, South Africa, 19 October 2002. Available at: **http://www.wougnet.org/WSIS/ug/WSIS2005/docs/HalfwayProposition_Draft4.pdf**

[50] For a comprehensive survey of interconnection costs, see: Esmat B, Fernandez J (2006) International Internet Connections Costs, in Drake WJ (2006) *Reforming Internet Governance: Perspectives from the Working Group on Internet Governance* (WGIG). WGIG: New York, NY, USA, pp. 73–86. Available at: **http://www.wgig.org/book-Launch.html**

[51] You can find a comprehensive analysis of the topic in Jensen M (2005) Interconnection Costs. APC: Melville, South Africa. Available at: **http://www.apc.org/en/pubs/issue/accessibility/all/interconnection-costs**

[52] Huston (2005) *op. cit.* pp. 7–9.

[53] One of the limitations of negotiating this issue between governments is that most interconnection agreements are concluded between private telecommunication operators. They are often confidential.

[54] ACLU White paper (ND) *No competition: How monopoly control of the broadband Internet threatens free speech*. ACLU: New York, NY, USA.

[55] For more information on the ITU Global Cybersecurity Agenda, see: **http://www.itu.int/osg/csd/cybersecurity/gca/**

[56] The convention text is available at: **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm**

[57] The official name of these instruments is the Mutual Legal Assistance in Criminal Matters Treaties (MLATs).

[58] The Clipper approach was proposed by the US government back in 1993. At its core was the use of a Clipper chip which was supposed to be used in all telephones and other voice communication tools. The Clipper chip had a 'back door' which could be used by governments for lawful surveillance. After strong opposition from human rights activists and the general public, the US government dropped this proposal in 1995. See: Denning D (1995) The case for clipper. *MIT Technology Review*. MIT: Cambridge, MA, USA. Available at: **http://encryption_policies.tripod.com/us/denning_0795_clipper.htm**

[59] More references to Can-Spam are available at: **http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm**

[60] The Contact Network of Spam Enforcement Authorities (CNSA) was established in February 2005 by 13 EU countries (France, Austria, Belgium, Cyprus, the Czech Republic, Denmark, Greece, Ireland, Italy, Lithuania, Malta, the United Kingdom, and Spain). It aims to promote both cooperation among these states and coordination with entities outside the EU, such as the OECD and ITU.

[61] European Commission, Information Society (2010). *Unsolicited communication: fighting spam.* Available at: **http://ec.europa.eu/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm**

Section 3

The legal basket

The legal basket

Almost all Internet governance issues have a legal aspect, yet the shaping of a legal framework to mould the rapid development of the Internet is still in its early stages. The two prevalent approaches are:

1 A 'real-law' approach, where the Internet is essentially treated no differently from previous telecommunication technologies, in the long evolution from smoke signals to the telephone. Though faster and more comprehensive, the Internet still involves communication between individuals over distance. Consequently, any existing legal rules can also be applied to the Internet.[1,2]

1 A 'cyber-law' approach based on the presumption that the Internet introduces new types of social relationships in cyberspace. Consequently, there is a need to formulate new cyber laws in order to regulate cyberspace. One argument for this approach is that the sheer speed and volume of Internet-facilitated cross-border communication hinders the enforcement of existing legal rules.

Although both approaches contain valid elements, the real-law approach is gaining predominance. The general thinking is that a considerable part of existing legislation can be applied to the Internet. For certain issues, real laws would have to be adapted in order to be applicable to the cyber world. For some, limited issues, new rules must be devised.

Legal instruments

A wide variety of legal instruments exist that have either already been applied or could be applied to Internet governance.

National and community legal instruments

Legislation

Every piece of legislation consists of rules and sanctions. Rules stipulate certain socially accepted behaviours (e.g. do not commit a crime, pay your taxes) and sanctions specify punishments in case the rules are not observed (e.g. fines, imprisonment, the death penalty in some societies).

Legislative activities have progressively intensified in the Internet field. This is especially the case within Organisation for Economic Co-operation and Development (OECD) countries, where the Internet is widespread and has a high degree of impact on economic and social relations. To date, the priority areas for legislative regulations have been privacy, data protection, intellectual property, taxation, and cybercrime.

Yet, social relations are too complex to be regulated only by legislators. Society is dynamic and legislation always lags behind change. This is particularly noticeable in this day and age, when technological development reshapes social reality much faster than legislators can react. Sometimes, rules become obsolete even before they can be adopted. The risk of legal obsolescence is an important consideration in Internet regulation.

Social norms (customs)

Like legislation, social norms proscribe certain behaviour. Unlike legislation, no state power enforces those norms. They are enforced by the community through peer-to-peer pressure. In the early days, the Internet's use was ruled by a set of social norms labelled 'netiquette', where peer pressure and exclusion were the main sanctions. During this period, in which the Internet was used primarily by relatively small, mainly academic communities, social rules were widely observed. The growth of the Internet has made those rules inefficient. This type of regulation can still be used, however, within restricted groups with strong community ties.

Real law vs cyber law

Regardless of which approach is more appropriate – real law or cyber law – the general principle remains that **laws do not make prohibited behaviour impossible, only punishable.** The fact that fraud is prohibited in both the cyber world and the real world does not mean that fraud will be eradicated as a result. This distinction is relevant because one of the frequent arguments for separate cyber regulations is that prohibited behaviour (fraud, crime, etc.) is already prevalent in cyberspace and that real-law regulations cannot be efficiently used.

Self-regulation

The US government's *White Paper on Internet Governance* (1998) proposes self-regulation as the preferred regulatory mechanism for the Internet. Self-regulation has elements in common with previously described social norms. The main difference is that unlike social norms, which typically involve a diffuse regulatory system, self-regulation is based on an intentional and well-organised approach. Self-regulatory rules are usually codified in codes of practice or good conduct.

The trend towards self-regulation is particularly noticeable among Internet service providers (ISPs). In many countries, ISPs are under growing pressure from government authorities to enforce rules related to content policy; they are increasingly using self-regulation as a method of imposing certain standards of behaviour and, ultimately, preventing government interference in their activities.

While self-regulation can be a useful regulatory technique, some risks remain in using it to regulate areas of high public interest, such as content policy. It remains to be seen to what extent ISPs will be able to regulate content hosted on their websites. Can they make decisions in lieu of legal authorities? Can ISPs judge what acceptable content is? Other issues need to be addressed, too; issues such as freedom of expression and privacy.

Jurisprudence

Jurisprudence (court decisions) constitutes an important element of the US legal system, the first to address Internet legal issues. In this system, precedents create law, especially in cases involving the regulation of new issues, such as the Internet. Judges have to decide cases even if they do not have the necessary tools – legal rules.

The first legal tool judges use is legal analogy, where something new is related to something familiar. Most legal cases concerning the Internet are solved through analogies.

International legal instruments

The difference between international private law and international public law

The need for the use of international law is frequently raised in Internet governance discussions. The term 'international law' is mainly used as a synonym for international 'public law', established by nation states and international organisations, usually through the adoption of treaties and

conventions. However, most possible international legal cases regarding the Internet include a strong private law feature, involving such issues as contracts and torts. In dealing with such issues, there is a need to use international private law, the rules of which are stipulated in national legislation, not in international treaties.[3] The rules of international private law specify the criteria for establishing applicable jurisdiction and law in legal cases with foreign elements (e.g. legal relations involving two or more entities from different countries). The criteria for identifying the applicable jurisdiction and law include the link between an individual and national jurisdiction (e.g. nationality, domicile) or the link between a particular transaction and national jurisdiction (e.g. where the contract was concluded, where the exchange took place).

International private law

Given the global nature of the Internet, legal disputes involving individuals and institutions from different national jurisdictions are very frequent. However, only rarely has international private law been used for settling Internet-based issues, possibly because its procedures are usually complex, slow, and expensive. The main mechanisms of international private law developed at a time when cross-border interaction was less frequent and less intensive and proportionally fewer cases involved individuals and entities from different jurisdictions.

International public law

International public law regulates relations between nation states. Some international public law instruments already deal with areas of relevance to Internet governance (e.g. telecommunication regulations, human rights conventions, and international trade treaties). In this section, the analysis will focus on the elements of international public law that could be used in the field of Internet governance, including treaties and conventions , customs, 'soft law', and *ius cogens* (compelling law – a peremptory norm).

International conventions

The main set of conventions on Internet-related issues was adopted by the Information Telecommunication Union (ITU), with the International Telecommunication Regulation (1988) being the most important for preparing a telecommunication policy framework for subsequent Internet developments. Apart from the ITU conventions, the only convention that deals directly with Internet-related issues is the Council of Europe Convention on Cybercrime. However, many other international legal instruments address broader aspects of Internet governance, such as human rights, trade, and intellectual property rights.

International customary law

The development of customary rules includes two elements: general practice *(consuetudo)* and recognition that such practice is legally binding *(opinio juris)*. It usually requires a lengthy time-span for the crystallisation of general practice.

Some elements of emerging custom appear in the way the US government exercises oversight of the Internet root. It has a consistent practice of non-intervention in the issue of national domains in the Internet root zone file. General practice is the first element in identifying customary law. It remains to be seen if such general practice was based on awareness by the US government that it was in line with international legal rules (existence of *opinio iuris*). If this is the case, there is the possibility of identifying international customary law in managing parts of the Internet root server system that deal with the country domains of other countries. It would be difficult to extend such reasoning to the legal status of gTLDs – generic top-level domains – (.com, .org, .edu, .net) which do not involve other countries.

Soft law

'Soft law' is a frequently used term in the Internet governance debate. Most definitions of soft law focus on what it is not: it is not a legally binding instrument. Instruments of soft law contain principles and norms rather than specific rules. It is usually found in international documents such as declarations, guidelines, and model laws.

The main World Summit on the Information Society (WSIS) documents, including the Final Declaration, Plan of Action, and Regional Declarations, have the potential to develop certain soft-law norms. They are not legally binding, but they are usually the result of prolonged negotiations and acceptance by all countries. The commitment that nation states and other stakeholders put into negotiating soft-law instruments and in reaching a necessary consensus creates the first element in considering that such documents are more than simple political declarations.[4]

Soft law provides certain advantages in addressing Internet governance issues. First, it is a less formal approach, not requiring the official commitment of states and, thereby, not requiring prolonged negotiations. Second, it is flexible enough to facilitate the testing of new approaches and adjust to rapid developments in the field of Internet governance. Third, soft law provides greater opportunity for a multistakeholder approach than does an international legal approach restricted to states and international organisations.

Ius Cogens

Ius cogens is described by the Vienna Convention on the Law of Treaties as:

> *...a norm, accepted and recognised by the international community of States as a whole, from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character.*[5]

Professor Brownlie lists the following examples of *ius cogens* rules:[6]

- The prohibition of the use of force.
- The law of genocide.
- The principle of racial non-discrimination.
- Crimes against humanity.
- The rules prohibiting trade in slaves and piracy.

In Internet governance, *ius cogens* could be used for the introduction of a certain set of rules, such as the prohibition of online child pornography.

Jurisdiction

The number of Internet-related disputes has been steadily increasing, which has made the issue of jurisdiction one of the hot aspects of Internet governance. Confusion over jurisdiction can have two immediate and simultaneous consequences:

1. an inability of the state to exercise its legal power as a responsible entity in regulating social relations within its territory; and
2. an inability of individuals and legal entities to exercise their rights to justice (denial of justice).

Other consequences of ambiguous jurisdiction might be:

- Legal insecurity on the Internet, including 'forum shopping'.
- Slower development of e-commerce.
- Compartmentalisation of the Internet into legal safe zones.

Because of these consequences, the clarification of jurisdiction and its procedures is a vital matter in Internet governance.

The relationship between jurisdiction and the Internet

The relationship between jurisdiction and the Internet has a built-in ambiguity, since jurisdiction rests predominantly on the geographical division of the globe into national territories. Each state has the sovereign right to exercise jurisdiction over its territory. However, the Internet facilitates considerable cross-border exchange, difficult (although not impossible) to monitor via traditional government mechanisms. The question of jurisdiction on the Internet highlights one of the central dilemmas associated with Internet governance: how is it possible to 'anchor' the Internet within existing legal and political geography?[7]

Jurisdiction – basic techniques

Three main considerations are important when thinking about jurisdiction:

1. Which court or state authority has the proper authority (procedural jurisdiction).
2. Which rules should apply (substantive jurisdiction).
3. How to implement court decisions (enforcement jurisdiction).

The following principal criteria establish jurisdiction in particular cases:

- **Territorial Principle** – the right of the state to rule over persons and property within its territory.
- **Personality Principle** – the right of the state to rule over its citizens wherever they might be (nationality principle).
- **Effects Principle** – the right of the state to rule on economic and legal effects on its territory, stemming from activities conducted abroad.

Another important principle introduced by modern international law is that of universal jurisdiction.[8]

> *The concept of universal jurisdiction in its broad sense [is] the power of a state to punish certain crimes, wherever and by whomsoever they have been committed, without any required connection to territory, nationality, or special state interest.*[9]

Universal jurisdiction covers such crimes as piracy, war crimes, and genocide.

Conflict of jurisdiction

The principles for establishing jurisdiction (territorial, nationality, and effect) inevitably lead to situations where jurisdiction is invoked by courts from several states. Problems with jurisdiction arise when disputes involve an extra-territorial component (e.g. involving individuals from different states, or international transactions). Since all Internet content is accessible from anywhere, any Internet user may be exposed to any national jurisdiction. When placing content on the Internet, it is difficult to know which national law, if any, might be violated. In this context, almost every Internet activity has an international aspect that could lead to multiple jurisdictions or a so-called 'spill-over effect'.[10]

One of the most illustrative and frequently quoted cases that exemplify the problem of jurisdiction is the 2001 Yahoo! case in France. The Yahoo! case prosecuted in French courts reiterated the relevance of the problem of multiple jurisdictions.[11] It was prompted by a breach of French law on Nazi materials, which prohibits the exhibition and sale of such objects, even though the website that provided these items – the Yahoo.com auction website – was hosted in the USA, where the display of such materials was, and still is, legal. The court case was solved through the use of a technical solution (geo-location software and filtering of access). Yahoo! was forced to identify users who accessed from France and to block their access to web pages containing Nazi materials.[12]

Besides technical solutions (geo-location and filtering), other approaches for solving the conflict of jurisdiction include harmonisation of national laws and the use of arbitration and other dispute-resolution solutions.

See Section 2 for further discussion on cybersecurity and spam

The harmonisation of national laws could result in the establishment of one set of equivalent rules at global level. With identical rules in place, the question of jurisdiction would become less urgent. Harmonisation might be achieved in areas where a high level of global consensus already exists; for example, regarding child pornography, piracy, slavery, terrorism, and cybercrime. Views are converging on other issues, too, such as spam and cybersecurity. However, in some fields, including content policy, it is not very likely that a global consensus on the basic rules will be reached, since cultural differences continue to clash in the online environment more saliently than in the offline world.[13] Another potential consequence of a lack of harmonisation is the migration of web materials to countries with lower levels of Internet regulation. Using the analogy of the Law of the Sea, some countries might become 'flags of convenience' or the offshore centres of the Internet world.

A short overview presenting the main differences between traditional court systems and arbitration.

Elements	Court jurisdiction	Arbitration
Organisation	Settled by laws/treaties – permanent	Settled by parties (temporary, ad hoc) Settled by conventions (permanent)
Applicable law	The law of the court (the judge decides the applicable law)	Parties can choose the law; if they do not, then the law indicated in the contract; if there is no indication, then the law of the arbitration body
Procedure	Court procedures settled by laws/ treaties.	Settled by parties (temporary, ad hoc) Settled by arbitration body regulation (permanent)
Competence/ Object of dispute	Settled by laws/treaties in relation with the object of dispute	Settled by parties
Decision	Binding	Binding

Arbitration

Arbitration is a dispute-resolution mechanism, involving one or more independent arbitrators chosen by the disputants. International arbitration within the business sector has a long-standing tradition. An arbitration mechanism is usually set out in a private contract with parties agreeing to settle any future disputes through arbitration. A wide variety of arbitration contracts are available, specifying such issues as place of arbitration, procedures, and choice of law.

In comparison to traditional courts, arbitration offers many advantages, including higher flexibility, lower expenses, speed, choice of jurisdiction, and the easier enforcement of foreign arbitration awards. One of the main advantages of arbitration is that it overcomes the problem of selecting procedural and substantive jurisdictions. Both are selected in advance by the disputants. Arbitration has particular advantages in regard to one of the most difficult tasks in Internet-related court cases: enforcement of decisions (awards). The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards regulates the enforcement of arbitration awards.[14] According to this Convention, national courts are obliged to enforce arbitration awards. It is easier to enforce such awards in foreign countries by using the New York Convention regime than by using regular court judgments.

The main limitation of arbitration is that it cannot address issues of higher public interest; these require the intervention of state-established courts.

Arbitration has been used extensively in commercial disputes. A well-developed system of rules and institutions dealing with commercial disputes has been established. The main international resource is the United Nations Commission on International Trade Law (UNCITRAL) Model Law on International Commercial Arbitration (1985), supplemented by other UNCITRAL instruments.[15] The leading international arbitration bodies are usually attached to chambers of commerce, and are organised at international (e.g. the International Court of Arbitration), regional (e.g. the European Court of Arbitration), and national levels.

Arbitration and the Internet

Arbitration and other alternative dispute-resolution systems are used extensively to fill the gap engendered by the inability of current international private law to deal with Internet cases. A particular example of an alternative dispute resolution method in Internet cases is the Uniform Domain-Name Dispute-Resolution Policy (UDRP), which was developed by WIPO (World Intellectual Property Organization) and implemented by ICANN (Internet Corporation for Assigned Names and Numbers) as the primary dispute resolution procedure.[16]

The UDRP is stipulated in advance as a dispute resolution mechanism in all contracts involving the registration of gTLDs (.com, .edu, .org, .net) and for some ccTLDs (country code top-level domains) as well. Its unique aspect is that arbitration awards are applied directly through changes in the Domain Name System (DNS) without resorting to enforcement through national courts.

See Section 1 for further discussion on DNS

Arbitration provides a faster, simpler, and cheaper way of settling disputes. However, the use of arbitration as the main Internet dispute settlement mechanism has a few serious limitations. First, since arbitration is usually established by prior agreement, it does not cover a wide area of issues when an agreement between parties has not been set in advance (libel, various types of responsibilities, cybercrime).

Second, many view the current practice of attaching an arbitration clause to regular contracts disadvantageous for the weaker side in the contract (usually an Internet user or an e-commerce customer).

Third, some are concerned that arbitration extends precedent-based law (US/UK legal system) globally and gradually suppresses other national legal systems. In the case of commercial law, this might prove to be more acceptable, given the already high level of unification of substantive rules. However, it is a more delicate proposition when content and sociocultural aspects are at issue, where a national legal system reflects specific cultural content.

Copyright

Copyright only protects the expression of an idea, when it is materialised in various forms, such as a book, CD, computer file, etc. The idea itself is not protected. In practice, it is sometimes difficult to make a clear distinction between the idea and its expression.

The copyright regime has closely followed the technological evolution. Every new invention, such as the printing press, radio, television, and VCR, has affected both the form and the application of copyright. The Internet is no exception. The traditional concept of copyright has been challenged in numerous ways, from those as simple as cutting and pasting text from the Web to more complex activities, such as the distribution of music and video files via the Net without significant cost.

Paradoxically, the Internet also empowers copyright holders, by providing them with more powerful technical tools for protecting and monitoring the use of copyright material. In the most extreme case, copyright holders can prohibit access to copyrighted materials altogether, which would render the whole concept of copyright irrelevant.

Intellectual property rights (IPR)

Knowledge and ideas are key resources in the global economy. The protection of knowledge and ideas through IPR has become one of the predominant issues in the Internet governance debate, and has a strong development-oriented component.

IPR has been affected by the development of the Internet, mainly through the digitisation of knowledge and information, as well as through new possibilities for their manipulation. Internet-related IPR include copyright, trademarks, and patents. Other IPR include designs, utility models, trade secrets, geographical indications and plant varieties.

These developments endanger the delicate balance between authors' rights and the public interest, which is the very basis of copyright law.

So far, copyright holders, represented by the major record and multimedia companies, have been more proactive in protecting their interests. The public interest has only been vaguely perceived and not sufficiently protected. This has gradually been changing, however, mainly through numerous global initiatives focusing on open access to knowledge and information.

The current situation

Stricter copyright protection at national and international level

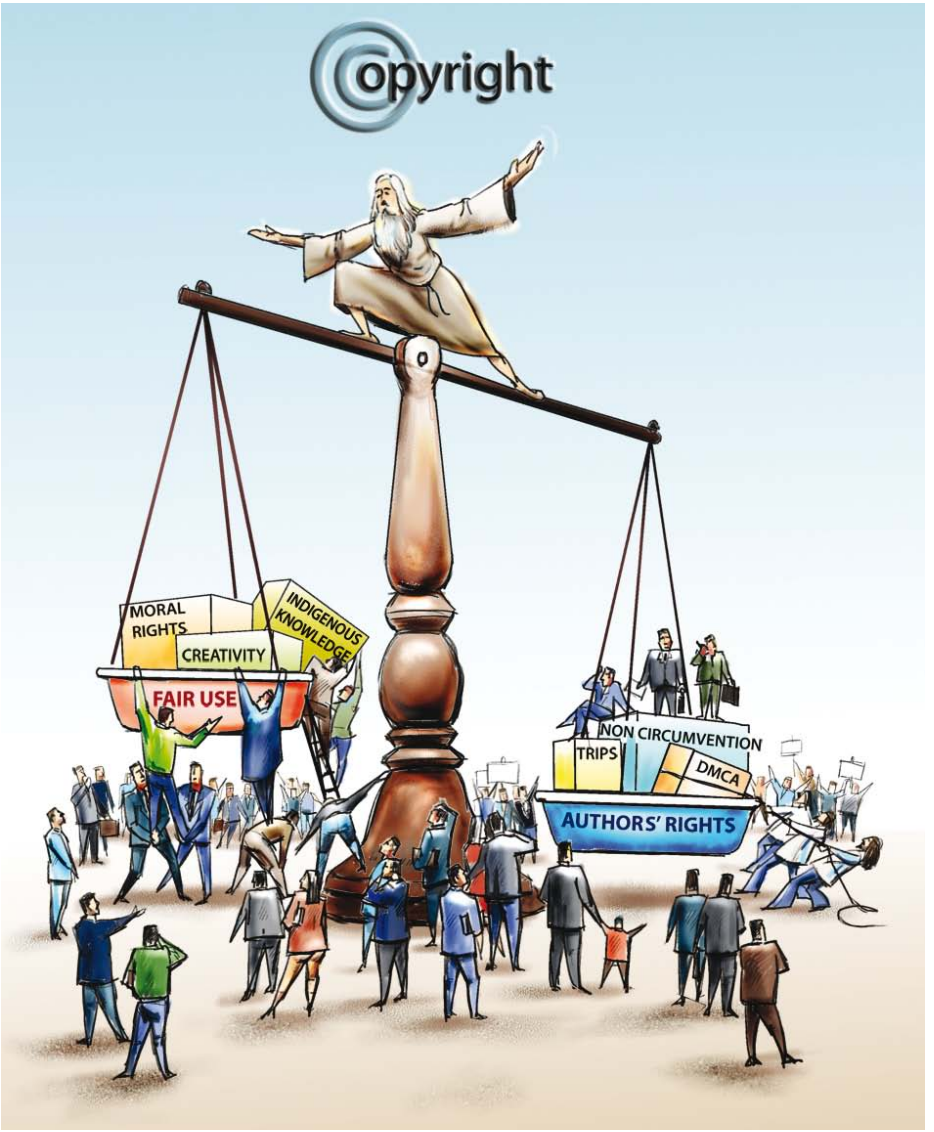
The recording and entertainment industries have been lobbying intensively at national and international level to strengthen copyright protection. In the USA, stricter protection of copyright was introduced through the US Digital Millennium Copyright Act (DMCA) of 1998. At international level, the protection of digital artefacts was introduced in the WIPO Copyright Treaty (1996). This treaty also contains provisions for tightening the copyright protection regime, such as stricter provisions for the limitations of authors' exclusive rights, the prohibition of circumventing the technological protection of copyrights, and other related measures.

The increasing number of court cases

In 2003 alone, approximately 1000 DMCA-based subpoenas against ISPs were issued, requesting them to stop their subscribers' file-sharing activities and more than 500 lawsuits against individuals were launched. A particularly relevant case to the future of copyright on the Internet is the case against Grokster and StreamCast, two companies that produce P2P (peer-to-peer) file-sharing software. Following DMCA provisions, the US Record Association requested these companies to desist from the development of file-sharing technology that contributes to copyright infringement. Initially, the US courts chose not to hold software companies like Grokster and StreamCast responsible for possible copyright infringement, under reasonable circumstances. However, in June 2005, the US Supreme Court ruled that software developers were responsible for any possible misuse of their software.

Software against copyright infringement

Tools that are used by offenders can be used by defenders, too. Traditionally, state authorities and businesses carried out their responsibilities through legal mechanisms. However, the use of 'alternative' software tools by the business sector against copyright offenders is increasing.



An article in the *New York Times* listed the following software-based tactics, used by recording/entertainment companies to protect their copyrights:[17]

- A **Trojan Horse** redirects users to websites where they can legitimately buy the song they tried to download.
- '**Freeze**' software blocks computers for a period of time and displays a warning about downloading pirated music.
- '**Silence**' software scans hard disks and an attempt is made to remove any pirated files found.

- '**Interdiction**' software prevents access to the Net for those who try to download pirated music.

Professor Lawrence Lessig of Stanford Law School has warned that such measures might be illegal. He noted that among the measures passed to deal with copyright infringement, these were not included. Would the companies that took such self-help measures be breaking the law?

Technologies for digital rights management

As a long-term and more structural approach, the business sector introduced various technologies for managing access to copyright protected materials. Microsoft introduced Digital Rights Management (DRM) software to manage the downloading of sound files, movies, and other copyrighted materials. Similar systems were developed by Xerox (ContentGuard), Philips, and Sony (InterTrust).

The use of technological tools for copyright protection received support at both international level (WIPO Copyright Treaty) and in the DMCA. Moreover, the DMCA criminalised activity that is aimed at circumventing the technological protection of copyrighted materials.

The issues

Amend existing or develop new copyright mechanisms?

How should copyright mechanisms be adjusted to reflect the profound changes effected by information and communication technology (ICT) and Internet developments? One answer suggested by the US government's *White Paper on Intellectual Property and the National Information Infrastructure*[18] is that only minor changes are needed, mainly through 'dematerialising' the copyright concepts of fixation, distribution, transmission, and publication. This approach was followed in the main international copyright treaties, including the trade-related aspects of intellectual proprerty rights (TRIPS) and WIPO Copyright Conventions.

However, the opposite view argues that changes in the legal system must be profound, since copyright in the digital era no longer refers to the 'right to prevent copying' but also to the 'right to prevent access'. Ultimately, with ever-greater technical possibilities of restricting access to digital materials, one can question whether copyright protection is necessary at all. It remains to be seen how the public interest, the second part of the copyright equation, will be protected.

Protection of the public interest – the 'fair use' of copyright materials

Copyright was initially designed to encourage creativity and invention. This is the reason why it combined two elements: the protection of authors' rights and the protection of the public interest. The main challenge was to stipulate how the public might consult copyrighted materials to enhance creativity, knowledge, and global well-being. Operationally speaking, this public interest was protected through the concept of the 'fair use' of protected materials. Fair use is defined as the 'use of copyrighted material without requiring permission from the rights holders, such as for commentary, criticism, news reporting, research, teaching or scholarship'.[19]

Copyright and development

Any restriction of fair use could weaken the position of developing countries. The Internet provides researchers, students, and others from developing countries with a powerful tool for participating in global academic and scientific exchanges. A restrictive copyright regime could have a negative impact on capacity building in developing countries.

Another aspect is the increasing digitisation of cultural and artistic crafts from developing countries. Paradoxically, developing countries may end up having to pay for their cultural and artistic heritage when it becomes digitised, repackaged, and owned by foreign entertainment and media companies.

WIPO and TRIPS

As already mentioned, two main international regimes exist for intellectual property rights. WIPO manages the traditional IPR regime, based on the Bern and Paris Conventions. Another emerging regime is run by the World Trade Organization (WTO) and based on TRIPS. The shift of international IPR coordination from WIPO to WTO was carried out in order to strengthen IPR protection, especially in the field of enforcement. This was one of the major gains of the developed countries during the Uruguay Round of the WTO negotiations.

Many developing countries are concerned with this development. WTO's strict enforcement mechanisms could reduce the manoeuvring room of developing countries and the possibility of balancing development needs with the protection of international, mainly US-based, IPR. So far, the main focus of WTO and TRIPS has been on various interpretations of IPR for pharmaceutical products. It is very likely that future discussions will extend to IPR and the Internet.

ISP's liability for copyright infringement

The international enforcement mechanisms in the field of intellectual property have been further strengthened by making ISPs liable for hosting materials in breach of copyright if the material is not removed upon notification of infringement. This has made the previously vague IPR regime directly enforceable in the Internet field.

Trademarks

Trademarks are relevant to the Internet because of the registration of domain names. In the early phase of Internet development, the registration of domain names was based on a 'first come, first served' basis. This led to cybersquatting, the practice of registering names of companies and selling them later at a higher price.

This situation compelled the business sector to place the question of the protection of trademarks at the centre of the reform of Internet governance, leading to the establishment of ICANN in 1998. In the White Paper on the creation of ICANN, the US government demanded that ICANN develop and implement a mechanism for the protection of trademarks in the field of domain names. Soon after its formation, ICANN introduced the WIPO-developed UDRP.[20]

Patents

Traditionally, a patent protects a new process or product of a mainly technical or production nature; only recently have patents been granted to software. More patent registrations result in more court cases among US software companies, involving huge sums of money.

Some patents granted for business processes have been controversial, such as British Telecom's request for licence fees for the patent on hypertext links, which it registered in the 1980s. In August 2002, the case was dismissed.[21] If British Telecom had won this case, Internet users would have to pay a fee for each hypertext link created or used. The practice of granting patents to software and Internet-related procedures has not been accepted in Europe and other regions.[22]

Cybercrime

A dichotomy between real law and cyber law exists in the discussion of cybercrime. The real-law approach stresses that cybercrime is the same as an offline crime, but is usually committed while using a computer that is most likely connected to the Internet. The crime is the same, only the tools differ. The cyber-law approach stresses that the unique elements of cybercrime warrant special treatment, especially when it comes to enforcement and prevention.

The drafters of the Council of Europe Convention on Cybercrime were closer to the real-law approach, stressing that the only specific aspect of cybercrime is the use of ICT as a means of committing crime. The convention, which entered into force on 1 July 2004, is the main international instrument in this field.[23]

The issues

Definition of cybercrime

The definition of cybercrime is one of the core issues of cyber law, since it will uphold a practical legal result by also impacting the coverage of cybercrime. If the focus is on offences committed against computer systems, cybercrime would include unauthorised access; damage to computer data or programs; sabotage to hinder the functioning of a computer system or network; unauthorised interception of data to, from, or within a system or network; as well as computer espionage. A definition of cybercrime as 'all crimes committed via the Internet and computer systems' would include a broader range of crimes, including those specified in the Convention on Cybercrime: computer-related fraud, infringements of copyright, child pornography, and network security.

Cybercrime and the protection of human rights

The Convention on Cybercrime reinforced the discussion about the balance between security and human rights. Many concerns have arisen, articulated primarily by civil society, that the convention provides state authorities with too broad a power, including the right to check hackers' computers, the surveillance of communication, and more. These broad powers could potentially endanger some human rights, particularly privacy and freedom of expression.[24] The Convention on Cybercrime was adopted by the Council of Europe, one of the most active promoters of human rights. This may help in establishing the necessary balance between the fight against cybercrime and the protection of human rights.

Gathering and preserving evidence

One of the main challenges in fighting cybercrime is gathering evidence for court cases. The speed of today's communication requires a fast response from law enforcement agencies. One possibility for preserving evidence is to be found in network logs, which provide information about who accessed particular Internet resources, and when they did so. The Convention on Cybercrime specifies the obligation to preserve Internet traffic data. This rule could affect the role of ISPs in Internet-related law enforcement activities.

Labour law

It is frequently mentioned that the Internet is changing the way in which we work. While this phenomenon requires broader elaboration, the following aspects are of direct relevance to Internet governance:

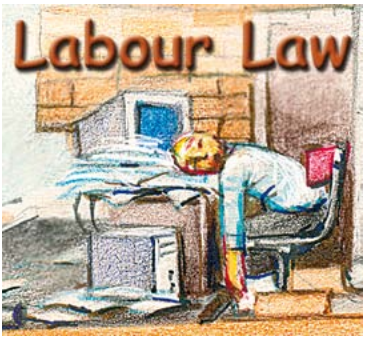
- The Internet introduced a high level of temporary and short-term workers. The term 'permatemp' was coined for employees who are kept for long periods on regularly renewed short-term contracts. This introduces a lower level of social protection of the workforce.
- Teleworking is becoming increasingly relevant with the further development of telecommunication, especially with broadband access to the Internet.
- Outsourcing to other countries in the ICT service sector, such as call centres and data processing units, is on the rise. A considerable number of these activities have already been transferred to low-cost countries, mainly in Asia and Latin America.

ICT has blurred the traditional routine of work, free time, and sleep (8+8+8 hours). It is increasingly difficult to distinguish where work starts and where it ends. These changes in working patterns may require new labour legislation, addressing such issues as working hours, the protection of labour interests, and remuneration.

In the field of labour law, one important issue is the question of privacy in the workplace. Is an employer allowed to monitor employees' use of the Internet (such as the content of e-mail messages or website access)? Jurisprudence is gradually developing in this field, with a variety of new solutions on offer.

In France, Portugal, and the United Kingdom, legal guidelines and a few cases have tended to restrict the surveillance of employee e-mail. The employer must provide prior notice of any monitoring activities. In Denmark, courts

considered a case involving an employer's dismissal for sending private e-mails and accessing a sexually oriented chat website. The court ruled that dismissal was not lawful since the employer did not have an Internet use policy in place banning the unofficial use of the Internet. Another rationale applied by the Danish court was the fact that the employee's use of the Internet did not affect his working performance.



Labour law has traditionally been a national issue. However, globalisation in general, and the Internet in particular, have led to the internationalisation of labour issues. With an increasing number of individuals working for foreign entities and interacting with work teams on a global basis, an increasing need arises for appropriate international regulatory mechanisms. This aspect was recognised in the WSIS declaration, which, in paragraph 47, calls for the respect of all relevant international norms in the field of the ICT labour market.

Endnotes

1 One of the strongest supporters of the 'real-law' approach is Judge Frank Easterbrook who is quoted as saying: 'Go home; cyberlaw does not exist.' In the article *Cyberspace and the law of the horse*, he argues that although horses were very important there was never a 'Law of the Horse'. Judge Easterbrook argues that there is a need to concentrate on the core legal instruments, such as contracts, responsibility, etc. Available at: **http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf**

2 Judge Frank Easterbrook's argument provoked several reactions, including one from Lawrence Lessig in *The law of the horse: What cyberlaw might teach.* Available at: **http://www.lessig.org/content/articles/works/finalhls.pdf**

3 A few international attempts have been made to harmonise international private law. The main global forum is the Hague Conference on International Private Law, which has adopted numerous conventions in this field.

4 There is a high frequency of the use of the word 'should' in the World Summit on the Information Society (WSIS) documents, one of the features of soft-law instruments. For more information, see: *The emerging language of ICT diplomacy – Qualitative analysis of terms and concepts.* Available at: **http://www.diplomacy.edu/IS/Language/html/words.htm**

5 Article 53 of the 1969 Vienna Convention on the Law of Treaties

6 Brownlie I (1999) *Principles of Public International Law, 5th Edn*. Oxford University Press: Oxford, UK, p. 513.

7 For more information, see:

- Salis RP (2001) *A summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving legal and business order in cyberspace: A report on global jurisdiction issues created by the Internet.* Available at: **http://www.lex-electronica.org/articles/v7-1/Salis.htm**
- Zittrain J (2006) *Jurisdiction in cyberspace,* Internet Law Program, Harvard Law School. Available at: **http://cyber.law.harvard.edu/ilaw/mexico_2006_module_9_jurisdiction**
- ABA (2002) *Jurisdiction over Internet disputes: Different perspectives under American and European law in 2002, ABA Section on International Law and Practice*. Annual Spring Meeting, New York, NY, USA, 8 May 2002. Available at: **http://www.howardrice.com/uploads/content/jurisdiction_internet.pdf**

8 Among the most important resources in this field is the *Princeton Principles on Universal Jurisdiction* (2001). Available at: **http://www1.umn.edu/humanrts/instree/princeton.html**

9 Malanczuk P (1997) *Akehurst's Modern Introduction to International Law.* Routledge: London, UK, p. 113.

10 For an overview of cases involving extraterritorial jurisdiction related to Internet content, see: Timofeeva YA (2005) Worldwide prescriptive jurisdiction in Internet content controversies: A comparative analysis. *Connecticut Journal of International Law* **20**: 199. Available at: **http://ssrn.com/abstract=637961**

[11] To follow the case development, see: **http://w2.eff.org/legal/Jurisdiction_and_sovereignty/**

[12] Other court cases include the German Federal Court of Justice case against Fredrick Toben, former German national with Australian nationality who had posted materials questioning the existence of the holocaust on an Australian-based website. Available at: **http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html**

[13] Racist content and pornography (in cases presented in notes 11 and 12) are not the only controversial issues – other examples include illegal gambling, tobacco advertising, and sale of drugs.

[14] The full text of the Convention is available at: **http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html**

[15] Other UNCITRAL instruments include UNCITRAL Arbitration Rules (1976), UNCITRAL Conciliation Rules (1980), UNCITRAL Notes on Organising Arbitral Proceedings (1996), and the UNCITRAL Model Law on International Commercial Conciliation (2002).

[16] Uniform Domain-Name Dispute-Resolution Policy, ICANN, 26 August 1999. Available at: **http://www.icann.org/udrp/udrp-policy-24oct99.htm**

[17] Sorkin AR (2003) Software bullet is sought to kill musical piracy. *New York Times* 4 May. Available at: **http://www.nytimes.com/2003/05/04/business/04MUSI.html**

[18] Available at: **http://www.uspto.gov/web/offices/com/doc/ipnii/**

[19] Available at: **http://en.wikipedia.org/wiki/Fair_use**

[20] For a comprehensive survey of the main issues involving UDRP, see: *WIPO's Overview of WIPO panel views on selected UDRP questions*. Available at: **http://arbiter.wipo.int/domains/search/overview/index.html**).

[21] Loney M (2002) *Hyperlink patent case fails to click.* CNET News.com. Available at: **http://news.com.com/2100-1033-955001.html**

[22] For more information about the debate in Europe on software patentability, see: http://swpat.ffii.org

[23] The full text of the Convention is available at: **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm**

[24] For critical views on the *Convention on Cybercrime* expressing the concern of civil society and human rights activists, see:

- Bailey C (2002) *Report on the Cybercrime Convention*. The Association for Progressive Communication. Available at: **http://rights.apc.org/privacy/treaties_icc_bailey.shtml**
- TreatyWatch.org website (2010). Available at: **http://www.treatywatch.org/**

Section 4

The economic basket

The economic basket

E-commerce has been one of the main engines promoting the growth of the Internet over the last 15 years. Its importance is illustrated by the title of the document that initiated the reform of Internet governance and established ICANN (Internet Corporation for Assigned Names and Numbers): Framework for Global Electronic Commerce (1997), which states that 'the private sector should lead' the Internet governance process and that the main function of this governance will be to 'enforce a predictable, minimalist, consistent, and simple legal environment for e-commerce'. These principles are the foundation of the ICANN-based Internet governance regime.

Definition of e-commerce

The choice of a definition for e-commerce has many practical and legal implications.[1] Specific rules are applied depending on whether a particular transaction is classified as e-commerce, such as those regulating taxation and customs.

For the US government, the key element distinguishing traditional commerce from e-commerce is 'the online commitment to sell goods or services'. This means that any commercial deal concluded online should be considered an e-commerce transaction, even if the realisation of the deal involves physical delivery. For example, purchasing a book via Amazon.com is considered an e-commerce transaction even though the book is usually delivered via traditional mail. The World Trade Organization (WTO) defines e-commerce as 'the production, distribution, marketing, sale, or delivery of goods and services by electronic means'.[2]

E-commerce takes many forms.

- **Business-to-consumer (B2C)** – the most familiar type of e-commerce (e.g. Amazon.com).
- **Business-to-business (B2B)** – economically the most intensive, comprising over 90% of all e-commerce transactions.
- **Business-to-government (B2G)** – highly important in the area of procurement policy.
- **Consumer-to-consumer (C2C)** – for example, e-Bay auctions.

Many countries have been developing a regulatory environment for e-commerce. Laws have been adopted in the fields of digital signatures, dispute resolution, cybercrime, customer protection, and taxation. At international level, an increasing number of initiatives and regimes are related to e-commerce.

WTO and e-commerce

The key policy player in modern global trade, WTO, regulates many relevant e-commerce issues, including telecommunication liberalisation, Intellectual property rights (IPR), and some aspects of information and communication technology (ICT) developments. E-commerce figures in the following WTO activities and initiatives:

- A temporary moratorium on custom duties on e-transactions which was introduced in 1998. It has rendered all e-transactions globally free of custom duties.
- The establishment of the WTO Work Programme for Electronic Commerce, which promotes discussion on e-commerce.[3]
- Dispute resolution mechanism. E-commerce was particularly relevant in the USA/Antigua online gambling case.[4]

Although e-commerce has been on the WTO diplomatic backburner, various initiatives have arisen and a number of key issues have been identified. Two such issues are mentioned here.

Should e-commerce transactions be categorised under services (regulated by GATS – General Agreement on Trade in Services) or goods (regulated by GATT – General Agreement on Tarrifs and Trade)?

Does the categorisation of music as a good or a service change depending on whether it is delivered on a CD (tangible) or via the Internet (intangible)? Ultimately, the same song could have different trade status (and be subject

to different customs and taxes) depending on the medium of delivery. The issue of categorisation has considerable implications, because of the different regulatory mechanisms for goods and services.

What should be the link between TRIPS (Trade-Related Aspects of Intellectual Property Rights) and the protection of IPR on the Internet?

Since the WTO TRIPS agreement provides much stronger enforcement mechanisms for IPR, developed countries have been trying to extend TRIPS coverage to e-commerce and to the Internet by using two approaches. First, by citing the principle of 'technological neutrality' they argue that TRIPS, like other WTO rules, should be extended to any telecommunication medium, including the Internet. Second, some developed countries requested the closer integration of WIPO's 'digital treaties' into the TRIPS system. TRIPS provides stronger enforcement mechanisms than WIPO conventions. Both issues remain open and they will become increasingly important in future WTO negotiations. During the current stage of trade negotiations, it is not very likely that e-commerce will receive prominent attention on the WTO agenda. The lack of global e-commerce arrangements will be partially compensated by some specific initiatives (regarding, for example, contracts and signatures) and various regional agreements, mainly in the EU and the Asia-Pacific region.

Other international e-commerce initiatives

One of the most successful and widely supported international initiatives in the field of e-commerce is UNCITRAL's (UN Commission on International Trade Law) Model Law on Electronic Commerce. The focus of the Model Law is on mechanisms for the integration of e-commerce with traditional commercial law (e.g. recognising the validity of electronic documents). The Model Law has been used as the basis for e-commerce regulation in many countries. Another initiative designed to develop e-commerce is the introduction of e-business XML (ebXML) by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFAT), which is a set of standards based on the XML technology. In fact, ebXML could soon become the main standard for the exchange of electronic trade documents, replacing the current one – Electronic Data Interchange (EDI).

The EU has carried out a broad set of actions in the field of e-commerce, its main focus being on small and medium enterprises.[5] The activities of the Organistion for Economic Co-operation and Development (OECD) touch on various aspects related to e-commerce, including customer protection and digital signatures. OECD activities emphasise promotion and research regarding e-commerce through its recommendations and guidelines.

UNCTAD (UN Conference on Trade and Development) is particularly active in research and capacity building, focusing on the relevance of e-commerce to development. Every year it publishes the *E-Commerce and Development Report*, which contains both a survey of the current situation and proposals for future developments.

In the business sector, the most active international organisations are the International Chamber of Commerce (ICC), which produces a wide range of recommendations and analyses in the field of e-commerce, and the Global Business Dialogue, which promotes e-commerce in both international and national contexts.

Regional initiatives

The EU developed an e-commerce strategy at the so-called 'Dot Com Summit' of EU leaders in Lisbon (March, 2000). Although it embraced a private and market-centred approach to e-commerce, the EU also introduced a few corrective measures aimed at protecting public and social interests (the promotion of universal access, a competition policy involving consideration of the public interest, and a restriction in the distribution of harmful content). The EU adopted the Directive on Electronic Commerce as well as a set of other directives related to electronic signatures, data protection, and electronic financial transactions. In the Asia-Pacific region, the focal point of e-commerce co-operation is Asia-Pacific Economic Co-operation (APEC). APEC established the E-Commerce Steering Group, which addresses various e-commerce issues, including consumer protection, data protection, spam, and cybersecurity. The most prominent initiative is APEC's Paperless Trading Individual Action Plan, aiming to create completely paperless trade in goods in the region by 2010.

See Section 5 for further discussion on universal access

See Section 2 for further discussion on spam and cybersecurity

Consumer protection

Consumer trust is one of the main preconditions for the success of e-commerce. E-commerce is still relatively new and consumers are not as confident with it as with 'real-world' shopping. Consumer protection is an important legal method for developing trust in e-commerce. E-commerce regulation should protect customers in a number of areas:

- the online handling of payment card information;
- misleading advertising; and
- the delivery of defective products.

A new idiosyncrasy of e-commerce is the internationalisation of consumer protection, which is not a vital issue in traditional commerce. In the past, consumers rarely needed international protection. Consumers were buying locally and therefore needed customer protection locally. With e-commerce, an increasing number of transactions take place across international borders.

Jurisdiction is a significant issue surrounding consumer protection. It involves two main approaches. The first favours the seller (mainly e-business) and is a country-of-origin/prescribed-by-seller approach. In this scenario, e-commerce companies have the advantage of relying on a predictable and well-known legal environment. The other approach, which favours the customer, is a country-of-destination approach.

The main disadvantage for e-commerce companies is the potential for exposure to a wide variety of legal jurisdictions. One possible solution to this dilemma is a more intensive harmonisation of consumer protection rules, making the question of jurisdiction less relevant.

See Section 3 for further discussion on jurisdiction

As with other e-commerce issues, the OECD assumed the lead by adopting the Guidelines for Consumer Protection in the Context of E-commerce (2000) and the Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003). The main principles established by the OECD have been adopted by other business associations, including ICC and the Council of Better Business Bureaus.

The EU offers a high level of e-commerce consumer protection. The problem of jurisdiction has been solved via the Brussels Convention, which stipulates that consumers will always have recourse to local legal protection. At global level, no apposite international legal instruments have been established. One of the most apt, the UN Convention on Contracts for the International Sale of Goods (1980), does not cover consumer contracts and consumer protection.

A number of private associations and non-governmental organisations (NGOs) also focus on consumer e-commerce protection, including Consumers International, the Consumer Project on Technology, the International Consumer Protection and Enforcement Network, and Consumer Web Watch.

The future development of e-commerce will require either the harmonisation of national laws or a new international regime for e-commerce customer protection.

Taxation

> *Sir, I do not know what it is good for. But of one thing I am quite certain, some day you will tax it.*
>
> **Michael Faraday's answer to sceptical politicians about the purpose of his invention of electromagnetic induction back in 1831.**[6]

With the Internet moving into the mainstream of modern society, the question of taxation has come into sharper focus. It has become even more important since the financial crisis in 2008. Many governments have been trying to increase fiscal income in order to reduce growing public debt. The taxation of economic activities on the Internet became one of the first possibilities for increasing fiscal income. One of the most frequent requests is to limit online gambling in order to stop the drain of tax income from traditional gambling centres. Other proposals include the introduction of special taxes on Internet access.

The Internet governance dilemma of whether cyber issues should be treated differently from real-life issues is clearly mirrored in the question of taxation.[7] Since the early days, the USA has been attempting to declare the Internet a tax-free zone. In 1998, the US Congress adopted the Tax Freedom Act, which was again extended for another three years in December 2004. In October 2007, the Act was extended until 2014, in spite of some fears that it could lead to a substantial revenue loss.[8]

The OECD and the EU have promoted the opposite view, namely that the Internet should not have special taxation treatment. The OECD's Ottawa Principles specify that no difference exists between traditional and e-taxation that would require special regulations. By applying this principle, in 2003, the EU introduced a regulation requesting non-EU e-commerce companies to pay value added tax (VAT) if they sold goods within the European Union. The main motivation for the EU's decision was that non-EU (mainly US) companies had an edge over European companies, which had to pay VAT on all transactions, including electronic ones.

Another e-taxation issue that remains unresolved between the EU and the USA is the question of the location of taxation. The Ottawa Principles introduced a 'destination' instead of 'origin' principle of taxation. The US government has a strong interest in having taxation remain at the origin of transactions, since most e-commerce companies are based in the USA. In contrast, the EU's interest in destination taxation is largely inspired by the actuality that the EU has more e-commerce consumers than sellers.

Digital signatures

Broadly speaking, digital signatures are linked to the authentication of individuals on the Internet, which affects many aspects of the Internet, including jurisdiction, cybercrime, and e-commerce. The use of digital signatures should contribute to building trust on the Internet. Digital authentication in general is part of the e-commerce framework. It should facilitate e-commerce transactions through the conclusion of e-contracts. For example, is an agreement valid and binding if it is completed via e-mail or through a website? In many countries, the law requires that contracts must be 'in writing' or 'signed'. What does this mean in terms of the Internet? Faced with these dilemmas and pressured to establish an e-commerce enabling environment, many governments have started adopting legislation on digital signatures.

When it comes to digital signatures, the main challenge is that governments are not regulating an existing problem, such as cybercrime or copyright infringement, but creating a new regulatory environment in which they have no practical experience. This has resulted in a variety of solutions and a general vagueness in the provisions on digital signatures. Three major approaches to the regulation of digital signatures have emerged.[9]

The first is a 'minimalist' approach, specifying that electronic signatures cannot be denied because they are in electronic form. This approach specifies a very broad use of digital signatures and has been adopted in common law countries: the United States, Canada, Australia, and New Zealand

The second approach is 'maximalist', specifying a framework and procedures for digital signatures, including cryptography and the use of public key identifiers. This approach usually specifies the establishment of dedicated certificate authorities, which can certify future users of digital signatures. This approach has prevailed in the laws of European countries, such as Germany and Italy.

The third approach, adopted within the EU Digital Signatures Directive, combines these two approaches.[10] It has a minimalist provision for the recognition of signatures supplied via an electronic medium. The maximalist approach is also recognised through granting that 'advanced electronic signatures' will have stronger legal effect in the legal system (e.g. easier to prove these signatures in court cases).

At global level, in 2001, UNCITRAL adopted the Model Law on Electronic Signatures, which grants the same status to digital signatures as to handwritten ones, providing some technical requirements are met. ICC issued a General Usage in International Digitally Ensured Commerce (GUIDEC), which provides a survey of the best practices, regulations, and certification issues.[11] Directly related to digital signatures are public key infrastructure (PKI) initiatives. Two organisations, ITU (International Telecommunication Union) and IETF (Internet Engineering Task Force), are involved with PKI standardisation.

The issues

Privacy and digital signatures

Digital signatures are part of a broader consideration of the relationship between privacy and authentication on the Internet. They are just one important technique (but not the only one) for the identification of individuals on the Internet.[12] For instance, SMS authentication via mobile phones is used by banks for approving customers' online transactions in some countries where the digital signature legislation or standards and procedures have not yet been set up.

The need for detailed implementation standards

Although many developed countries have adopted broad digital signature legislation, it often lacks detailed implementation standards and procedures. Given the novelty of the issues involved, many countries are waiting to see in which direction concrete standards will develop. Standardisation initiatives occur at various levels, including international organisations (ITU) and professional associations (IETF).

The risk of incompatibility

The variety of approaches and standards in the field of digital signatures could lead towards incompatibility between different national systems. Patchwork solutions could restrict the development of e-commerce at global level. Necessary harmonisation should be provided through regional and global organisations.

E-payments: e-banking and e-money

The common element in various definitions of electronic (e-) is that financial transactions occur in online environments through the use of online payment systems. The existence of an electronic payment system is a precondition for the successful development of e-commerce. The field of electronic payments requires differentiation between e-banking and e-money.

E-banking involves the use of the Internet to conduct conventional banking operations, such as card payments or fund transfers. The novelty is only in the medium; the banking service remains essentially the same. E-banking provides advantages to customers by introducing new services and reducing the costs of transactions. For example, customer transactions, which cost US$1 in traditional banking, cost only US$0.02 in Internet banking.[13] In terms of governance, e-banking poses new challenges when it comes to the licensing of banks by financial authorities. How should virtual banks be licensed? Another governance issue is customer protection at international level.

E-money, on the other hand, introduces considerable innovation. The US Federal Reserve Board defines e-money as 'money that moves electronically'. E-money is usually associated with so-called 'smart cards' issued by companies such as Mondex, Visa Cash, and CyberCash. All e-money has the following characteristics:

- It is stored electronically, typically on a card with magnetic record or a microprocessor chip.
- It is transferred electronically. In most cases, this occurs between consumers and merchants. Sometimes it is possible to conduct transfers between individuals.
- Transactions involve a complex system, including the issuer of the e-money value, the network operators, and the clearer of transactions.

So far, e-money is still in the early stages of development. It has not been widely used, because of limited security and lack of privacy. It might develop in two directions.

The first is an evolutionary development, which would include more sophisticated methods for electronic-based transactions, including the development of efficient micropayments. Ultimately, all of those transactions would be anchored in the existing banking and monetary system.

The second is a revolutionary development, which would move e-money out of the control of central banks. Already, the Bank for International Settlements has identified a diminished control over capital flow and money supply as risks associated with e-money. Conceptually, issuing e-money would be akin to printing money without the control of a central banking institution. Such an approach would enable private institutions to issue money primarily for e-commerce. The recent introduction of Facebook virtual raised concerns that due to the volume of its online activities, it may in the future *de facto* take some monetary function.[14] In the context of the recent financial crisis and attempts by governments to regain control of the financial system, it is not very likely that experiments with e-money will be encouraged.

The issues

Changes to the worldwide banking system

The further use of both e-banking and e-money could bring about changes to the worldwide banking system, providing customers with additional possibilities while simultaneously reducing banking charges. Bricks-and-mortar banking methods will be seriously challenged by more cost-effective e-banking.[15] It should be noted that many traditional banks have already adopted e-banking. In 2002, there were only 30 virtual banks in the United States. Today it is difficult to find a bank without e-banking services.

Cybersecurity

Cybersecurity is one of the main challenges to the wider deployment of e-payments. How can the safety of financial transactions via the Internet be ensured? On this point, it is important to stress the responsibility of banks and other financial institutions for the security of online transactions. The main development in this respect was the Sarbanes-Oxley Act, adopted by the US Congress as a reaction to the Enron, Arthur Andersen, and WorldCom financial scandals. This Act tightens financial control and increases the responsibility of financial institutions for the security of online transactions. It also shares the burden of security responsibility between customers, who have to demonstrate certain prudence, and financial institutions.[16]

Lack of payment methods

Surveys of e-commerce list the lack of payment methods (e.g. cards) as the third reason, after security and privacy, for not using e-commerce. Currently, e-commerce is conducted primarily by credit card. This is a significant obstacle for developing countries that do not have a developed credit card market.

The governments in those countries would have to enact the necessary legal changes in order to enable the faster introduction of card payments.

Digital cash

In order to foster the development of e-commerce, governments worldwide would need to encourage all forms of cash-free payments, including credit cards and e-money. The faster introduction of e-money will require additional governmental regulatory activities. After Hong Kong, the first to introduce comprehensive e-money legislation, the EU adopted the Electronic Money Directive in 2000.[17] Governments are reluctant to introduce e-money due to the potential risks to the authority of the central banks. Serious warnings are provided by views such as that expressed by the economist David Saxton: 'Digital cash is a threat to every government on this planet that wants to manage its own currency.'[18] Governments are also concerned about the potential use of e-money for money laundering.

Small transactions

Some analysts believe that the real expansion of e-commerce is linked to the introduction of effective and reliable services for small transactions. For example, Internet users are still reluctant to use credit cards for small payments (of a few euro/dollars), which are usually charged for accessing articles or other services on the Internet. A micro-payment scheme based on e-money may provide the necessary solution. It is interesting to note that W3C (World Wide Web Consortium), the main Web standardisation body, has ceased its e-commerce/micropayment activities, which was a set-back to the global efforts towards standardisation in this field.[19]

Addressing the issue at international level

Due to the nature of the Internet, it is likely that e-money will become a global phenomenon – providing a reason to address this issue at international level. One potential player in the field of e-banking is the Basel Committee E-Banking Group. This group has already started addressing authorisation, prudential standards, transparency, privacy, money laundering, and cross-border supervision, all key issues for the introduction of e-money.[20]

The law enforcement link

The recent request from the New York State Attorney General to PayPal and Citibank not to execute payments to Internet casinos directly links electronic payment to law enforcement.[21] What the law enforcement authorities could not achieve through legal mechanisms, they could accomplish through the control of electronic payments.

Endnotes

[1] The legal relevance of establishing a clear definition is openly explained in the EU's interactive page on e-commerce: *Normally, we avoid defining electronic commerce, aside from the vague non-definition of e-commerce being about doing business electronically. However there is a need for a legal definition for legal papers.* Source: **http://ec.europa.eu/archives/ISPO/ecommerce/drecommerce/answers/000025.html**

[2] WTO (1998) Work programme on electronic commerce. Available at: **http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm**

[3] This section of the WTO website focuses on e-commerce: **http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm**

[4] For more information about the USA/Antigua online gambling case, see: **http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm**

[5] For more information about EU's e-commerce initiatives, see: **http://ec.europa.eu/information_society/eeurope/2002/action_plan/ecommerce/index_en.htm**

[6] Maastricht Economic Research Institute on Innovation and Technology (MERIT). Available at: **http://www.merit.unimaas.nl/cybertax/**

[7] For a discussion on various aspects of taxation policy and the Internet, see:

- Cockfield AJ (2001) Transforming the Internet into a taxable forum: A case study in e-commerce taxation, *Minnesota Law Review* **85:**1171–1236. Available at: **http://post.queensu.ca/~ac24/MinnLRevArticle.pdf**
- Morse EA (1997) State taxation of Internet commerce: Something new under the sun? *Creighton Law Review.* **30**: 1124–1127.
- Williams WR (2001) The role of Caesar in the next millennium? Taxation of e-commerce: An overview and analysis, *Wm. Mitchell Law Review* **27:** 1703–1707.

[8] Mazerov M (2007) *Making the 'Internet Tax Freedom Act' permanent could lead to a substantial revenue loss for states and localities.* Available at: **http://www.cbpp.org/7-11-07sfp.htm**

[9] For a more detailed explanation of these three approaches, see the *Survey of Electronic and Digital Signature Initiatives* provided by the Internet Law & Policy Forum. Available at: **http://www.ilpf.org/groups/survey.htm#IB**

[10] Directive 1999/93/EC by the European Parliament and Council on 13 December 1999 on a Community Framework for Electronic Signatures. Available at: **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML**

[11] GUIDEC (General Usage for International Digitally Ensured Commerce) by the International Chamber of Commerce. Available at: **http://cryptome.org/jya/guidec2.htm**

[12] Longmuir G (2000) *Privacy and digital authentication*. Available at: **http://caligula.anu.edu.au/~gavin/ResearchPaper.htm.** This paper focuses on the personal, communal, and governmental aspects of the need for authentication in a digital world.

[13] Nsouli SM, Schaechter A (2002) Challenges of the e-banking revolution. *Finance and Development* **39(3).** Available at: **http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm**

[14] For legal aspects of the introduction of Facebook virtual money, see: Claburn T (2010) Virtual money presents some legal problems, *InformationWeek.* Available at: **http://www.informationweek.com/news/security/app-security/showArticle.jhtml?articleID=223101009**

[15] Bankrate.com (2002) *What is online banking?* Available at: **http://www.bankrate.com/brm/olbstep2.asp.** This article provides an introduction to online banking and a survey of the advantages and disadvantages in comparison to traditional banking**.**

[16] For more information, see: Jacobs E (ND) *Security as a legal obligation: About EU legislation related to security and Sarbanes-Oxley in the European Union*. Available at: **http://www.arraydev.com/commerce/JIBC/2005-08/security.htm**

[17] Directive 2000/46/EC of the European Parliament and Council of 18 September 2000 on the taking up, pursuit of, and prudential supervision of the business of electronic money institutions. Available at: **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML**

[18] Holland K, Cortese A (1995) *The future of money: e-cash could transform the world's financial life*. Available at: **http://www.businessweek.com/1995/24/b3428001.htm**

[19] For arguments against micro-payments, see: Shirky C (2000) *The case against micropayments.* Available at: **http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html**

[20] The Basel Group is based at the Bank for International Settlements. It provides a regular *Survey of Developments in Electronic Money and Internet and Mobile Payments*. Available at: **http://www.bis.org/publ/cpss62.pdf**

[21] For more information, see**:** **http://www.ag.ny.gov/media_center/2002/aug/aug21a_02.html**

Section 5

The development basket

The development basket

Technology is never neutral. The history of human society provides many examples of technology empowering some individuals, groups, or nations, while excluding others. The Internet is no different in this respect. From the individual to global level, a profound change has occurred in the distribution of wealth and power. The impact of ICT/Internet on the distribution of power and development has given rise to many questions:

- How will ICT/Internet-accelerated changes affect the already existing divide between North and South? Will ICT/Internet reduce or broaden the existing divide?
- How and when will developing nations be able to reach the ICT levels of more industrially developed countries?

The answer to these and other questions requires an analysis of the relevance of development within the context of Internet governance.

Almost every Internet governance issue has a developmental aspect.

- The existence of a telecommunication infrastructure facilitates access, the first precondition for overcoming the digital divide.
- The current economic model for Internet access places a disproportionate burden on those developing countries that have to finance access to backbones based in developed countries.
- Spam has a comparatively higher negative impact on developing countries due to their limited bandwidth and lack of capability to deal with it.

See Section 2 for further discussion on infrastructure

See Section 4 for further discussion on economic aspects

- The global regulation of intellectual property rights (IPR) directly affects development because of the reduced opportunity of developing countries to access knowledge and information online.

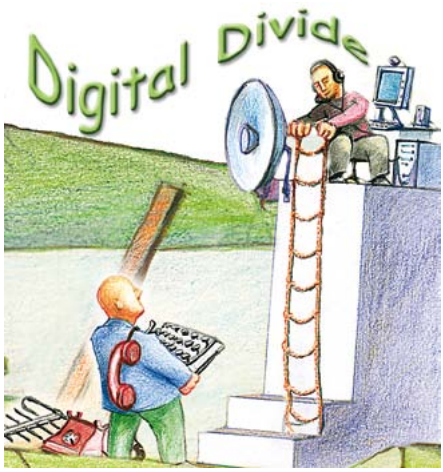
The developmental aspect of the World Summit on the Information Society (WSIS) has been frequently repeated, beginning with the UN General Assembly Resolution on WSIS, which stressed that WSIS should be 'promoting development, in particular with respect to access to and transfer of technology'. The WSIS Geneva Declaration and Plan of Action highlighted development as a priority and linked it to the Millennium Resolution and its promotion of 'access of all countries to information, knowledge, and communication technologies for development'. With the link to the millennium goals, WSIS is strongly positioned in the development context.

How does ICT affect the development of society?

The main dilemmas about ICT and development are summarised in an article in *The Economist*.[1] The article proposes arguments for and against the thesis that ICT provides specific impetus for development.

ICT does NOT facilitate development	ICT facilitates development
• The 'network externalities' help firstcomers establish a dominant position. This favours American giants so that local firms in emerging economies would be effectively frozen out of e-commerce. • The shift in power from seller to buyer (the Internet inevitably gives rise to 'an alternative supplier is never more than a mouse-click away' scenario) will harm poorer countries. It will harm commodity producers mainly from developing countries. • Higher interest in high-tech shares in rich economies will reduce investor interest in developing countries.	• ICT lowers labour costs; it is cheaper to invest in developing countries. • Very fast diffusion of ICT across borders occurs, compared to earlier technologies. Previous technologies (railways and electricity) took decades to spread to developing countries, but ICT is advancing in leaps and bounds. • The opportunity to leapfrog old technologies by skipping intermediate stages, such as copper wires and analogue telephones, encourages development. • ICT's propensity to reduce the optimal size of a firm in most industries is much closer to the needs of developing countries.

The digital divide



The digital divide can be defined as a rift between those who, for technical, political, social, or economic reasons, have access and capabilities to use ICT/Internet, and those who do not. Various views have been put forward about the size and relevance of the digital divide.

Digital divide(s) exist at different levels: within countries and between countries; between rural and urban populations; between the old and the young; as well as between men and women. Digital divides are not independent phenomena. They reflect existing broad socio-economic inequalities in education, health care, capital, shelter, employment, clean water, and food. This was clearly stated by the G8 DOT Force (Digital Opportunity Task Force):

> *There is no dichotomy between the digital divide and the broader social and economic divides which the development process should address; the digital divide needs to be understood and addressed in the context of these broader divides.*[2]

Is the digital divide increasing?

ICT/Internet developments leave the developing world behind at a much faster rate than advances in other fields (e.g. agricultural or medical techniques) and, as the developed world has the necessary tools to successfully use these technological advances, the digital divide appears to be continuously and rapidly widening. This is frequently the view expressed in various highly regarded documents, such as the United Nations Development Programme (UNDP) *Human Development Report* and the International Labour Organization (ILO) *World Employment Report*.

Some opposing views argue that statistics on the digital divide are often misleading and that it is in fact not widening at all. According to this view, the traditional focus on the number of computers, the number of Internet websites, or available bandwidth should be replaced with a focus on the broader impact of ICT/Internet on societies in developing countries. Frequently quoted examples are the digital successes of Brazil, China, and India.

Universal access

In addition to the digital divide, another frequently mentioned concept in the development debate is universal access, i.e. access for all. Although it should be the cornerstone of any ICT development policy, differing perceptions and conceptions of the nature and scope of this universal access policy remain. Frequent referral to universal access in the preambles of international declarations and resolutions without the necessary political and financial support renders it a vague principle of little practical relevance. The question of universal access at global level remains largely a policy issue, ultimately dependent on the readiness of developed countries to invest in the realisation of this goal.

Unlike at global level, in some countries universal access is a well-developed economic and legal concept. Providing telecommunication access to all citizens has been the basis of US telecommunication policy. The result has been a well-developed system of various policy and financial mechanisms, the purpose of which is to subsidise access costs in remote areas and regions with high connection costs. The subsidy is financed by regions with low connection costs, primarily the big cities. The EU has also taken a number of concrete steps towards achieving universal access.

Strategies for overcoming the digital divide

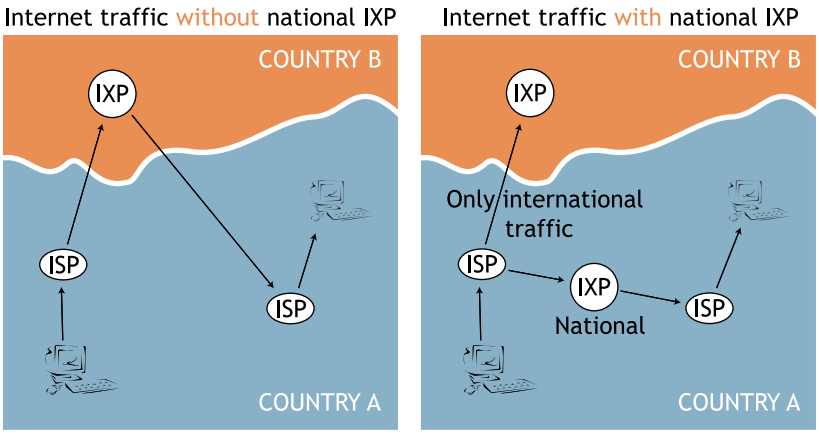
The technologically centred development theory, which has dominated policy and academic circles over the past 50 years, argues that development depends on the availability of technology. The more technology, the more development. However, this approach failed in many countries (mainly former socialist countries) where it became obvious that the development of society is a much more complex process. Technology is a necessary but not a self-sufficient precondition for development. Other elements include a regulatory framework, financial support, available human resources, and other sociocultural conditions. Even if all of these ingredients are present, the key challenge remains: how and when should they be used, combined, and interplayed.

Access: Developing telecommunications and Internet infrastructures

Access to the Internet is one of the main challenges to overcoming the digital divide. The Internet penetration rate in Africa is 5.6%, compared to 73.8%

in Japan or 60.7% in Europe.[3] There are two main aspects to access to the Internet in developing countries. First is access to international Internet backbones. Second is the connectivity within developing countries.

Access to international Internet backbones depends mainly on the availability of submarine fibre-optic cables. For long time, only Western Africa, up to South Africa, was serviced by submarine cable SAT-3. Then East Africa got access to submarine cables as well: East African Submarine System (EASSY) started operating in July 2010.[4] A few additional submarine cables should be commissioned over the next few years. It will create a strong digital ring around Africa which should substantially increase the available Internet bandwidth for the whole African continent.[5]



Second is the introduction of Internet eXchange points (IXPs) which keep local traffic within the country and reduce both usage and cost of international bandwidth.[6] Still, many developing countries do not have IXPs, which means a considerable part of traffic between the clients within the country is routed through another country. This increases the volume of long-distance international data traffic and the cost of providing Internet service. Various initiatives seek to establish IXPs in developing countries. One that has achieved some level of success is that of the Africa Internet Service Provider Association. This association has been responsible for the establishment of several IXPs in Africa.[7]

Connectivity within developing countries is another major challenge. The majority of Internet users were concentrated in major cities. Rural areas were usually without any access to the Internet. The situation started changing with

the rapid growth of mobile telephony and wireless communication. Patrick Gelsinger from Intel has advised developing countries to say 'no' to a copper-based telecommunications infrastructure and to use wireless as the solution for local-loops and fibre-optics for national backbones instead. Wireless communication might be the solution to the problem of developing a traditional terrestrial communications infrastructure (laying cables over very long distances throughout many Asian and African countries). In this way, the problem of the last-mile or local loop, one of the key obstacles to faster Internet development, can be overcome.

See Section 2 for further discussion on infrastructure

Financial support

Developing countries receive financial support through various channels, including bilateral or multilateral development agencies, such as the UNDP or the World Bank, as well as regional development initiatives and banks. With increased liberalisation of the telecommunication market, a tendency for developing telecommunication infrastructures through foreign direct investment has grown. Since telecommunication markets of developing countries are oversaturated, many international telecommunication companies see the markets of developing countries as the area for the future growth.

During the WSIS process, the importance of financial support for bridging the digital divide was clearly recognised. One idea proposed at WSIS was the establishment of a UN-administered Digital Solidarity Fund to help technologically disadvantaged countries build telecommunication infrastructures. However, the proposal did not garner broad support from the developed countries, which favoured direct investment instead of the establishment of a centralised development fund. After WSIS, the Digital Solidarity Fund was established in Geneva as an independent foundation mainly supported by cities and local authorities worldwide.

Sociocultural aspects

The sociocultural aspects of digital divides encompass a variety of issues, including literacy, ICT skills, training, education, and language protection.

See Section 6 for further discussion on sociocultural aspects

For developing countries, one of the main issues has been the 'brain drain', described as the movement of highly skilled labour from developing to developed countries. Through the brain drain, developing countries lose out in

a number of ways. The main loss is in skilled labour. Developing countries also lose their investment in the training and education of migrating skilled labour. It is likely that the brain drain will continue, given the various employment/emigration schemes that have been introduced in the USA, Germany, and other developed countries in order to attract skilled, mainly ICT-trained, labour.

One development that may stop or, in some cases, even reverse the brain drain, is the increase in the outsourcing of ICT tasks to developing countries. The most successful examples have been the development of India's software industry centres, such as Bangalore and Hyderabad.

At global level, the UN initiated the Digital Diaspora Network to promote development in Africa, through the mobilisation of the technological, entrepreneurial, and professional expertise and resources of the African diaspora in the field of ICT.

Telecommunication policy and regulation

Telecommunication policy issues are in many respects closely linked with overcoming the digital divide.

- Both private investors and, increasingly, public donors are not ready to invest in countries without a proper institutional and legal environment for Internet development.
- The development of national ICT sectors depends on the creation of necessary regulatory frameworks.
- The telecommunication policy should facilitate the establishment of efficient telecommunication market with more competition, lower costs, and a wider range of services provided.

See Section 3 for further discussion on the law

The creation of an enabling environment is a demanding task, entailing the gradual de-monopolisation of the telecommunication market, the introduction of Internet-related laws (covering cybercrime, copyright, privacy, e-commerce, etc.), and the granting of access to all citizens without restriction.

Institutionally speaking, one of the first steps is to establish independent and professional telecommunication regulatory authorities. Experience from developed countries shows that solid regulators are a precondition for fast growth in telecommunication infrastructure. In developing countries, the development of regulatory authorities is at a very early stage. Regulatory

authorities are generally weak, lack independence, and are often part of a system in which state operators are influential in regulatory and political processes.

Another major challenge has been the liberalisaton of the telecommunication market. India and Brazil are usually mentioned as developing countries where such liberalisation facilitated fast growth of the Internet and ICT sector. It also benefited overall economic growth in these countries. Other countries, in particular least developed ones, found liberalisation of the telecommunication market to be a major challenge. With the loss of telecommunication monopolies, governments in those countries lost an important source of budgetary income. The lower budgets affected all the other sectors of social and economic life. In some cases, while they lost telecommunication revenues, these countries did not harvest the benefits of liberalisation in the guise of lower costs and better telecommunication services. In many cases this was because the privatisation of telecommunication companies was not supplemented by the establishment of an effective market and competition. Such practices led the World Bank to emphasise that countries open major market segments to competition prior to, or at the same time as, privatising government-owned operators; in this way, they will reduce costs faster than those countries that privatise first and introduce competition later.[8]

Endnotes

1 Falling through the Net? *The Economist*, 21 September 2000.

2 DOT Force (2001) *Digital opportunities for all: Meeting the challenge*. Report of the Digital Opportunity Task Force (DOT Force) including a proposal for a Genoa Plan of Action. Available at: **http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html**

3 *Internet World Stats*. Available at: **http://www.internetworldstats.com/stats.htm**

4 **http://www.eassy.org/**

5 A map of submarine cables around Africa is available at: **http://manypossibilities.net/african-undersea-cables/**

6 Internet exchange points (IXPs) are technical facilities through which Internet service providers exchange Internet traffic through peering (without paying). IXPs are usually established in order to keep Internet traffic within smaller communities (e.g. city, region, country), avoiding unnecessary routing over remote geographical locations.

7 MTN (2008) *We are MTN*. Available at: **http://www.mtn.co.za/?pid=8049**

8 Ismail S (2006) *Analyzing the World Bank's blueprint for promoting 'information and communications. Federal Communications Law Journal* **59(1)**. Available at: **http://www.law.indiana.edu/fclj/pubs/v59/no1/13-Book%20ReviewFINAL.pdf**

Section 6

The sociocultural basket

The sociocultural basket

The Internet has made a considerable impact on the social and cultural fabric of modern society. It is difficult to identify any segment of social life that is not affected by the Internet. It introduces new patterns of communication, breaks down language barriers, and creates new forms of creative expression. Today, the Internet is increasingly becoming more of a social, as opposed to a technological, phenomenon.

Human rights

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 hotly debated both in the World Summit on the Information Society (WSIS) and the Internet Governance Forum (IGF) processes. While human rights are usually explicitly addressed, they are also involved in cross-cutting issues appearing when dealing with network neutrality (right to access, freedom of expression, anonymity), cybersecurity (observing human rights while carrying out cybersecurity and protection activities), content control, etc. WSIS recognised the importance of human rights, in particular the right to development and the right to freedom of expression.

See Section 2 for further discussion on network neutrality and cybersecurity

Real rights vs cyber rights

Parallel to the conceptual legal debate which discusses whether current law is sufficient to regulate the Internet or if there is a need for new cyber law, there has been discussion in human rights circles about whether traditional human

rights concepts need to be revised in view of their use on the Internet. The Association for Progressive Communication (APC) in the Internet Rights Charter argues that the Internet-related human rights are strongly embodied in the UN human rights system based on the Universal Declaration on Human Rights (UDHR) and other related instruments.[1]

There is also a proposal for establishing the right to communicate as a new type of human right mainly inspired by the new forms of Internet-based communication.

Survey of initiatives on human rights and the Internet

The main cyber rights initiative taking place currently is the Internet Bill of Rights (IBR), sponsored by the Italian government and civil society. This project triggered the process which is currently supported by the Internet Rights and Principles Dynamic Coalition[2] and includes other developments, such as Internet Rights Watch. IBR has been discussed at all previous IGFs. In an attempt to delineate cyber rights, APC drafted an Internet Rights Charter.[3] Another predominantly academic initiative is the Networked Communications Freedom Charter proposed by the Faculty of Law at the University of Toronto.

Right to access the Internet

Finland is one of the first countries to legally guarantee the right to access the Internet. As of July 2010 all citizens in Finland will have the right to a one-megabit (1MB) broadband connection.

Google, Microsoft, and a few other Internet companies started the Global Network Initiative in November 2008 with the main aim of promoting human rights, in particular freedom of expression and privacy. This initiative is particularly important because the commercial activities of major Internet companies can directly affect the way human rights are protected.[4]

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 Council of Europe. The Council is the core institution dealing with pan-European human rights, with the European Convention for the Protection of Human Rights and Fundamental Freedom (195)[5] as its main instrument. Since 2003, the Council of Europe has adopted several declarations highlighting the importance of human rights on the Internet.[6] The Council

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

See Section 3 for further discussion on cybercrime

Freedom of expression and the right to seek, receive, and impart information

One of the most contentious areas of human rights on the Internet involves freedom of expression. This is one of the fundamental human rights, usually appearing in the focus of discussions on content control and censorship. In the UDHR, freedom of expression (Article 19) is counter-balanced by the right of the state to limit freedom of expression for the sake of morality, public order, and general welfare (Article 29). Thus, both the discussion and implementation of Article 19 must be put in the context of establishing a proper balance between two needs. This ambiguous situation opens many possibilities for different interpretations of norms and ultimately different implementations. The controversy around the right balance between Articles 19 and 29 in the 'real' world is mirrored in discussions about achieving this balance on the Internet.

Freedom of expression is the particular focus of human rights non-governmental organisations (NGOs) such as Amnesty International and Freedom House. A recent study by Freedom House evaluates the level of Internet and mobile phone freedom experienced by average users in a sample of 15 countries across 6 regions. Covering the calendar years 2007 and 2008, the study addresses a range of factors that might affect such freedom, including the state of the telecommunication infrastructure, government restrictions on access to technology, the regulatory framework for service providers, censorship and content control, the legal environment, surveillance, and extralegal attacks on users or content producers. The selected indicators capture not only the actions of governments but also the vigour, diversity, and activism of the new media domain in each country, regardless of – or despite of – state efforts to restrict usage.[7]

Content policy

One of the main sociocultural issues is content policy, often addressed from the standpoints of human rights (freedom of expression and right to communicate), government (content control), and technology (tools for content control). Discussions usually focus on three groups of content.

1. Content that has a global consensus for its control. Included here are child pornography, justification of genocide, and incitement or organisation of terrorist acts, all prohibited by international law *(ius cogens)*.[8]
2. Content that is sensitive for particular countries, regions, or ethnic groups due to their particular religious and cultural values. Globalised online communication poses challenges for local, cultural, and religious values in many societies. Most content control in Middle Eastern and Asian countries is officially justified by the protection of specific cultural values. This often means that access to pornographic and gambling websites is blocked.[9]
3. Political censorship on the Internet. In 2007, Reporters without Borders reported that 12 countries perform political censorship on the Internet.[10]

How content policy is conducted

An *à la carte* menu for content policy contains the following legal and technical options, which are used in different combinations.

Governmental filtering of content

The common element for governmental filtering is an Internet Index of websites blocked for citizen access.[11] If a website is included in the Internet Index, access will not be granted. Technically speaking, filtering utilises mainly router-based Internet Protocol (IP) blocking, proxy servers, and Domain Name System (DNS) redirection.[12] In addition to the countries usually associated with these practices, such as China, Saudi Arabia, and Singapore, other countries increasingly adopt the practice. For example, Australia has a filtering system for specific national pages, although not international ones.[13]

Private rating and filtering systems

Faced with the potential risk of the disintegration of the Internet through the development of various national barriers (filtering systems), W3C (World Wide Web Consortium) and other like-minded institutions made proactive moves proposing the implementation of user-controlled rating and filtering systems.[14] In these systems, filtering mechanisms are built into Internet browsers. A label indicates the accessibility of particular content on a particular website. The use of this type of filtering is especially favoured in accessing child-friendly websites.

Content filtering based on geographical location

Another technical solution related to content is geo-location software, which filters access to particular web content according to the geographic or national origin of users. The Yahoo! case was important in this respect, since the group of experts involved, including Vint Cerf, indicated that in 70–90% of cases Yahoo! could determine whether sections of one of its websites hosting Nazi memorabilia were accessed from France.[15] This assessment helped the court come to a final decision, which requested Yahoo! to filter access from France to Nazi memorabilia. Geo-location software companies claim that they can identify the home country without mistake and the city in about 85% of cases, especially if it is a large city.[16]

See Section 3 for further discussion on jurisdiction

Content control through search engines

The bridge between the end-user and web content is usually a search engine. It has been reported that the Chinese authorities initiated one of the first examples of content control via search engines. If users entered prohibited words into Google Search, they lost their IP connectivity for a few minutes.[17] The response of the Chinese information department:

> *...it is quite normal with some Internet sites that sometimes you can access them and sometimes you can't. The ministry has received no information about Google being blocked.*[18]

The filtering of searches was one of the reasons behind the recent tension between Google and Chinese authorities.[19]

To adjust to local laws, Google decided to restrict some materials on its national websites. For example, on German and French versions of Google it is not possible to search for and find websites with Nazi materials. This involves a certain level of self-censorship to avoid possible court cases.[20]

Web 2.0 challenge: users as contributors

With the development of Web 2.0 platforms – blogs, forums, document-sharing websites, and virtual worlds – the difference between the user and the creator has blurred. Internet users can create large portions of web content, such as blog posts, YouTube videos, and photo galleries.

Identifying, filtering, and labelling 'improper' websites is becoming increasingly difficult. While automatic filtering techniques already exist, automatic recognition, filtering, and labelling of visual content does not occur.

One approach, used on a few occasions by Morocco, Pakistan, Turkey, and Tunisia, is to block access to YouTube throughout the country. This maximalist approach, however, results in unobjectionable content, including educational material, being blocked.

The need for an appropriate legal framework

The legal vacuum in the field of content policy provides governments with high levels of discretion in deciding which content should be blocked. Since content policy is a sensitive issue for every society, the adoption of legal instruments is vital. National regulation in the field of content policy may provide better protection for human rights and resolve the sometimes ambiguous roles of Internet service providers (ISPs), enforcement agencies and other players. In recent years, many countries have introduced content policy legislation.

International initiatives

At international level, the main initiatives arise in European countries with strong legislation in the field of hate speech, including anti-racism and anti-Semitism. European regional institutions have attempted to impose these rules on cyberspace. The primary legal instrument addressing the issue of content is the Council of Europe Additional Protocol to the Convention on Cybercrime.

The EU has initiated content control, adopting the European Commission Recommendation against Racism via the Internet. On a more practical level, the EU introduced the EU Safer Internet Action Plan, which includes the following main points:

- Setting up a European network of hotlines for the reporting of illegal content.
- Encouraging self-regulation.
- Developing content rating, filtering, and benchmark filtering.
- Developing software and services.
- Raising awareness of the safer use of the Internet.[21]

The Organisation of Security and Cooperation in Europe is also active in this field. Since 2003, it has organised a number of conferences and meetings with a particular focus on freedom of expression and the potential misuses of the Internet (e.g. racist, xenophobic, and anti-Semitic propaganda).

The issues

Content control vs freedom of expression

When it comes to content control, the other side of the coin is very often restriction of freedom of expression. This is especially important in the USA, where the First Amendment guarantees broad freedom of expression, even the right to publish Nazi-related and similar materials.

Freedom of expression largely shapes the US position in the international debate on content-related issues on the Internet. For example, while the USA has signed the Convention on Cybercrime, it cannot sign the Additional Protocol to this Convention, dealing with hate speech and content control. The question of freedom of expression was also brought up in the context of the Yahoo! court case. In its international initiatives, the USA will not step beyond the line which may compromise freedom of expression as is stipulated in the First Amendment.

Illegal offline – illegal online

This brings the discussion about content to the dilemma between the real world and the cyber world. Existing rules about content can be implemented on the Internet. This is frequently highlighted within the European context. The EU Council Framework Decision on Combating Racism and Xenophobia explicitly indicates 'what is illegal offline is illegal online'. One of the arguments of the cyber approach to Internet regulation is that quantity (intensity of communication, number of messages) makes a qualitative difference. In this view, the problem of hate speech is not that no regulation against it has been enacted, but that the sharing and spreading through the Internet makes it a different kind of legal problem. More individuals are exposed and it is difficult to enforce existing rules. Therefore, the difference that the Internet brings is mainly related to problems of enforcement, not to the rules themselves.

The effectiveness of content control

In discussions on Internet policy, a key argument is that the decentralised nature of the Internet can bypass censorship. The Internet includes many techniques and technologies that can provide effective control. Technically speaking, however, control mechanisms can be bypassed.

In countries with government-directed content control, technically gifted users have found a way around such control. Nonetheless, content control is not intended for this small group of technically gifted users; it is aimed at the broader population. According to Lessig, 'A regulation need not be absolutely effective to be sufficiently effective.'[22]

Who should be responsible for content policy?

The main players in the area of content control are governments. Governments prescribe what content should be controlled and how. ISPs, as Internet gateways, are commonly held responsible for implementation of content filtering, either according to government prescriptions or to self-regulation (at least in regard to issues of broad consensus, such as child pornography).[23] Some groups of individual users, such as parents, are keen to introduce a more efficient content policy to protect children. Various rating initiatives help parents to find child-friendly content. New versions of Internet browser software usually include many filtering options. Private companies and universities also perform content control. In some cases, content is controlled through software packages; for example, the Scientology movement has distributed a software package to members - Scienositter - which prevents access to websites critical of Scientology.[24]

Privacy and data protection[25]

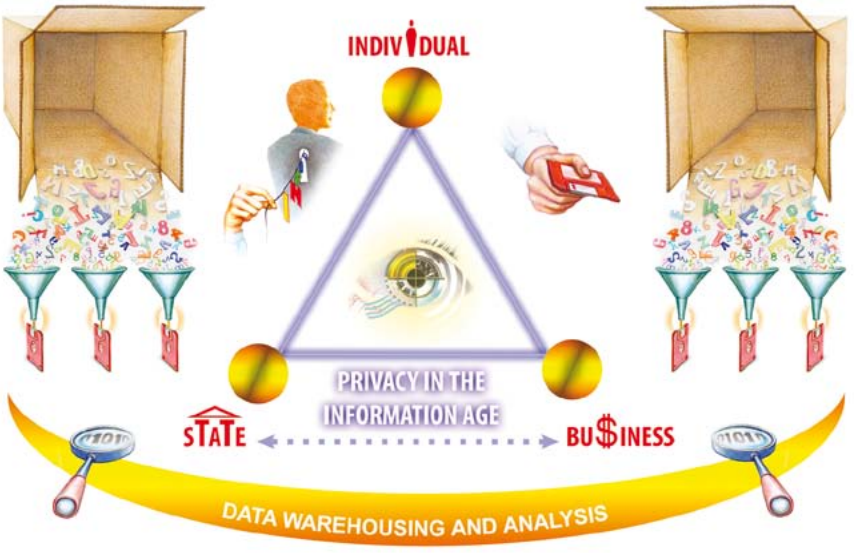
Privacy and data protection are two interrelated Internet governance issues. Data protection is a legal mechanism that ensures privacy. Yet, what is privacy? It is usually defined as the right of any citizen to control his or her own personal information and to decide about it (to keep or disclose information). Privacy is a fundamental human right. It is recognised in the UDHR, the International Covenant on Civil and Political Rights, and in many other international and regional human rights conventions.

National cultures and ways 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, as depicted in the privacy triangle illustrated on the opposite page.[26]

Privacy protection: the issues

Individuals and states

Information has always been an essential tool for states to exercise authority over their territories and populations. Governments collect vast amounts of personal information (birth and marriage records, social security numbers,



voting registration, criminal records, tax information, housing records, car ownership, etc.). It is not possible for an individual to opt out of providing personal data, short of emigrating to another country, where he or she would confront the same problem. Information technology, such as that used in data mining, aids in the aggregation and correlation of data from many specialised systems (e.g. taxation, housing records, car ownership) to conduct sophisticated analyses, searching for usual and unusual patterns and inconsistencies. One of the main challenges of e-governance initiatives is to ensure a proper balance between the modernisation of government functions and the guarantee of citizens' privacy rights.

After the events of 11 September 2001 in the USA, the US Patriot Act and comparable legislation in other countries broadened government authority to collect information, including a provision for lawful interception of information.[27] The concept of lawful interception in gathering evidence is also included in the Council of Europe's Convention on Cybercrime (Articles 20 and 21).

Individuals and businesses

In the privacy triangle depicted above, the second, and increasingly important relationship is that between individuals and the business sector. People disclose personal data when they open a bank account, book a flight or a hotel, make an online payment by credit card, browse or search the Internet. Multiple traces of data are often left in each of these activities.

In an information economy, information about customers, including their preferences and purchase profiles, becomes an important market commodity. For some companies, such as Google and Amazon, information about customers' preferences constitutes a cornerstone of their business model. The success and sustainability of e-commerce, both business-to-customer and business-to-business, depend on the establishment of extensive trust in both business privacy policies and the security measures they establish to protect clients' confidential information from theft and misuse.[28] With the expansion of social networking platforms, concerns arise over the eventual misuse of personal data – not only by the owner or administrator of a social networking platform, but also by other individuals participating in it.

States and businesses

The third side of the privacy triangle is the least publicised, yet perhaps the most significant privacy issue. Both states and businesses collect considerable amounts of data about individuals. Some of this data is exchanged with other states and businesses to impede terrorist activities. In some situations, however, such as those to which the European Directive on Data Protection applies, the state supervises and protects data about individuals held by businesses.

Individuals and individuals

The last aspect of privacy protection, not represented within the privacy triangle, is the potential risk to privacy from individuals. Today, any individual with sufficient funds may own powerful surveillance tools. Even a simple mobile phone equipped with a camera can become a surveillance tool. Technology has 'democratised surveillance' to quote *The Economist*. Many instances of the invasion of privacy have occurred, from simple voyeurism to the sophisticated use of cameras for recording card numbers in banks and for electronic espionage. The main problem for protection from this type of privacy violation is that most legislation focuses on the privacy risks stemming from the state. Faced with this new reality, a few governments have taken some initial steps. The US Congress adopted the Video Voyeurism Prevention Act, prohibiting the taking of photos of unclothed people without their approval. Germany and a few other countries have adopted similar privacy laws, preventing individual surveillance.

The international regulation of privacy and data protection

One of the main international instruments on privacy and data protection is the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. Although it was adopted by the Council of Europe, it is open for accession by other states,

including non-European states. Since the Convention is technology neutral, it has withstood the test of time. More recently, it has been examined for applicability to the collection and processing of biometric data.

The EU Data Protection Directive (Directive 45/46/EC) has also formed an important legislative framework for the processing of personal data in the European Union and has had a huge impact on the development of national legislation not only in Europe but also globally.

Another key international – non-binding – document on privacy and data protection is that of the Organisation for Economic Co-Operation and Development (OECD) Guidelines on Protection of Privacy and Transborder Flows of Personal Data, from 1980. These guidelines and the OECD's subsequent work have inspired many international, regional, and national regulations on privacy and data protection. Today, virtually all OECD countries have enacted privacy laws and empowered authorities to enforce those laws.

While the principles of the OECD guidelines have been widely accepted, the main difference is in the way they are implemented, particularly between the European and US approaches. In Europe there is comprehensive data protection legislation while in the United States the privacy regulation is developed for each sector of the economy including financial privacy (Graham-Leach-Bliley Act)[29,30] and children's privacy (Children's Online Privacy Protection Act),[31] and medical privacy (the proposed Health and Human Services regulations).[32]

Another major difference is that in Europe privacy legislation is enforced by public authorities, while in the United States enforcement principally rests on the private sector and self-regulation. Businesses set privacy policies. It is up to companies and individuals to decide about privacy policies themselves. The main criticism of the US approach is that individuals are placed in a comparatively weak position; they are seldom aware of the importance of options offered by privacy policies and commonly agree to them without informing themselves.

Safe Harbor Agreement between the USA and the EU

These two approaches – US and EU – to privacy protection have started to conflict. The main problem stems from the use of personal data by business companies. How can the EU impose its regulations on, for example, a US-based software company? How can the EU ensure that data about its citizens is protected according to the rules specified in its Directive on

Data Protection? According to whose rules (the EU's or the USA's) is data transferred through a company's network from the EU to the USA handled? The EU threatened to block the transfer of data to any country that could not ensure the same level of privacy protection as spelled out in its directive. This request inevitably led to a clash with the US self-regulatory approach to privacy protection.

This deep-seated difference made any possible agreement more difficult to achieve. Moreover, adjusting US law to the EU Directive would not have been possible since it would have required changing a few important principles of the US legal system. The breakthrough in the stalemate occurred when US Ambassador Aaron suggested a 'Safe Harbor' formula. This reframed the whole issue and provided a way out of the impasse in the negotiations.

A solution was hit upon where EU regulations could be applied to US companies inside a legal safe harbour. US companies handling EU citizens' data could voluntarily sign up to observe the EU's privacy protection requirements. Having signed, companies must observe the formal enforcement mechanisms agreed upon between the EU and the USA.

When it was signed in 2000, the Safe Harbor Agreement was received with a great hope as the legal tool that could solve similar problems with other countries. However, the record is not very encouraging. It has been criticised by the European Parliament for not sufficiently protecting the privacy of EU citizens. US companies were not particularly enthusiastic about using this approach. According to a recent study done by Galexia, out of 1597 companies registered in the Safe Harbor Framework, only 348 meet the basic requirements (e.g. privacy policy).[33] Given the high importance of privacy and data protection in the EU, it is likely to expect higher pressure to find some solution for the dysfunctional Safe Harbor Agreement.

Multilingualism and cultural diversity

Since its early days, the Internet has been a predominantly English-speaking medium. According to some statistics, approximately 80% of web content is in English, whereas 80% of the world's population does not speak English. This situation has prompted many countries to take concerted action in promoting multilingualism and in protecting cultural diversity. The promotion of multilingualism is not only a cultural issue, but is directly related to the need for the further development of the Internet.[34] If the Internet is to be used by

wider parts of society and not just national elites, content must be accessible in more languages.

The issues

Non-Roman alphabets

The promotion of multilingualism requires technical standards that facilitate the use of non-Roman alphabets. One of the early initiatives related to the multilingual use of computers was undertaken by the Unicode Consortium – a non-profit institution that develops standards to facilitate the use of character sets for different languages. In their turn, ICANN (Internet Corporation for Assigned Names and Numbers) and IETF (Internet Engineering Task Force) took an important step in promoting Internationalised Domain Names (IDN). IDN facilitates use of domain names written in Chinese, Arabic, and other non-Latin alphabets.[35]

Machine translation

Many efforts have endeavoured to improve machine translation. Given its policy of translating all official activities into the languages of all member states, the EU has supported various development activities in the field of machine translation. Although major breakthroughs have been made, limitations remain.

Appropriate government frameworks

The promotion of multilingualism requires appropriate governance frameworks. The first element of governance regimes has been provided by organisations such as UNESCO (United Nations Educational, Scientific and Cultural Organization). UNESCO has instigated many initiatives focusing on multilingualism, including the adoption of important documents, such as the Universal Declaration on Cultural Diversity. Another key promoter of multilingualism is the EU, since it embodies multilingualism as one of its basic political and working principles.

The evolution and wide usage of Web 2.0 tools, allowing ordinary users to easily become contributors and content developers, offers an opportunity for greater availability of local content in a wide variety of languages. Nevertheless, without a wider framework for the promotion of multilingualism, the opportunity might end up creating an even deeper gap, if the existing positive feedback loop is not cut: 'new Internet users find it helpful to learn English and employ it on-line, thus reinforcing the language's prestige and forcing subsequent new users to learn English as well'.[36]

Global public goods

The concept of global public goods can be linked to many aspects of Internet governance. The most direct connections are found in areas of access to the Internet infrastructure, protection of knowledge developed through Internet interaction, protection of public technical standards, and access to online education.

Private companies predominantly run the Internet infrastructure. One of the challenges is the harmonisation of the private ownership of the Internet infrastructure with the status of the Internet as a global public good. National laws provide the possibility of private ownership being restricted by certain public requirements, including providing equal rights to all potential users and not interfering with the transported content.

One of the key features of the Internet is that through worldwide interaction of users, new knowledge and information is produced. Considerable knowledge has been generated through exchanges on mailing lists, social networks, and blogs. With the exception of 'creative commons',[37] there is no legal mechanism to protect such knowledge. Left in the legal vacuum, it is made available for modification and commercialisation. This common pool of knowledge, an important basis of creativity, is at risk of being depleted. The more the Internet content is commercialised, the less spontaneous exchanges may become. This could lead towards reduced creative interaction.

The concept of global public goods, combined with initiatives such as creative commons, could provide solutions that would both protect the current Internet creative environment and preserve Internet-generated knowledge for future generations.

With regard to standardisation, almost continuous efforts are made to replace public standards with private and proprietary ones. This was the case with Microsoft (through browsers and ASP) and Sun Microsystems (through Java). The Internet standards (mainly TCP/IP: Transmission Control Protocol/ Internet Protocol) are open and public. The Internet governance regime should ensure protection of the main Internet standards as global public goods.

The issues

Balance between private and public interests

One of the underlying challenges of the future development of the Internet is to strike a balance between private and public interests. The question is how to provide the private sector with a proper commercial environment while ensuring the development of the Internet as a global public good. In many cases it is not a 'zero-sum' but a 'win-win' situation. Google and many other companies of the Web 2.0 wave managed to develop business models which both provide income and enable the creative development of the Internet.

Protecting the Internet as a global public good[38]

Some solutions can be developed based on existing economic and legal concepts. For example, economic theory has a well-developed concept of public goods, which was extended at the international level to global public goods. A public good has two critical properties: non-rivalrous consumption and non-excludability. The former stipulates that the consumption of one individual does not detract from that of another; the latter, that it is difficult, if not impossible, to exclude an individual from enjoying the good. Access to web-based materials and many other Internet services fulfil both criteria: non-rivalrous consumption and non-excludability.

Rights of people with disabilities[39]

The UN estimates that there are 500 million people with disabilities in the world today. This number is increasing every year due to factors such as war and destruction, unhealthy living conditions, or the absence of knowledge about disability, its causes, prevention, and treatment.[40] The Internet provides new possibilities for social inclusion of people with disabilities. In order to maximise technological possibilities for people with disabilities there is a need to develop the necessary Internet governance and policy framework. The main international instrument in this field is the Convention on the Rights of Persons with Disabilities, approved by United Nations in 2006 and already signed by 139 countries, which establishes rights that are now in the process of being included in national legislations, which will make them enforceable within a few years.[41]

Awareness of the need for technological solutions that include people with disabilities is increasing with the work of organisations that teach and foster support for the disabled community, such as the IGF Dynamic Coalition on

Accessibility and Disability[42] and the Internet Society Disability and Special Needs Chapter.[43]

The lack of accessibility arises from the gap between the abilities required to use hardware, software, and content, and the abilities of a person with a disability. To narrow this gap there are two directions of policy actions:

1. Include accessibility standards in the requirements for the design and development of equipment, software, and content.
2. Foster the availability of accessories in hardware and software that increase or substitute the functional capabilities of the person.

In the field of Internet governance, the main focus is on web content, as it is in rapid development and constitutes a kind of infrastructure. Many web applications do not comply with accessibility standards due to a lack of awareness or perceived complexity and high costs (which is far from today's reality). The international standards in web accessibility are developed by W3C which calls them Web Content Accessibility Guidelines (WCAG).[44]

One policy action that should increase the access of people with disabilities is the Internet Society's (ISOC's) Universal Design for the Internet:

> *Universal Design for the Internet is making sure that the presentation of content on the Internet and the design of Internet technology is flexible enough to accommodate the needs of the broadest range of users possible, regardless of age, language, or disability.*[45]

Education

The Internet has opened new possibilities for education. Various e-learning, online learning, and distance learning initiatives have been introduced; their main aim is to use the Internet as a medium for the delivery of courses. While it cannot replace traditional education, online learning provides new possibilities for learning, especially when constraints of time and space impede attendance in person in classes. Some estimates forecast that the online learning market will grow to approximately US$10 billion by the end of 2010.

Traditionally, education has been governed by national institutions. The accreditation of educational institutions, the recognition of qualifications, and quality assurance are all governed at national level. However, cross-

border education requires the development of new governance regimes. Many international initiatives aim at filling the governance gap, especially in areas such as quality assurance and the recognition of academic degrees.

The issues

WTO and education

One controversial issue in the World Trade Organization (WTO) negotiations is the interpretation of Articles 1 (3) (b) and (c) of the General Agreement on Trade in Services (GATS), which specify exceptions from the free trade regime for government provided services. According to one view, supported mainly by the USA and the UK, these exceptions should be treated narrowly, *de facto* enabling free trade in higher education. This view is predominately governed by interests of the English-speaking educational sector to gain global market coverage in education, and has received considerable opposition from many countries.

The forthcoming debate, likely to develop within the context of WTO and other international organisations, will focus on the dilemma of education as a commodity or a public good. If education is considered a commodity, WTO's free trade rules will be implemented in this field as well. A public goods approach, on the other hand, would preserve the current model of education in which public universities receive special status as institutions of importance for national culture.

Quality assurance

The availability of online learning delivery systems and easy entry into this market has opened the question of quality assurance. A focus on online delivery can overlook the importance of the quality of materials and didactics. A variety of possible difficulties can endanger the quality of education. One is the easy entry of new, mainly commercially driven, educational institutions, which frequently have few of the necessary academic and didactical capabilities. Another problem of quality assurance is that the simple transfer of existing paper-based materials to an online medium does not take advantage of the didactic potential of the new medium.

The recognition of academic degrees and the transfer of credits

When it comes to online learning, the main challenge is the recognition of degrees beyond the regional context, mainly at global level.

The EU has started to develop a regulatory framework with the European Credit Transfer System (ECTS). The Asia-Pacific region is following the European lead by introducing its own regional model for the exchange of students and a related credit system (UCTS).

The standardisation of online learning

The early phase of online learning development was characterised by rapid development and high diversity of materials, in the sense of platforms, content, and didactics. However, there is a need to develop common standards in order to facilitate the easier exchange of online courses and introduce a certain standard of quality.

Most standardisation is performed in the USA by private and professional institutions. Other, including international, initiatives are on a much smaller scale.

Child safety online[46]

Children have always been vulnerable to victimisation. Most of the issues related to Internet safety are primarily concerned with youth, especially minors. Yet, the blurred lines commonly become sharper when it comes to child safety. Objectionable content is clearly noted as improper and inappropriate, and includes a wide variety of materials including pornography, hate and violence content, content hazardous to health, suicide advice, anorexia advice, and the like.

The issues

Cyberbullying

Harassment is a particular challenge when minors are targeted. Minors are vulnerable when using the numerous communication tools available such as messaging, chat-rooms, and social networks. Children can easily become victims of cyberbullying – most often from their peers using ICT, combining mobile phone cameras, file-sharing systems and social networks, as convenient tools.

Abuse and sexual exploitation

Harmful conduct targeting minors can be particularly dangerous when conducted by adults. The masked identity is one of the most frequent

approaches undertaken by paedophiles on the Internet. While pretending to be peers, these 'online predators' collect information and steadily groom the chid, easily managing to win the child's trust, even aiming to establish a physical meeting. The virtual conduct thereby transforms to a real contact and can go as far as abuse and exploitation, paedophilia, the solicitation of minors for sexual purposes, and even child trafficking.

Violent games

Violent games (normally in a network environment, i.e. dungeons) are rapidly dominating the 'passively' violent movies. The impact violence has on the behaviour of young people is widely debated. The most infamous games involve sophisticated weapons (showing features of real weapons, and/or other fantasy features) and bloodshed, and are usually tagged as 'stress eliminators'. Indeed, the top 10 games for different hardware platforms, including Microsoft Xbox, Nintendo DS, Nintendo Wii, PC, Playstation, PSP, are dominated by action/violent games.

Addressing the challenges

The major challenge that educators and parents are facing in protecting children online is the fact that the 'digital natives' are much more knowledgeable in how to use ICT; they know more, yet they understand less. Close cooperation between peers, parents, educators, and the community is most important. Parents, policy-makers, and the wider community worldwide are, nevertheless, slowly becoming aware of the situation and are developing initiatives for safeguarding children in computer-mediated environments.

To raise awareness among stakeholders, the European Commission has launched the InSafe project – a European network of e-safety awareness nodes, providing numerous awareness-building materials for parents and educators in several languages, free for download and dissemination. The Polish media campaign on cyberbullying resulted in sets of video clips and an e-learning course on Internet safety for kids. The NetSafe initiative in New Zealand, founded in 1998, is among the first national initiatives on Internet safety; it gathers key stakeholders including ministries, the business sector, and the media.

Among the most successful models of national awareness and training campaigns is the Cyber-Peace Initiative (CPI) of Egypt, under the auspices of Suzanne Mubarak of the Women's International Peace Movement. A group of young enthusiasts, Net-Aman, as well as a group of parents' representatives, have been trained to lead further activities. Together with partners, including

the Ministry of Telecommunications and Microsoft of Egypt, as well as international partners such as ChildNet International, CPI has reached out to tens of thousands of young people and parents around the country within the past few years. It has produced several awareness and educational kits for kids, parents, and educators, translated into Arabic.

A much-needed step beyond awareness building and training of youth, parents, and educators is capacity building in the area of Internet safety, targeted at the multistakeholder composition of policy-makers: government officials, business entities, media, academia and think-thanks, NGOs, etc. Various international organisations are currently discussing possible models of cooperation in establishing such programmes, among which also are the Council of Europe, ITU, CPI, and DiploFoundation.

On a longer timescale, educational curriculum updates are needed, to include Internet safety issues such as: protecting personal privacy and security, protecting personal and others' reputation online, ethics, reporting abuse, transferring real-life morals and skills to the online world, etc. Several such initiatives exist worldwide, such as Cyber Smart!, iKeepSafe, i-Safe, and NetSmartz.

Synchronised national and international legal and policy mechanisms are an indispensable component. One example is the successful pan-European Prague Declaration for a Safer Internet for Children adopted at the Ministerial Conference (April, 2009). The ITU Global Cybersecurity Agenda (GCA) presents the Child Online Protection (COP) initiative as an integral part. There are many other international forums where child protection is an issue high on the agenda, including the IGF with its Dynamic Coalition on Child Online Safety.

International cooperation in the field of child protection has a successful track record in the area of international emergency and hotlines. Some of the successful initiatives are:

- Official cooperation COSPOL Internet Related Child Abusive Material Project (CIRCAMP) initiated by the European Chief of Police Task Force.
- Work of NGOs in cooperation with governments such as Internet Watch Foundation, Perverted Justice Foundation, ICMEC, ECPAT, Save the Children, Internet Content Related Association, Child Exploitation, and Online Protection Centre.
- Public-private partnerships, such as cooperation between the Norway Telecom and the Norway Police.

Endnotes

1 APC's Internet Rights Charter. Available at: **http://www.apc.org/en/node/5677/**

2 Internet Rights and Principles Coalition (2010). Available at: **http://internetrightsandprinciples.org/**

3 The ACP Internet Rights Charter includes: Internet access for all; freedom of expression and association; access to knowledge; shared learning and creation – free and open source software and technology development; privacy, surveillance and encryption; governance of the Internet; awareness, protection and realisation of rights. Available at: **http://www.apc.org/en/node/5677**

4 Global Network Initiative (2010) Available at: **http://www.globalnetworkinitiative.org**

5 Convention on Cybercrime. Available at: **http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm**

6 The Council of Europe adopted the following main declarations of relevance for human rights and the Internet: The Declaration of Freedom of Communication on the Internet (28 May 2003); and The Declaration on Human Rights and the Rule of Law in the Information Society (13 May 2005).

7 Freedom House (2009) *Freedom on the Internet: A global assessment of Internet and digital media.* Available at: **http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTheNet_FullReport.pdf**

8 Zick T (1999) Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998. *Creighton Law Review* **32**:1147, 1153, 1201.

9 For a discussion of Internet gambling, see: Karadbil JF (2000) Note: Casinos of the next millennium: a look into the proposed ban on internet gambling. *Arizona Journal of International and Comparative Law* **17:**413, 437–38.

10 *Internet under surveillance*. Available at: **http://en.rsf.org/spip.php?page=recherche&lang=en&recherche=internet+enimies&image.x=47&image.y=13&image=%3E%3E**

11 Zittrain J, Edelman B (2008) *Documentation of Internet filtering worldwide.* Open Net Initiative. Available at: **http://cyber.law.harvard.edu/filtering/**

12 Official Saudi filtering is provided through 'a proxy farm system'. See: **http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring-mechanism.htm**

13 Electronic Frontiers Australia (2006) *Internet censorship laws in Australia*. Available at: **http://www.efa.org.au/Issues/Censor/cens1.html**

14 Resnick P, Miller J (1996) PICS: Internet access controls without censorship. *Communications of the ACM* **39(10):** 87–93. Available at: **http://www.w3.org/PICS/iacwcv2.htm**

[15] Although Vint Cerf participated in the panel, he objected to the final report, which he said did not focus on the flaws or the larger implications of installing online gates. Guernsey L (2001) *Welcome to the world wide web. Passport please*. Available at: **http://www.criminology.fsu.edu/transcrime/articles/Welcome%20to%20the%20World%20Wide%20Web_%20Passport,%20Please.htm**

[16] Akami claims that it can identify people's geographical location as far as their ZIP codes. This is the technological limit. Information about street addresses cannot be obtained from IP numbers. *Silicon Valleys Quova Inc., one of the leading providers of this technology, claims it can correctly identify a computer user's home country 98 percent of the time and the city about 85 percent of the time, but only if it's a large city. Independent studies have pegged the accuracy rate of such programs, which also are sold by companies such as InfoSplit, Digital Envoy, Netgeo, and Akami, at 70 to 90 percent*. Cha AE (2002) Rise of internet borders prompts fears of web's future. *Washington Post,* 4 January. Available at: **http://www.google-watch.org/geolocat.html**

[17] For a survey of articles about the Google-China case, see: **http://searchenginewatch.com/sereport/article.php/2165031**

[18] Knight W (2002) Google keywords knock Chinese surfers offline. *New Scientist Internet edition*, 13 September. Available at: **http://www.newscientist.com/article/dn2797-google-keywords-knock-chinese-surfers-offline.html**

[19] Knight W (2002) On-off access for Google in China. *New Scientist Internet edition*, 13 September. Available at: **http://www.newscientist.com/article/dn2795-onoff-access-for-google-in-china.html**

[20] Zittrain J, Edelman B (2002) *Localised Google search result exclusions: statement of issues and call for data*. Harvard Law School. Available at: **http://cyber.law.harvard.edu/filtering/google/**

[21] EU Information Society (2005) *Safer Internet Programme*. Available at: **http://europa.eu/legislation_summaries/information_society/l24190d_en.htm**

[22] Lessig L (1996) The zones of cyberspace. *Standford Law Review* **48:** 1403, 1405.

[23] European Internet Service Providers Association (EuroISPA) adopted *Human rights guidelines for Internet service providers*. It is an interesting example of self-regulation on the issues of broader public relevance (human rights). Available at: **http://www.euroispa.org/files/human_rights_guidelines.pdf**

[24] Operation Clambake (2010) *Church of Scientology censors net access for members*. Available at: **http://www.xenu.net/archive/events/censorship**

[25] Valuable comments and input were provided by Katitza Rodriguez.

[26] This report explains the problem of the privatisation of surveillance and new challenges linked to the protection of privacy: Stanley J (2004) *The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society*. ACLU: New York, NY, USA. Available at: **http://www.aclu.org/FilesPDFs/surveillance_report.pdf**

[27] USA Patriot Act (2001) Available at: **http://www.epic.org/privacy/terrorism/hr3162.html**

[28] For a discussion of customer trust in business privacy protection, see: Whiting R (2002) Wary customers don't trust business to protect privacy. *Information Week,* 19 August. Available at: **http://www.informationweek.com/shared/printableArticle.jhtml?articleID=6503045**

[29] Overview of the Gramm-Leach-Bliley Act. Available at: **http://www.frbsf.org/publications/banking/gramm/grammpg1.html**

[30] Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information. Available at: **http://www.ftc.gov/privacy/glbact/glboutline.htm**

[31] Children's Online Privacy Protection Act of 1998. Available at: **http://www.ftc.gov/ogc/coppa1.shtm**

[32] Health Insurance Portability and Accountability Act of 1996, *Public Law* 104–191, § 264; Department of Health and Human Services, Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59917. Available at: **http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html**

[33] Connolly C (2008) *The US Safe Harbor – Fact or Fiction?* Galexia: Pyrmont, Australia. Available at: **http://www.galexia.com/public/research/articles/research_articles-pa08.html**

[34] For more information regarding multilingualism on the Internet, see: Al-Shatti Q, Aquirre R, Cretu V (2007) *Multilingualism – the communication bridge.* DiploFoundation Internet Governance Research Project. Available at: **http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241**

[35] For more information on IDN, see: Marson C (2010) Internationalization in Names and Other Identifiers. *IEFT Journal* **5(3).** Available at: **http://www.isoc.org/tools/blogs/ietfjournal/?p=1521** (scroll down).

[36] Wikipedia (2010) *English in computing.* Available at: **http://en.wikipedia.org/wiki/English_on_the_Internet#Internet_content**

[37] Creative Commons (CC) is a non-profit organisation headquartered in San Francisco, California, United States devoted to expanding the range of creative works available for others to build upon legally and to share. The organisation has released several copyright-licenses known as Creative Commons licenses free of charge to the public. These licenses allow creators to communicate which rights they reserve, and which rights they waive for the benefit of recipients or other creators (Source: Wikipedia).

[38] Arata S, Psaila S (2006) *Protection of Public Interest on the Internet.* DiploFoundation Internet Governance Research Project. Available at: **http://www.diplomacy.edu/ig/Research/display.asp?Topic=Research%20Themes%20II#Protection**

[39] Valuable comments and inputs were provided by Jorge Plano.

[40] hrea.org (2010) *Human rights of persons with disabilities.* Available at: **http://www.hrea.org/index.php?base_id=152**

[41] UN Enable (2010) *Rights and dignity of persons with disabilities.* Available at: **http://www.un.org/disabilities/**

[42] IGF (2010) *Dynamic Coalition on Accessibility and Disability*. Available at: **http://www.intgovforum.org/cms/dynamic-coalitions/80-accessibility-and-disability**

[43] ISOC (2010) *Internet Society Disability and Special Needs Chapter*. Available at: **http://www.isocdisab.org**

[44] W3C (1999) *Web Content Accessibility Guidelines 1.0*. Available at: **http://www.w3.org/TR/WCAG10/**

[45] Burks M, Waddell C (2001) *Universal design for the Internet.* ISOC Member Briefing No. 2. Available at: **http://www.isoc.org/briefings/002/isocbriefing02.txt**

[46] This text was prepared by Vladimir Radunovic for the Advanced Course on Cybersecurity and Internet Safety (Internet Governance Capacity Building Program – DiploFoundation).

Section 7

Internet governance stakeholders

Internet governance stakeholders

One of the distinctive features of Internet governance has been multistakeholder participation, a natural facet of Internet governance discussions as non-state actors have played predominant roles in the development and management of the Internet. Civil society, particularly academia, has been a vital player in the Internet field since its early days. It established the core Internet protocol (Transmission Control Protocol/Internet Protocol; TCP/IP) and services (e-mail). The business sector is developing the technological infrastructure, including computers, networks, and software. Governments are relative newcomers to the Internet governance field.[1]

The major difference between Internet governance negotiations and other global negotiations, such as environmental negotiations, is that while in other negotiations, intergovernmental regimes gradually opened to non-governmental players, in Internet governance negotiations, governments had to enter an existing non-governmental regime, built around IETF (the Internet Engineering Task Force), ISOC (the Internet Society) and ICANN (the Internet Corporation for Assigned Names and Numbers). Once Internet governance became a global issue, there was a need to converge these two regimes (non-governmental and traditional diplomatic) through the development of a multistakeholder policy framework.

The first successful experiment in this direction was the Working Group on Internet Governance (WGIG) during the Word Summit on the Information Society (WSIS) process (2002–2005).[2] WGIG was more than an expert,

Internet governance – variable geometry approach

Internet governance requires the involvement of a variety of stakeholders who differ in many aspects, including international legal capacity, interest in particular Internet governance issues, and available expertise. Such variety may be accommodated within a single Internet governance framework using the variable geometry approach. This approach, which reflects stakeholder interests, priorities, and capacities to tackle Internet governance issues, is implied in Article 49 of the WSIS declaration, which specifies the following roles for the main stakeholders:

- States – policy authority for Internet-related public policy issues (including international aspects).
- The private sector – development of the Internet, both in the technical and economic fields.
- Civil society – important role on Internet matters, especially at the community level.
- Intergovernmental organisations – the coordination of Internet-related public policy issues.
- International organisations – development of Internet-related technical standards and relevant policies.[4]

advisory group, but less than a decision-making body.[3] It did not produce official UN documents, but it substantially influenced WSIS negotiations on Internet governance. WGIG was a compromise in which pro-ICANN governments let Internet governance issues officially emerge onto the multilateral diplomatic agenda and in which other governments, mainly from developing countries, accepted the participation of non-state actors. This compromise resulted in the success of WGIG.

As a follow-up to WSIS, Internet governance remains on the global agenda through the Internet Governance Forum (IGF).

The IGF follows the WGIG participation structure. Both WGIG and the IGF remain useful examples for the future development of multistakeholder partnerships at international level.

Governments

The last seven years – since the introduction of Internet governance to policy agendas in 2003 – have been a learning process for many governments. Even for large and wealthy countries, dealing with Internet governance issues has

posed numerous challenges, such as managing the multidisciplinary nature of Internet governance (technological, economic, and social aspects), and has involved a wide variety of actors. Many governments had to train officials, develop policy, and actively participate in various Internet governance forums while still getting to grips with the new phenomenon of Internet governance.

National coordination

In 2003, at the beginning of the WSIS process, most countries addressed Internet governance issues through 'technical' ministries, usually those that had been responsible for relations with the International Telecommunication Union (ITU). Gradually, as they realised that Internet governance was more than 'wires and cables', governments began to involve officials from other, less technical ministries, such as culture, media, and justice.

The principal challenge for many governments has been to develop a strategy to gather and effectively coordinate support from non-state actors, such as universities, private companies, and non-governmental organisations (NGOs) that have the necessary expertise to deal with Internet governance issues. During the WSIS process, most large and medium-sized states managed to develop sufficient institutional capacity to follow global Internet governance negotiations. Some of them, such as Brazil, developed an innovative national structure for following the Internet governance debate, involving telecom ministries, the diplomatic service, the business sector, civil society, and academia.[5]

Cable 'geo-strategy' and policy (in)coherence

The Anglo-French Entente was established in 1904. However, by establishing a close cooperation with Germany, the French Telegraph Ministry did not follow the country's general policy. The ministry wanted to reduce British dominance in the global 'cable geo-strategy' while laying new telegraph cables in cooperation with Germany. French historian Charles Lesage made the following comment on this policy (in)coherence:

The prolonged disagreement between the general principles of French diplomacy and the procedures of the telegraphic policies come, I believe, from the fact that in this country, each ministry has its own foreign policy: the Ministry of Foreign Affairs has one, the Ministry of Finance has another.... The Postal and Telegraph Administration also has, from time to time, a foreign policy; as it so happened, in these past few years, without being entirely hostile to England, it demonstrated a strong inclination to Germany.[6]

Policy coherence

Given the multidisciplinary nature of Internet governance and the great diversity of actors and policy forums, it is particularly challenging to achieve policy coherence. It requires many governments to have a flexible form of policy coordination, including horizontal communication among different ministries, the business sector, and other actors. Traditional governmental structure, based on a strong hierarchy, could be an obstacle to the development of such flexible coordination.

Apart from the management challenge, achieving policy coherence is usually limited by the existence of competing policy interests. This is especially true in countries with well-developed and diversified Internet economies. For example, network neutrality is one of the latest issues in which the US government has become involved in a delicate balancing act between the Internet sector of the economy (Google, Yahoo!) who are strong supporters and the telecommunication/entertainment sector (Verizon and AT&T, Hollywood lobby), which sees it as an obstacle to developing a new business model based on faster Internet(s) for delivery of multimedia content.

Technological convergence between various media will provide another impetus for achieving policy coherence. Previously distinct policy areas, such as telecommunication and broadcasting, will have to merge in order to reflect technological convergence.

See Section 2 for further discussion on convergence

The importance of Geneva-based permanent missions

For many governments, their permanent missions in Geneva were important, if not vital, players in the WSIS and Internet governance processes. Most activities took place in Geneva, home to ITU, which played the main role in the processes. The first WSIS in 2003 took place in Geneva and all but one of the preparatory meetings were held in Geneva, keeping permanent missions based in Geneva directly involved. Currently, the IGF Secretariat is based in Geneva and all IGF preparatory meetings are held in the city.

For large and developed countries, the permanent missions were part of the broad network of institutions and individuals that dealt with the WSIS and Internet governance processes. For small and developing countries, permanent missions were the primary and, in some cases, the only players in the processes. The WSIS portfolio added to the agenda of the usually small and over-stretched missions of developing countries. In many cases, the same diplomat had to undertake the tasks associated with WSIS along with other issues, such as human rights, health, trade, and labour.

'Diplomatisation' of the Internet governance process

WSIS put the Internet on the global diplomatic agenda. Prior to WSIS, the Internet had been discussed primarily in non-governmental circles or at national level. The 'diplomatisation' of Internet policy issues stimulated different reactions. Kenneth Neil Cukier, technology correspondent for *The Economist*, stressed the negative aspect of the 'diplomatisation' of the Internet governance discussion:

> *...by elevating the issue to a formal United Nations summit, this by nature escalates the importance of the topic inside governments. As a result, issues about the Information Society, that were treated by less political and less visible parts of the government – as science and technology and policy or as a media and cultural matter – were shifted to foreign ministries and long-standing diplomats, who are more accustomed to power politics and less knowledgeable of technology issues and the Internet's inherent requirement for cooperation and interdependence.*[7]

The diplomatisation process had certain positive effects on the WSIS discussions. For example, diplomats provided non-partisan contributions to long-standing debates on issues related to ICANN: domain names, Internet numbers, and root servers.

See Section 8 for further discussion on the role of Nitin Desai and Markus Kummer in the IGF

The contributions of diplomats were particularly noticeable in the WGIG debate. WGIG's diplomatic leadership (Chairperson Nitin Desai and Executive Director Markus Kummer) created an inclusive atmosphere where differences among representatives, including those of the technical community, did not block the process. The WGIG process resulted in a Final Report that voiced differences, but also provided a process-related solution for future discussions by establishing the IGF.

The US government's position

The Internet was developed as part of a US-government-sponsored project. From the origin of the Internet until today, the US government has been involved in Internet governance through various departments and agencies, initially, the Department of Defense, later the National Science Foundation, and most recently the Department of Commerce. The Federal Communication Commission has also played an important role in creating a regulatory framework for the deployment of the Internet.

One constant of US government involvement has been its hands-off approach, usually described as 'distant custodian'. It sets the framework while leaving the governance of the Internet to those directly working with it, mainly the Internet community. However, the US government has intervened more directly on a few occasions, as occurred in the mid-1990s when the CORE project could have moved the root server and management of the core Internet infrastructure from the USA to Geneva. This process was stopped by a famous – at least in the history of the Internet – diplomatic note sent by then US Secretary of State Madeleine Albright to the ITU Secretary General.[8] In parallel to stopping the CORE initiative, the US government initiated consultations that resulted with the establishment of ICANN.

Since the creation of ICANN, the US government has indicated its intention to withdraw from the supervision of ICANN once it achieves institutional and functional robustness. This withdrawal process was initiated at the beginning of October 2009 with signing of the Affirmation of Commitments by the US Department of Commerce and ICANN. According to this document, ICANN will become an independent organisation. The other element of the special relationship between the US Department of Commerce and ICANN – the IANA (Internet Assigned Numbers Authority) contract – will be reviewed in 2011.

On the global scene, during the WSIS process, the USA opposed a possible take-over of ICANN's functions by an intergovernmental body. However, in the WSIS process, the US government took the first steps towards internationalisation of ICANN's role by recognising the right of national governments over their respective domain names and accepting the continuation of international discussions through the establishment of the IGF.

The position of other governments

An Internet governance policy spectrum started to take shape recently with governments developing their national positions. At one end of the policy spectrum, there was a view that an intergovernmental organisation, such as ITU, should govern the Internet. This was the initial position of many developing countries. The most vocal in advocating a prominent role for ITU were China, Iran, and Russia. Some developing countries argued for creating a new international organisation to replace ITU, including the establishment of a new treaty-based organisation, such as the 'International Internet Organisation', perhaps. Other countries argued that a new type of multistakeholder organisation should govern the Internet.

In the centre of the policy spectrum were governments arguing that ICANN should retain its technical functions while a new international public body should have the policy oversight function. This is the position that has gradually been taken by the EU.

At the other end of the policy spectrum, the USA argued that nothing in the current ICANN-based regime needed to change. Canada, Australia, and New Zealand offered similar views, additionally arguing for greater internationalisation of ICANN. Those countries, together with the EU, Switzerland, and a few developing countries have been significant in achieving compromise solutions on Internet governance during the WSIS process.

The position of small states

The complexity of the issues and the dynamics of activities made it almost impossible for many small and, in particular, small developing countries, to follow developments, let alone have any substantive effect. As a result, some small states supported a one-stop-shop structure for Internet governance issues.[9] The sheer size of the agenda and the limited policy capacity of developing countries in both their home countries and in their diplomatic missions remained one of the main obstacles for their full participation in the process. The need for capacity building in the field of Internet governance and policy was recognised as one of the priorities for the WSIS Tunis Agenda for the Information Society.

The business sector[10]

See Section 3 for further discussion on trademarks

When ICANN was established in 1998, one of the main concerns of the business sector was the protection of trademarks. Many companies were faced with cybersquatting and the misuse of their trademarks by individuals who were fast enough to register them first. In the process of creating ICANN, business circles clearly prioritised dealing with the protection of trademarks and, accordingly, this issue was immediately addressed once ICANN was created.[11]

Today, with the growth of the Internet, the business interest in Internet governance has widened and diversified, with the following main groups of business companies: domain name companies, Internet service providers (ISPs), telecommunication companies, software developers, and Internet content companies.

The International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC), well known as an association representing business across sectors and geographic borders, positioned itself as one of the main representatives of the business sector in the global Internet governance process. ICC was actively involved in the early WGIG negotiations and WSIS, and continues to be an active contributor in the current IGF process.

Domain name companies

Domain name companies include registrars and registries who sell Internet domain names (e.g. .com, .edu). The main players in this sector include VeriSign and Affilias. Their business is directly influenced by ICANN policy decisions in areas such as the introduction of new domains and dispute resolution. It makes them one of the most important stakeholders in the ICANN policy-making process. They have also been involved in the broader Internet governance policy process (WSIS, WGIG, IGF) with the main objective of reducing the risk of a potential take-over of ICANN's role by other players, mainly national governments and international organisations.

Internet service providers

See Section 2 for further discussion on ISPs

ISPs are companies or organisations that act as gateways through which the Internet is accessed. Since ISPs are the key online intermediaries, it makes them particularly important for Internet governance. Their main involvement is at national level in dealing with government and legal authorities. At global level, some ISPs particularly from the USA and Europe have been active in the WSIS/WGIG/IGF processes individually, even more so through ICC and its BASIC initiative, and through national and regional or sector-specific business organisations such as ETNO (European Telecommunications Network Operators' Association), ITAA (Information Technology Association of America), and others.

Telecommunication companies

These companies facilitate Internet traffic and run the Internet infrastructure. The main players include companies such as Verizon and AT&T. Traditionally, telecommunication companies have participated in international telecommunication policy through ITU. They have been increasingly involved in the activities of ICANN and the IGF. Their primary interest in Internet

governance is to ensure a business-friendly global environment for the development of an Internet telecommunication infrastructure.

Software companies

See Section 3 for further discussion on IPR

Companies such as Microsoft, Adobe, and Oracle are mainly involved in the activities of different standardisation bodies (W3C – Word Wide Web Consortium; IETF). In the early days of the WSIS process, their main concern was the possibility of opening discussion on intellectual property rights (IPR) on the Internet. After it was clear that WSIS would not move into the IPR field, the software companies' interest in participating in the WSIS process diminished. This trend has continued since the Summit.

Internet content companies

These include the main Internet brand names such as Google, Facebook, and Twitter. This group of companies became increasingly important with the development of Web 2.0 applications. Their business priorities are closely linked to various Internet governance issues such as intellectual property, privacy, and cybersecurity. Their presence is increasingly noticeable in global Internet governance processes.

Civil society

NGOs and WSIS

NGO participation in WSIS was relatively low. Out of close to 3000 NGOs that have consultative status with the UN ECOSOC (Economic and Social Council), only 300 participated in WSIS.

Civil society has been the most vocal and active promoter of a multistakeholder approach to Internet governance. The usual criticism of civil society participation in previous multilateral forums had been a lack of proper coordination and the presence of too many, often dissonant, voices. In the WSIS process, however, civil society representation managed to harness this inherent complexity and diversity through a few organisational forms, including a Civil Society Bureau, the Civil Society Plenary, and the Content and Themes Group. Faced with limited possibilities to influence the formal process, civil society groups developed a two-track approach. They continued their presence in the formal process by using available opportunities

to participate and to lobby governments. In parallel, they prepared a Civil Society Declaration as an alternative vision to the main declaration adopted at the Geneva WSIS summit.

Due to WGIG's multistakeholder nature, civil society attained a high level of involvement. Civil society groups proposed eight candidates for WGIG, all of whom were subsequently appointed by the UN Secretary General. In the Tunis phase (the second phase of WSIS, after Geneva), the main policy thrust of civil society organisations shifted to WGIG, where they influenced many conclusions as well as the decision to establish the IGF as a multistakeholder space for discussing Internet governance issues. Civil society has continued to be actively involved in IGF activities.

International organisations

ITU was the central international organisation in the WSIS process. It hosted the WSIS Secretariat and provided policy input on the main issues. ITU involvement in the WSIS process was part of its ongoing attempt to define and consolidate its new position in the fast-changing global telecommunications arena, increasingly shaped by the Internet. ITU's role has been challenged in various ways. It was losing its traditional policy domain due to the WTO-led liberalisation of the global telecommunications market. The latest trend of moving telephone traffic from traditional telecommunications to the Internet (through Voice-over Internet Protocol – VoIP) further reduced the ITU's 'regulatory footprint' on the field of global telecommunications.

The possibility that ITU might have emerged from the WSIS process as the *de facto* 'International Internet Organisation' caused concern in the USA and some developed countries, while garnering support in some developing countries. Throughout WSIS, this possibility created underlying policy tensions. It was particularly clear in the field of Internet governance, where tension between ICANN and ITU had existed since the establishment of ICANN in 1998. WSIS did not resolve this tension. With the increasing convergence of various communication technologies, it is very likely that the question of ITU's more active role in the field of Internet governance will be re-emerging in policy discussion.

Another issue concerned the anchoring of the multidisciplinary WSIS agenda within the family of UN specialised agencies. Non-technical aspects

of communications and Internet technology, such as social, economic, and cultural features, are part of the mandate of other UN organisations. The most prominent player in this context is UNESCO (UN Educational, Scientific and Cultural Organization), which addresses issues such as multilingualism, cultural diversity, knowledge societies, and information sharing. The balance between ITU and other UN organisations was carefully managed. The WSIS follow-up processes also reflect this balance, with the main players including ITU, UNESCO, and UNDP (United Nations Development Programme).

Other participants

In addition to the formal WSIS stakeholders, other players – the Internet community and ICANN – who were not officially recognised as stakeholders participated in the process mainly through civil society and business sectors.

The Internet community

Terminology

Other terms are used interchangeably with 'Internet community', such as Internet developers, Internet founders, Internet fathers, and technologists. We use the term 'Internet community' because it implies a high level of shared values among its members. This set of shared values is one of the distinctive characteristics of the community.

The Internet community includes institutions and individuals who have developed and promoted the Internet since its inception. Historically, members of the Internet community were linked to US universities, where they worked primarily to develop technical standards and establish the basic functionality of the Internet. The Internet community also created the initial spirit of the Internet, based on the principles of sharing resources, open access, and opposition to government involvement in Internet regulation. From the beginning, its members protected the initial concept of the Internet from intensive commercialisation and extensive government influence.

In the context of international relations, the Internet community is an epistemic community.[12] The early Internet community was coordinated by a few, mainly tacit, rules and one main formal procedure – Request for Comments (RFC). All main and basic standards of the Internet are described through RFCs. While they did not have a strict regulation or formal structure, the early Internet communities were governed by strong custom and peer-

to-peer pressure. Most participants in this process shared similar values, appreciation systems, and attitudes.

See Section 1 for further discussion on the DNS war

The early management of the Internet by the Internet community was challenged in the mid-1990s after the Internet became part of global social and economic life. Internet growth introduced a group of new stakeholders, such as the business sector, that came with different professional cultures and understanding of the Internet and its governance, which led to increasing tension. For example, in the 1990s, Internet communities and Network Solutions,[13] were involved in the so-called 'DNS war', a conflict over the control of the root server and Domain Name System.

Today, the Internet community is represented through ISOC and IETF. ISOC has played a vital role in Internet standardisation and the promotion of the Internet's core values, such as openness. It is also actively involved in capacity building and in assisting developing countries, mainly in Africa, to develop a basic Internet infrastructure.

The Internet community has been an important actor in the process of both establishing and running ICANN. One of the 'fathers of the Internet', Vint Cerf, was the Chair of the ICANN Board from 2000 to 2007. Members of the Internet community hold important positions in various ICANN decision-making bodies.

Another criticism focuses on the fact that, with 2 billion users, the Internet has outgrown the ICANN-based policy framework focusing on the Internet community as the main constituency. Following this argument, as the line between citizens and Internet-users blurs, greater involvement of governments and other structures representing citizens is required, rather than those representing Internet users only, frequently described as the 'Internet community'. Those who argued for more government involvement in Internet governance used this approach of representing citizens rather than Internet users and communities.

The Internet community usually justifies its special position in Internet governance by its technical expertise. It argues that ICANN is a mainly technical organisation and, therefore, technical people using technical knowledge should run it. With the growing difficulty of maintaining ICANN as an exclusively technical organisation, this justification of the special role of the Internet community has faced frequent challenges. It is very likely that the members of the Internet community will gradually integrate into the core stakeholder groups, mainly civil society and business, but also governments.

While the Internet community may disappear as a distinct stakeholder group, it will be important to preserve the values it has been promoting: openness, knowledge sharing, and the protection of the interests of Internet users.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is the main Internet governance institution. Its responsibility is to manage the core Internet infrastructure, which consists of Internet Protocol (IP) addresses, domain names, and root servers. Growing interest in a role for ICANN developed in parallel with the rapid growth of the Internet in the early 2000s and ICANN came to the attention of global policy circles during the WSIS process (2002–2005).

While ICANN is the main actor in the Internet governance field, it does not govern all aspects of the Internet. It is sometimes, although erroneously, described as the 'Internet government'. ICANN manages the Internet infrastructure, but it does not have authority over other aspects of Internet governance, such as cybersecurity, content policy, copyright protection, protection of privacy, maintenance of cultural diversity, or bridging the digital divide.

ICANN is a non-profit corporation registered in California. Its functional authority rested on its Memorandum of Understanding (MoU) with the US Department of Commerce, initially signed in 1998 and extended twice, the second time from September 2006 to September 2009. As of 1 October 2009, the formal basis for ICANN's function is the Affirmation of Commitments signed by ICANN and the US Department of Commerce. This document paves the way for ICANN as an independent institution.

ICANN is a multistakeholder institution involving a wide variety of actors in different capacities and roles. They fall into four main groups.

1. Actors that have been involved since the days when ICANN was established, including the Internet community, the business community, and the US government.
2. International organisations, with the most prominent role played by ITU and the World Intellectual Property Organization (WIPO).
3. National governments whose increasing interest in having a bigger role in ICANN started with the WSIS process.
4. Internet users (at-large community).

ICANN has experimented with various approaches in order to involve Internet users. In its early days, the first attempt was to involve Internet users through direct elections of their representatives to ICANN governing bodies. It was also an attempt to secure ICANN a legitimate base. With low turnout and misuse of the process, the direct vote failed by not providing real representation of Internet users. More recently, ICANN has been trying to involve Internet users through an 'at-large' governance structure. This organisational experiment is ongoing.

ICANN's decision-making process was influenced by early Internet governance processes based on bottom-up, transparent, open, and inclusive approaches. One main difference between the early Internet community of the 1980s and the current ICANN decision-making context is the level of 'social capital'. In the past, the Internet community had high levels of mutual trust and solidarity that made decision-making and dispute resolution much simpler than it is now. The growth of the Internet involved other stakeholders and, consequently, it would be difficult to identify any social capital among current Internet users. Thus, the request by the Internet community to keep some of the early Internet decision-making procedures is largely utopian. Without social capital, the only way to ensure a fully functional decision-making process is to formalise it and develop various checks-and-balance mechanisms.

Some corrections to decision-making procedures have already been made to reflect this changing reality. The most important was the 2002 reform of ICANN, which included strengthening the Governmental Advisory Committee (GAC) and abandoning the direct voting system.

The issues

Technical vs policy management

The dichotomy between technical and policy management has created continuous tension in ICANN's activities. ICANN has portrayed itself as a 'technical coordination body for the Internet' that deals only with technical issues and stays away from the public policy aspects of the Internet. ICANN officials considered this specific technical nature as the main conceptual argument for defending the institution's unique status and organisational structure. The first Chair of ICANN, Esther Dyson, stressed that:

> *ICANN does not 'aspire to address' any Internet governance issues; in effect, it governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the DNS in particular.*[14]

Critics of this assertion usually point to the fact that no technically neutral solutions exist. Ultimately, each technical solution or decision promotes certain interests, empowers certain groups, and affects social, political, and economic life. Decisions on issues such as the .xxx (adult materials) clearly illustrate that ICANN will have to deal with public policy aspects of technical issues.

ICANN's international status

The special ties between ICANN and the US government have been the major focus of criticism, which takes two main forms. The first rests on principle considerations, stressing that the vital element of the global Internet infrastructure, which could affect all nations, be supervised by one country alone. This criticism was apparent during the WSIS process and was enhanced by general suspicion of US foreign policy after the military intervention in Iraq. At this level of discussion, the usual counter-argument is that the Internet was created in the USA with the government's financial support. This gives the US government the moral grounds to decide on the form and tempo of the internationalisation of Internet governance. This argument is particularly powerful in the US Congress, which has strongly opposed any such internationalisation.

The second form rests on practical and legal considerations. For example, some critics argue that if the US judiciary exercises its role and properly implements the sanctions regime against Iran and Cuba, it could force ICANN – as a US private entity – to remove country domains for those two countries from the Internet. According to this argument, by retaining the Iranian and Cuban domain names, ICANN is breaching US sanctions law. While removal of country domain names has never happened, it remains a possibility given the current legal status of ICANN.

A new point in the discussion of the status of ICANN is signalled by the signing of the Affirmation of Commitments. It provides the basis for an independent ICANN and opens a new set of issues about future supervision, reporting, relations with governments, etc.

Both key issues – dealing with public policy matters and internationalisation – could be settled by changing the status of ICANN, which would reduce the ambiguities and improve the clarity of its mission. The future development of ICANN will require innovative solutions. A possible compromise solution could be to transform ICANN into a *sui generis* international organisation, which would preserve all the advantages of the current ICANN structure as well as address shortcomings, particularly the problem of its international legitimacy.

Endnotes

1 The exception was the US government and a few developed countries (Australia, New Zealand and, at that time, the European Commission).

2 The WSIS process started with the first preparatory meeting held in July 2002 in Geneva. The first summit was held in Geneva (December, 2003) and the second summit in Tunisia (November, 2005).

3 The selection of WGIG members combined both representation and expertise criteria. The representation structure was guided by a principle of one-third of participants from governments, civil society, and the business sector. Government representatives were selected according to the usual criteria of the UN regional groups. While observing the representation aspect, selected members were supposed to be knowledgeable about the subject in order to contribute substantially to the WGIG discussion.

4 WSIS Declaration of Principles, WSIS-03/GENEVA/DOC/4-E, 12 December 2003, Article 49. Available at: **http://www.itu.int/wsis/docs/geneva/official/dop.html**

5 The Brazilian model of the management of its country domain name is usually taken as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains is open to all users, including government authorities, the business sector, and civil society. Brazil gradually extended this model to other areas of Internet governance, especially in the process of the preparation for the 2007 IGF, which was hosted in Rio de Janeiro.

6 Lesage C (1991) *La rivalite franco-britannique. Les cables sous-marins allemands* (Paris, 1915) pp. 257–258; quoted in Headrick DR, *The Invisible Weapon: Telecommunications and International Politics 1851–1945.* Oxford University Press: Oxford, UK, p. 110.

7 Cukier KN (2005) The WSIS wars: an analysis of the politicization of the Internet, in *The World Summit on the Information Society: Moving from the past into the future.* Stauffacher D, Kleinwächter W (eds). United Nations ICT Task Force: New York, NY, USA, p. 176.

8 The US government criticised ITU involvement in the establishment of CORE in a telegram: *'without authorization of member governments to hold a global meeting involving an unauthorized expenditure of resources and concluding 'international agreements'*.

9 The convenience of one-stop shopping was one of the arguments for establishing ITU as the central Internet governance player.

10 Valuable comments were provided by Ayesha Hassan.

11 Establishment of the Uniform Domain-Name Dispute-Resolution Policy (UDRP).

12 The Internet community fulfils all the criteria in Peter Haas's definition of an epistemic community: *a professional group that believes in the same cause and effect relationships, truth test to accept them, and shares common values; its members share a common understanding of the problem and its solutions*. Haas P (1990) *Saving the Mediterranean: the politics of international environmental co-operation.* Columbia University Press: New York, NY, USA, p. 55.

[13] Network Solutions is a technology company founded in 1979. The domain name registration business has become the most important division of the company. As of January 2009, Network Solutions managed more than 6.6 million domain names (Source: Wikipedia).

[14] The Berkman Center for Internet and Society, *The debate over Internet governance: a snapshot in the year 2000.* Available at: **http://cyber.law.harvard.edu/is99/governance/introduction.html#_ftn10**

Section 8

Internet governance process

Internet governance process

This section presents the experiences of the Internet Governance Forum (IGF) policy process, which although not particularly visible on the global policy scene, is an extremely relevant experiment in global governance. In a time when there is a need to improve the success rate in global governance, the IGF can provide some useful lessons.

What policy-makers can learn from the IGF

The debate on the reform of global governance accelerated after the failure of the 2009 Copenhagen summit on climate change with the focus on two underlying questions:

1. How to make global governance broad enough to include all relevant players.
2. How to make global governance deep enough to incorporate an efficient and effective decision-making process.

The recipes are different. Many are trying to reduce complexity by introducing a G20-type 'global management board' or focusing on input from regional/interest groups or reducing the 'noise' of participation by non-state actors.[1] Others consider that the UN can/should be reformed to become a principal venue for managing global issues. More still are looking for new and innovative formats that will make global governance both broad enough (legitimate) and deep enough (efficient/effective) to address complex policy issues, such as climate change, migration, and global health.

What is the Internet Governance Forum?

The IGF is the main global body for addressing Internet public policy issues. It was created at the World Summit on the Information Society (WSIS) in Tunis in 2005 as a result of a compromise between government-centred and non-governmental management of the Internet.[2] As a result of this compromise, the IGF was neither the subject of great expectations nor the result of a grand design. Step by step, without fancy words or sonorous proclamations, the IGF's *modus operandi* has developed. So far the IGF has had four annual meetings: Athens (2006), Rio de Janeiro (2007), Hyderabad (2008), Sharm el Sheikh (2009). It has a tiny Secretariat based in Geneva. It has also inspired the creation of series of regional and national IGFs, academic networks (GIGANet) and other side activities.

When discussing how other global governance fields can benefit from the IGF experience, it is important to keep in mind two differences between Internet governance and traditional multilateralism. First, the latter, such as climate change, has gradually opened up to non-governmental players. In the case of Internet governance, governments were obliged to enter an already-existing non-governmental organisation (NGO) managed by ICANN (Internet Corporation for Assigned Names and Numbers), IETF (Internet Engineering Task Force), and other entities. Secondly, the IGF is not a decision-making body. It does not have a mandate to adopt international treaties or other legal documents. It is a 'decision-shaping' forum which, through its deliberation, creates a basis for decisions adopted by other institutions such as ICANN, ITU (International Telecommunication Union) and WIPO (World Intellectual Property Organization) to name a few.

The IGF experience and lessons learned are organised in four main clusters:

1. Approaches for addressing global policy issues.
2. Management of policy processes.
3. Dealing with scientific and technical aspects of policy issues.
4. Increasing inclusiveness and participation.

Approaches for addressing global policy issues

Global challenges do not necessarily need global solutions

One of the global governance mantras is that for global problems we need global solutions. Climate change does not observe national borders. Internet communication easily bypasses traditional sovereign limitations. The argument is that if the policy is not global, there is a risk that national and regional practices may undermine the global cause. For example, some countries

increasing their $C0_2$ emissions could undermine the effect of other countries' attempts to decrease theirs. Thus, using this line of argument, the only way to address global problems is through global solutions. Other arguments could sound counterintuitive.

The problem is that while trying to reach a global deal, it is possible to miss out on many other local, national, and regional policy possibilities. Copenhagen climate change negotiations showed that it is not easy to reach a global deal. It is difficult to incorporate the diversity of interests and professional/national approaches in one paper to be signed by everybody. In the field of climate change, there are many non-global policy initiatives, including those from the private sector, local authorities, and the business sector. The IGF is a role model in this respect.

The IGF was not designed to create a global, legally binding deal. Instead, it has provided space to promote diverse regional and national Internet governance initiatives as well as to create links and synergies between them. Brazil has a remarkable way of managing national IGF policy. Egypt is a leader in child safety. Latin America has an excellent programme for the coordination of managing Internet names and numbers. India is making breakthrough after breakthrough in bringing Internet to the poorest communities. The list is long. These examples have been presented to the IGF, discussed, and in many cases emulated (e.g. Brazilian national management). The global cause of developing the Internet has been advanced without a global, legally binding arrangement.

Increase policy coherence through multistakeholderism

One of the main challenges for any global policy process today is to achieve policy coherence in dealing with multidisciplinary issues. The IGF serves as an umbrella under which different existing regimes, including information technology, human rights, trade, and intellectual property, can come together. Through the IGF process, various policy communities are discovering that their previously isolated policy areas are indeed part of the broader Internet governance process. In some issue areas, such as multilingualism, the IGF has helped very diverse organisations including governments, ICANN, UNESCO (United Nations Educational, Scientific and Cultural Organization), and ITU to coordinate their focus on the same topic. The unusually broad multistakeholder participation diluted the usual turf battles between various organisations and provided space for linking otherwise diverse initiatives within a coherent policy process. It also reduced the problem of duplication in dealing with policy issues.

Facilitate coordination among national, regional, and global policy levels

In an increasingly integrated world, instant communication and the growing influence of non-state actors blur the line between national, regional, and global policy spaces. Policy issues move quickly between different levels. Some NGOs use 'forum shopping' to insert their policy initiatives at the most favourable policy level. Some governments in the EU, for example, use so-called 'policy laundering': If an initiative is not adopted at national level, it is forwarded through regional level and re-imported as a country's 'international obligation'.

In the Internet governance field, the network of policy forums is complex and existed long before the IGF was created (international organisations, ICANN, ISOC – the Internet Society, and various standardisation bodies). In addition, Internet governance policy actors are very agile, moving easily from one policy layer and forum to another using modern communications technology. The IGF has attempted to maximise the benefits and reduce the risks of multilevel policy processes. It coordinates global, regional, and national activities through both bottom-up (in the preparation of the IGF) and top-down approaches (dissemination of knowledge from the IGF). The IGF's transparency makes the process less open to 'forum shopping'.

Management of policy processes

Efficient and effective leadership: sage on the stage, guide on the side

One of the main reasons for the IGF's success is the leadership of Nitin Desai, Chair, and Markus Kummer, Executive Coordinator of the Secretariat. Both have considerable and complementing diplomatic experience. Desai was in charge of the preparation of several major UN summits; Kummer has had a successful career in the Swiss diplomatic service. While Desai is managing 'the stage' of the IGF's main events, Kummer is building understanding and inclusiveness through timely online, off-stage communication and participation in major events of the various professional communities gathered around the IGF. Their in-depth knowledge of UN rules, procedures, and practice has helped them to find creative solutions and to implement the IGF's effective, although unwritten, *modus operandi*.

Build trust through proper timing and sequencing

The IGF has gathered participants from diverse professional and cultural backgrounds around the same table. They do not have a prior history of

working for the same institutions, attending the same universities, moving in the same social circles, and other ways for building trust. Trust had to be built in an atmosphere where suspicions were already present because of past disputes (e.g. between ITU and ICANN), or to a general feeling of 'geo-suspicion' caused by the Iraq War, or the common labelling of 'us *vs* them'.

Trust-building requires patience and a careful sequencing of activities. Each phase of the IGF process aimed at increasing mutual understanding and bringing new knowledge and information to the table. The result was a gradual building of trust as well as a very informed debate. Some proposals, such as an early call to adopt the Framework Convention on the Internet, were declined: the time was not ripe for further formalisation of the Internet governance field. Five years ago it could have created tension and potentially broken the Internet governance process. Today, there is discussion on the global cybersecurity treaty. Proper time management has been essential for handling the highly controversial question of the central role of ICANN, a US-based institution, in managing Internet names and numbers, the core of the global Internet infrastructure. Five years ago, it was the cause of major controversy. Today, since the US government started the internationalisation of ICANN's role and structure, things are not as controversial as they used to be. It is a good example that policy issues can be ameliorated over time, if handled carefully and not allowed to degenerate into a policy crisis. The IGF has been very successful in this respect. Diplomats and policy-makers can learn from the IGF about effective trust-building through proper timing of activities and careful sequencing. Time is essential, though not sufficient, for trust-building.

See Section 7 for further discussion on ICANN

Let the policy process evolve

In modern society, there is a focus on setting logically consistent schemes and measuring their inputs/outcomes. Global governance and diplomacy are no exceptions to this trend. The 2008 global financial crisis provides an example of how a system, based to a large extent on mathematical modelling, can lead to collapse if it does not consider the complexity of social conditions.

In diplomatic history, the risk associated with over-managing policy processes is well illustrated by the success of the Congress of Vienna (1814) and the failure of the Treaty of Versailles (1919). The Congress of Vienna created the basis for one of the most peaceful periods of European history: almost 100 years without a major war. The Treaty of Versailles, on the other hand,

collapsed only a few years after it was signed. In Vienna, slowly, without a predetermined grand design and with a lot of social interaction, negotiators created an effective peace deal. The diplomatic genius of Metternich and Talleyrand helped achieve this. In Versailles, however, diplomats engaged in an extremely organised process in which hundreds of scientists, statisticians, and cartographers collaborated to create a 'scientifically constructed peace'. They tried to quantify justice, and ultimately created the political conditions that led to the Second World War. The stark differences in the very ways in which negotiations in Vienna and Versailles were managed provide a convincing argument against over-managing diplomatic processes.

While the IGF cannot be compared to these grand diplomatic events, its practice is closer to the approach of the Vienna Congress. The IGF has involved minimum necessary planning and structuring. IGF processes have unfolded and taken optimal shape through the collective moulding of involved participants, including those with opposing views.

Recognise that text remains central to diplomacy

Despite all the promises of virtual conferencing and other technologies, today – even more so than in the past – text remains diplomacy's central tool.[3] Text is central to the IGF process, even though the IGF has not produced any official final document (i.e. convention, treaty, or declaration). Most exchanges between preparatory sessions are done via mailing lists and e-mail. The website is text-intensive, with little use of photos or images. The IGF is supported by very active social media, using text-intensive tools such as blogs and Twitter.

A new relevance of text has emerged through verbatim reporting at IGF meetings, which could have substantive impact on multilateral diplomacy and negotiations. Verbatim reporting is the simultaneous transcription and display of each oral intervention in a meeting as it is presented. Learning from ICANN's practice, the Secretariat of the Working Group on Internet Governance (WGIG) introduced verbatim reporting in April 2005. The IGF continued the practice. All verbal interventions are transcribed simultaneously by special stenographers and immediately displayed on a large screen in the conference room, as well as broadcast via the Internet. While delegates are speaking, transcripts of their speeches appear on the screen.

Verbatim reporting has had an important effect on the diplomatic *modus operandi*. The awareness that what is said will be preserved in print makes many participants more careful in choosing the level and length of their

verbal interventions. Verbatim reporting also increases the transparency of diplomatic meetings.

Recognise that informality in international conferences could cause inequality in participation

One challenge facing the IGF is the juxtaposition of the formal culture of UN diplomacy and the informal culture of the Internet community. After four annual IGF meetings, it seems that the informal culture has prevailed. While this culture creates an inclusive atmosphere and facilitates the participation of youth and wider communities worldwide, it also poses a few challenges. Participants from those national cultures with a strong respect for social hierarchy may feel uncomfortable and hesitant to speak in a very informal working environment. Furthermore, in diplomatic, legal, and some other professional cultures, participation in debates is structured by professional protocols.

Paradoxically, the informality of proceedings and discussion may inhibit the participation of some delegates and create potential inequality. The IGF addressed this risk by seeking ways to accommodate various levels of formality, offering settings where different stakeholders could participate at ease. For example, it increased the level of protocol of some, mainly plenary, sessions, adding more of the typically diplomatic rules of procedure (e.g. speaking slots, formal representation) and organised special sessions for parliamentarians.

Dealing with scientific and technical aspects of policy issues

Acknowledge that science and technology are rarely policy neutral

The IGF process has reconfirmed that science and technology (S&T) issues have implications for policy-making, empowering various groups and interests. At some point, most S&T issues evolve into policy issues; policy issues, in turn, require decisions about values and the interests at stake.

In this context, it is risky to portray S&T issues as policy neutral. If S&T arguments are promoted as the 'ultimate truth', this approach can backfire. For example, in climate change negotiations, such an approach contributed to making scientific arguments extremely vulnerable. E-mails leaked from the University of East Anglia and false data on Himalayan glaciers, cast doubt on – otherwise solid – scientific arguments on climate change.

The question of interplay between science and policy is also important in other policy areas, such as health and food security. Scientists must increase their presence in the diplomatic arena, while diplomats will have to learn how to handle scientific issues.

In the IGF process, S&T contributed to informed policy-making. Technical issues have been discussed in the broader social and economic context. The multistakeholder composition of the IGF, involving scientists, computer specialists, diplomats, economists, and others created an enabling context for an effective interplay between S&T and policy-making.

Improve communication among different professional and organisational cultures

A significant number of books have been written on the subject of cross-cultural communication: how to speak to Arabs, Chinese, American, etc. IGF experience, however, shows that in a policy process, the main challenge is often to facilitate exchange between different professional cultures (e.g. lawyers, engineers) and different organisational cultures (e.g. international organisations, governments, companies). In today's globalised world, with its instant communication, it is often easier to communicate within the same professional circles, even across national borders. Professions share the same way of framing problems and finding solutions. For example, a German computer engineer may find that he or she communicates better with another engineer in China than, say, with a German diplomat.

As global issues become increasingly technical (e.g. climate change, trade, and health), effective interprofessional communication becomes increasingly important. Improvements in interprofessional communication can be achieved through training, education, and exposure to other cultures. Better interprofessional communication may also contribute to better policy coherence among ministries and international organisations. The IGF has made positive steps in interprofessional communication through facilitating the effective exchange of ideas between specialists from a variety of professions, including computer science, diplomacy, and economics. A good example of this is the broad professional and institutional diversity of panellists involved in IGF discussions.

Make the right blend between technical knowledge and diplomatic skills

In most global policy processes, there is a dilemma: should they be managed by specialists (e.g. scientists in climate change) or generalists (diplomats).

The argument for specialists is that in order to address technical issues, one needs in-depth knowledge of those issues. According to this view, for example, scientific background is needed in order to negotiate climate change issues. Diplomats usually deal with political, social, and other non-technical aspects of negotiated issues.

The success of the IGF's leadership – Desai and Kummer – challenged the urban governance myth that technical issues must be managed by technical experts. As newcomers to the Internet governance field, Desai and Kummer provided a non-partisan contribution to a long-standing debate on issues such as the position of ICANN, regulation of domain names, etc. Sometimes, as the IGF shows, the 'diplomatisation' of dealing with technical issues can help overcome traditional disputes in technical communities. The IGF experience confirms that there isn't a ready-made recipe for engaging specialists and generalists. It is a dynamic interplay that depends on specific contexts and individuals involved. The only 'tip' is to develop awareness about the risk of specialists or generalists having an exclusive role.

Increase inclusiveness and participation

Enhance national 'diplomatic footprints' through involvement of non-state actors in diplomatic initiatives[4]

With more players and more complex issues to deal with, the traditional diplomatic approach is limited. Even the most efficient diplomatic services cannot provide as much 'diplomatic bandwidth' (i.e. qualified human resources) as is required. Broader diplomatic bandwidth can be provided by the inclusion of actors from civil society, the business sector, local authorities, and other entities involved in global policy processes.

Some, such as Canada, Switzerland, and the Scandinavian states, recognised this evolution earlier on and have already integrated non-state actors in their foreign policy activities. This practice is not common in many developing countries, where the diplomatic services are small with limited financial and human resources, and where national multistakeholder structures have appeared only during the last few years.

The IGF contributed in a practical way towards raising awareness of the advantages of multistakeholderism in government circles, in particular among developing countries. Apart from the broader principle of inclusiveness, the

IGF's multistakeholderism has demonstrated a practical solution that helps countries to increase their diplomatic footprint without allocating additional resources. Multistakeholder national IGF bodies are appearing. Governments are coordinating more with business and civil society. Some small and developing states are represented in Internet governance policy processes by experts from academia and NGOs.

Sometimes, fostering such inclusiveness is mainly a matter of coordination, and creating a national multistakeholder framework. Dedicated capacity building through training programmes involving various stakeholders from the same state also helps: co-participants in a training programme tend to develop mutual trust and a team spirit.

Strengthen remote participation through the establishment of hubs[5]

It is natural for a forum that discusses Internet governance to use the Internet to extend participation in IGF meetings beyond those who can physically attend. Nowadays, besides regular Internet broadcasting of meetings, the main innovation of the IGF has been the introduction of 'remote hubs'. Remote hubs are defined as local meetings that take place during and parallel to IGF meetings, hosted by universities, information and communication technology (ICT) centres, NGOs, and other players who deal with Internet governance and policy issues. They project a simultaneous webcast of the meeting so that remote participants can stay informed about what is being debated. As part of a remote hub, participants can send text and video questions to be answered by IGF panellists in real-time interventions. In addition, hubs host panels and roundtable discussions correlating to IGF themes from a local perspective. Through these activities, the local hubs enrich coordination between global and local policy processes. For example, during 2008 IGF, the remote hub in Madrid followed the session on cybersecurity and later continued its discussion on cybersecurity in the specific Spanish context. A total of eight remote hubs operated in parallel with the 2008 IGF (Madrid, Lahore, Barcelona, Belgrade, Buenos Aires, São Paulo, Bogota, and Pune). More than 450 event hours were broadcast for remote participation and a total of 522 remote attendees joined the meeting during the four-day event.[6]

After successful test implementation in 2008, the concept of remote hubs was adopted by the IGF Secretariat. As a result of strong support from the host country and Remote Participation Working Groups (RPWG),[7] the IGF in Sharm El Sheikh in 2009 saw an increase in the level of remote participation to 12 hubs from every continent. The remote webcast was greatly improved, and both main sessions and workshops were attended remotely by hubs and

individuals from all over the world. The incorporation of webcast real-time captioning was another improvement that increased access for those with hearing disabilities, as well as compensating for technical (audio) difficulties for those with slow Internet connections.

IGF experience shows that remote participation significantly increases the inclusiveness and openness of international meetings. It creates a direct link between global and local, which is often missing in multilateral diplomacy.

Harvest a variety of inputs through policy's 'long tail'

The concept of policy's 'long tail' is inspired by viral marketing and refers to the possibility of harvesting a wide variety of policy inputs that would normally be lost in traditional intergovernmental processes. Individuals and groups have been able to voice their opinions directly to the IGF through personal involvement in events, web communication, and remote participation. These new ideas and insights, which would not reach the top global forums in most policy processes, have considerably enriched the IGF process. One of the lessons the IGF can convey is that the first step towards a more inclusive policy process is the facilitation of open participation. The full benefit of open and inclusive participation is achieved only if a wide variety of contributions are collected, considered and, whenever possible, included in policy deliberations. Inclusiveness increases the legitimacy of the process and the feeling of ownership among the wide range of stakeholders.

Ensure meaningful participation from developing states: moving from formal to functional equality

In the UN world, small and developing states usually ensure their equal status by insisting on formal representation and procedures. Unlike developed and large states, they lack an organised network of parallel representation of the interests of wider society through business, civil society, and academic communities. It is not surprising, therefore, that they have reservations about multistakeholder participation. In large-scale meetings, which gather thousands of participants on an equal basis, a small and developing state loses the safeguard of the UN procedures where it is one of 194 state representatives with equal formal status, regardless of size or power.

At the beginning of the WSIS process back in 2002, many small and developing states strongly opposed the initiative to introduce equal participation of business and civil society representatives. Some of these states argued for a one-stop-shop approach to Internet governance which would

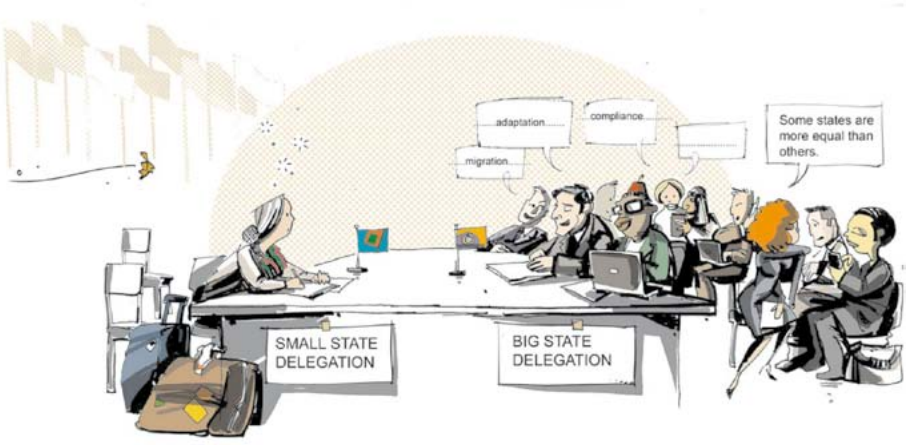
provide them with one, preferably intergovernmental, 'address' where they could discuss all related issues.[8]

Since 2002, WSIS, WGIG, and in particular the IGF have made considerable progress in strengthening pro-development aspects of the multistakeholder process, including addressing the risk of under-representation of small and developing states.

On a formal level, the IGF ensures that all sessions and panels have adequate participation from the various stakeholders in developing states. The increasing level of participation from developing countries was visible at the IGFs in Rio and in Hyderabad.

The IGF process has helped many small and developing states to make better use of available human resources. These may not be diplomats, but other nationals with Internet governance expertise, working at Internet organisations or universities around the world. Taking advantage of experts working abroad is essential, especially for small states.

Physical participation – i.e. attending the meetings – does not necessarily equate to equal participation. Equal participation requires adequate knowledge, skills, and confidence on the part of each delegate to engage in the policy process. The IGF has tried to ensure equal participation through capacity-building activities. Since 2002, more than 850 officials and professionals from small and developing states have been involved in training and other capacity-building activities that go beyond traditional academic



Formal vs functional equality in climate change negotiations

courses by providing a unique blend of teaching, policy research, and policy immersion aimed at helping participants understand the dynamics of the IGF and gain the necessary confidence for full and meaningful participation in policy processes. The involvement of various stakeholders (diplomats, officials, engineers) in the training process provides participants with an understanding of the advantages of a multistakeholder approach and gives them the confidence to participate in meetings with other professional communities.

The IGF process has also fostered the development of Internet governance communities of practice in the global south on both regional (e.g. West Africa, East Africa, and Latin America) and national levels (e.g. Kenya, Brazil, Senegal). These communities have helped many small and developing states to develop their own multistakeholder representation by identifying non-governmental experts already involved in academic research and the Internet governance policy process.

At the IGF, by increasing participation levels, encouraging capacity building, and fostering the development of networks and communities, many developing countries have evolved from formal/passive to functional/active participation in Internet governance.

Endnotes

1 Norwegian Minister of Foreign Affairs, Johan Gahre Store, strongly criticises the lack of G20 legitimacy in his article *One of the greatest setbacks since World War II*. Available at: **http://www.spiegel.de/international/europe/0,1518,702104,00.html**

2 Compromise was achieved between two policy approaches. The government-centered approach, promoted predominantly by developing countries, argued that the Internet should be governed by international organisations, such as ITU. The non-governmental approach, favoured by developed countries and in particular the USA, argued for Internet governance with high involvement of the business sector and civil society. They opposed the exclusive role of organisations, such as ITU. Each side got something in the creation of the IGF as a compromise solution. The government-centered approach got anchoring of the IGF in the international organisation system. The IGF is conveyed by the UN Secretary General. The non-governmental approach got the multistakeholder nature of the IGF with involvement of the business sector and civil society. Some consider that in this compromise they also gained by linking the IGF to the UN Secretary General in order to prevent a more prominent role of ITU in Internet governance.

3 An interesting parallel is the use of SMS services on mobile phones, through which text remains essential in human communication in spite of powerful voice and video-based tools.

4 Multistakeholderism is best conceptualised as an approach to governance, described as: *The sum of the many ways individuals and institutions, public and private, manage their common affairs. It is a continuing process through which conflicting or diverse interests may be accommodated and cooperative action may be taken. It includes formal institutions and regimes empowered to enforce compliance, as well as informal arrangements that people and institutions either have agreed to or perceive to be in their interest* (Commission on Global Governance, 1995).

5 See **www.igfremote.com** for a meaningful and substantive comments provided by Ginger Paque and Marilia Marcel, who are also the driving force behind the RPWG.

6 A detailed report on remote participation at IGF 2008 is available at: **http://www.igfremote.com/ReportRPIGF-final.pdf**

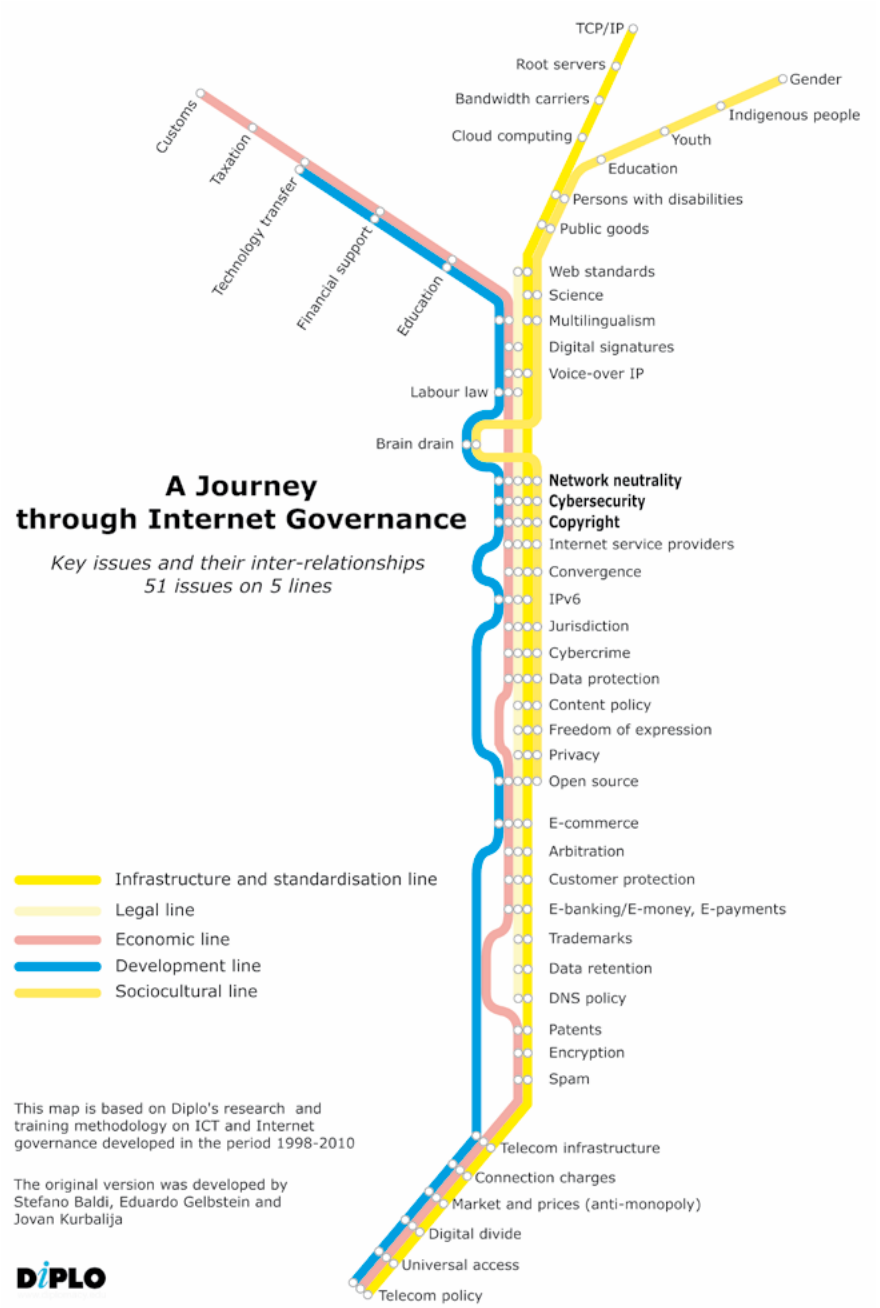
7 **http://www.igfremote.info**

8 Preliminary surveys show that 80–100 international organisations, standardisation bodies, forums, and other entities cover different aspects of Internet governance. Even for large, developed states, this wide field is almost impossible to cover. The IGF has tried to reduce and harness complexity by distilling Internet-governance-related aspects from other policy processes (privacy, intellectual property, human rights, development, e-commerce, etc.).

Section 9

Annex

Annex


A Journey
through Internet Governance
Key issues and their inter-relationships
51 issues on 5 lines
Infrastructure and standardisation line
Legal line
Economic line
Development line
Sociocultural line
This map is based on Diplo's research and training methodology on ICT and Internet governance developed in the period 1998-2010
The original version was developed by Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija
DiPLO
TCP/IP
Root servers
Bandwidth carriers
Cloud computing
Gender
Indigenous people
Youth
Education
Persons with disabilities
Public goods
Customs
Taxation
Technology transfer
Financial support
Education
Web standards
Science
Multilingualism
Digital signatures
Voice-over IP
Labour law
Brain drain
Network neutrality
Cybersecurity
Copyright
Internet service providers
Convergence
IPv6
Jurisdiction
Cybercrime
Data protection
Content policy
Freedom of expression
Privacy
Open source
E-commerce
Arbitration
Customer protection
E-banking/E-money, E-payments
Trademarks
Data retention
DNS policy
Patents
Encryption
Spam
Telecom infrastructure
Connection charges
Market and prices (anti-monopoly)
Digital divide
Universal access
Telecom policy

The Internet governance cube

The WHAT axis is related to the ISSUES of Internet governance (e.g. infrastructure, copyright, privacy). It conveys the **multidisciplinary** aspect of this approach.

The WHO axis of the cube focuses on the main ACTORS (states, international organisations, civil society, the private sector). This is the **multistakeholder** side.

The WHERE axis of the cube deals with the FRAMEWORK in which Internet issues should be addressed (self-regulatory, local, national, regional, and global). This is a **multilayered** approach to Internet governance.

When we move pieces in the IG cube we get the intersection – HOW. This is the section of the cube that can help us to see how particular issues should be regulated, both in terms of cognitive, legal techniques (e.g. analogies) and in terms of instruments (e.g. soft law, treaties, and declarations). For example, one specific intersection can help us to see HOW privacy issues (what) should be addressed by civil society (who) at a national level (where).

Separate from the Internet governance Cube is a fifth component – WHEN

A survey of the evolution of Internet governance

Actor / Period	United States	Internet Guardians	International Organisations	Private Sector	Countries	Civil Society
	The Department of Defence (DoD) runs the Domain Name System (DNS)					
1986	The National Science Foundation (NSF) takes over from the DoD					
1994				Network Solutions Inc (NSI) signs a contract with NSF to manage DNS for the period 1994–1998		

The start of the DNS war
After NSF outsources the management of DNS to NSI (a private company), the Internet community (mainly ISOC – the Internet Society) tries for many years to return DNS management to the public domain. It succeeds after four years. This process involved a number of diplomatic techniques, such as: negotiation, coalition building, leverage use, consensus building, etc.

June 1996		Internet Assigned Numbers Authority (IANA)/ISOC plan to take over from NSI once its contract ends; additional domains are introduced; the trademark sector presents strong opposition to new top-level domains, as does ITU (International Telecommunication Union)				
Spring 1997		An IAHC (International Ad Hoc Committee) proposal. Participants in the IAHC: two representatives from the trademark interest groups, World Intellectual Property Organization (WIPO), ITU and NSF; and five representatives from the Internet Engineering Task Force (IETF). Conclusion of the generic top-level domain (gTLD) Memorandum of Understanding (MoU) specifying DNS as a 'public resource'; seven new domains; and strong protection for trademarks. Establishment of CORE (Council of Registers – signing ceremony in March 1997 at ITU, Geneva); CORE collapsed immediately. Strong opposition from the US government, NSI, and the EU.				

Actor / Period	United States	Internet Guardians	International Organisations	Private Sector	Countries	Civil Society
1997	US government transfers management of DNS to the Department of Commerce (DOC)					
June 1998	A DOC White Paper invites the main players to propose solutions of their own	Proposals are received from: IFWP (International Forum on the White Paper), ORSC (Open Root Server Confederation), and BWG (Boston Working Group) Instead of drafting a new paper, ISOC focuses on: • Building a broad coalition involving international organisations (from the IAHC initiative), the private sector (IBM) and key countries (Japan, Australia) and the EU. • Creating a new organisation.				
Second part of 1998		September 1998 – An ISOC-NSI Joint Draft Agreement October 1998 – ISOC abandons agreements and creates ICANN (Internet Corporation for Assigned Names and Numbers)				
15 Nov 1998	DOC transfers authority to ICANN	ICANN acquires two new crucial functions: 1 Authority to accredit registers for the gTLD. 2 Management of the authoritative role (the policy aspect is kept with the DOC).				
April 1999		A DOC – ICANN – NSI agreement and introduction of a shared registry system; NSI loses its monopoly but obtains a favourable transition arrangement (management of four domains, etc.)				
THE STRUCTURE AND FUNCTIONING OF ICANN						
June 1998		Formation of the PSO (Protocol Supporting Organisation) consisting of the IETF, the W3C (World Wide Web Consortium) and other Internet pioneers	Initialisation of the WIPO Internet Domain Name Process	ASO (Address Support Organisation) created to represent the association of DNS registries (ARN, RIPE, NCC). DNSO (Domain Name Supporting Organisation) established to protect trademark and commercial interests.	Thirty countries establish a Governmental Advisory Committee (GAC) in order to gain more influence in managing national domains. ICANN reacts by establishing the DNSO subcommittee – ccTLDs	

The end of the DNS war
The war ended through compromise. ISOC managed to get more public control of DNS management although commercial interests remained very strong. Thus the interests of both private business and the guardian communities were properly protected. This was not the case with the position of national states and the general Internet community. These are the two weakest aspects of ICANN governance.

Actor / Period	United States	Internet Guardians	International Organisations	Private Sector	Countries	Civil Society
2000–2003			Emergence of a greater focus on the Internet in ITU, WIPO, UNESCO (UN Educational, Scientific, and Cultural Organization), the OECD, the Council of Europe, and the World Bank	Strong push by the private sector for a regulated Internet (copyright laws, e-commerce, etc.)	Development of Internet legislation, court cases, etc.	NGO involvement in the digital divide, human rights, gender issues on the Internet
			Multisectoral and global initiatives focusing on Internet development, governance, etc.: G8 DOT Force, World Economic Forum, UN ICT Task Force, World Summit on the Information Society (WSIS), Global Knowledge Partnership			
June 2002 – Nov 2003	The first PrepComm for WSIS was held in June 2002; Internet governance emerged as an issue during the Regional PrepComm for West Asia in Beirut (February, 2003). At the first summit event in Geneva (2003) the decision was made to establish the Working Group on Internet Governance (WGIG). Multisectoral and global initiatives focusing on Internet development, governance, etc.: G8 Dot Force, World Economic Forum, UN ICT Task Force.					
2004–2005	The Working Group on Internet Governance (WGIG) shaped discussion on Internet governance in this period. WGIG was a multistakeholder body consisting of representatives of governments, the business community, and civil society. WGIG held four preparatory meetings and produced the Report which was the basis for the decision on Internet governance at WSIS – Tunisia (2005). In Tunisia, the Tunis IG Compromise introduced the Internet Governance Forum (IGF) a compromise between those who opposed any change in the ICANN-centred regime and those who argued that the Internet should be governed through an intergovernmental regime.					
2006–2009	Following the conclusion of WSIS-Tunis (2005), the IGF was established in order to continue the policy process on Internet governance. So far four IGFs have been held: Athens (2006), Rio de Janeiro (2007), Hyderabad (2008) and Sharm el Sheikh (2009). On 30 September 2009, the US government and ICANN signed the Affirmation of Commitments which ended US supervision of ICANN, one of the most controversial issues of Internet governance. ICANN entered a new phase as an independent organisation with more questions than answers about its future position and role.					
2010	The fifth IGF will be held in Vilnius (Lithuania). Based on the review of the first five years, the United Nations will make the decision in the autumn 2010 about the future of the IGF.					

The **African, Caribbean and Pacific Group of States (ACP)** is composed of signatories to the Georgetown Agreement between the ACP and the European Union, officially called the EU ACP Partnership Agreement or the Cotonou Agreement.

The ACP Group of States consists of 79 Member-States, of which 48 are from Sub-Saharan Africa, 16 from the Caribbean, and 15 from the Pacific. The Group was originally created with the aim of coordinating cooperation between its members and the EU focusing on negotiating and implementing cooperation agreements with the European Community. Over the years, the ACP Group of States has extended its range of activities beyond development cooperation with the EU and now covers other issues such as trade, economics, and culture, in diverse international forums such as the World Trade Organization (WTO).

The main objectives of the ACP Group of States:

- Promote sustainable development of its Member-States and their gradual integration into the global economy, which entails making poverty reduction a matter of priority and establishing a new, fairer, and more equitable world order.
- Coordinate the activities of ACP States in the framework of the EU ACP Partnership Agreement.
- Foster and strengthen solidarity among ACP States, and understanding between ACP peoples and governments.

DiPLO
www.diplomacy.edu

DiploFoundation is a non-profit organisation which works to strengthen the meaningful participation of all stakeholders in diplomatic practice and international relations. Our activities revolve around, and feed into, our focus on education, training and capacity building:

- **Courses:** We offer postgraduate-level academic courses and training workshops on a variety of diplomacy-related topics for diplomats, civil servants, staff of international organisations and NGOs, and students of international relations. Our courses are delivered through online and blended learning.
- **Capacity building:** With the support of donor and partner agencies, we offer capacity-building programmes for participants from developing

countries in a number of topics including Internet Governance, Human Rights, Public Diplomacy and Advocacy, and Health Diplomacy.

- **Research:** Through our research and conferences, we investigate topics related to diplomacy, international relations, and online learning.
- **Publications:** Our publications range from examination of contemporary developments in diplomacy to new analyses of traditional aspects of diplomacy.
- **Software development:** We have created a set of software applications custom designed for diplomats and others who work in international relations. We also excel in the development of online learning platforms.

Diplo is based in Malta, with offices in Geneva and Belgrade. Diplo emerged from a project to introduce information and communication technology (ICT) tools to the practice of diplomacy, initiated in 1993 at the Mediterranean Academy of Diplomatic Studies in Malta. In November 2002, Diplo was established as an independent non-profit foundation by the governments of Malta and Switzerland. Our focus has expanded from the application of information technology to diplomacy, to include other new and traditional aspects of the teaching and practice of diplomacy and international relations.

The **European Union's European Development Fund (EDF)** is the main funding instrument in the framework of the Cotonou Agreement (EU ACP Partnership Agreement) for providing the European Community's aid for development cooperation with the African, Caribbean, and Pacific Group of States (ACP) and Overseas Countries and Territories (OCT). One of the objectives of the EDF is to promote the economic, cultural, and social development of the ACP states.

About the author

Jovan Kurbalija is the founding director of DiploFoundation. He is a former diplomat with a professional and academic background in international law, diplomacy, and information technology. In 1992, he established the Unit for Information Technology and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of training, research, and publishing, in 2002 the Unit evolved into DiploFoundation.

Since 1994, Dr Kurbalija has been teaching courses on the impact of ICT/Internet on diplomacy and ICT/Internet governance. He has lectured at the Mediterranean Academy of Diplomatic Studies in Malta, the Vienna Diplomatic Academy, the Dutch Institute of International Relations (Clingendael), the Graduate Institute of International and Development Studies in Geneva, the UN Staff College, and the University of Southern California. He conceptualised and currently directs DiploFoundation's Internet Governance Capacity Building Programme (2005–2010).
Dr Kurbalija's main research interests include the development of an international regime for the Internet, the use of the Internet in diplomacy and modern negotiations, and the impact of the Internet on modern international relations.

Dr Kurbalija has published and edited numerous books, articles, and chapters, including: *The Internet Guide for Diplomats, Knowledge and Diplomacy, The Influence of IT on Diplomatic Practice, Information Technology and the Diplomatic Services of Developing Countries, Modern Diplomacy* and *Language and Diplomacy.* With Stefano Baldi and Eduardo Gelbstein, he co-authored the *Information Society Library,* a set of eight booklets covering a wide range of Internet-related developments.

jovank@diplomacy.edu

For easy reference: a list of frequently used abbreviations

APEC	Asia-Pacific Economic Co-operation
ccTLD	country code Top-Level Domain
CIDR	Classless Inter-Domain Routing
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DRM	Digital Rights Management
GAC	Governmental Advisory Committee
gTLD	generic Top-Level Domain
HTML	HyperText Markup Language
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
aICT	Information and Communications Technology
IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
IPR	Intellectual Property Rights
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXP	Internet eXchange Point
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infrastructure
S&T	Science and Technology
SGML	Standard Generalized Markup Language
sTLD	sponsored Top-Level Domain
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLD	Top-Level Domain
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UNECOSOC	United Nations Economic and Social Council
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	United Nations Educational, Scientific and Cultural Organization
VoIP	Voice-over Internet Protocol
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
XML	eXtensible Markup Language

An Introduction to Internet Governance provides a comprehensive overview of the main issues and actors in this field. The book is written in a clear and accessible way, supplemented with numerous figures and illustrations. It focuses on technical, legal, economic, development, and sociocultural aspects of Internet governance, providing a brief introduction, a summary of major questions and controversies, and a survey of different views and approaches for each issue. The book offers a practical framework for analysis and discussion on Internet governance.

Since 1997 more than 1000 diplomats, computer specialists, civil society activists and academics have attended training courses based on the text and approach presented in this book. With every delivery of the course, materials are updated and improved. This regular updating makes the book particularly useful as a teaching resource for introductory studies in Internet governance.

DiPLO
www.diplomacy.edu

9 789993 253235