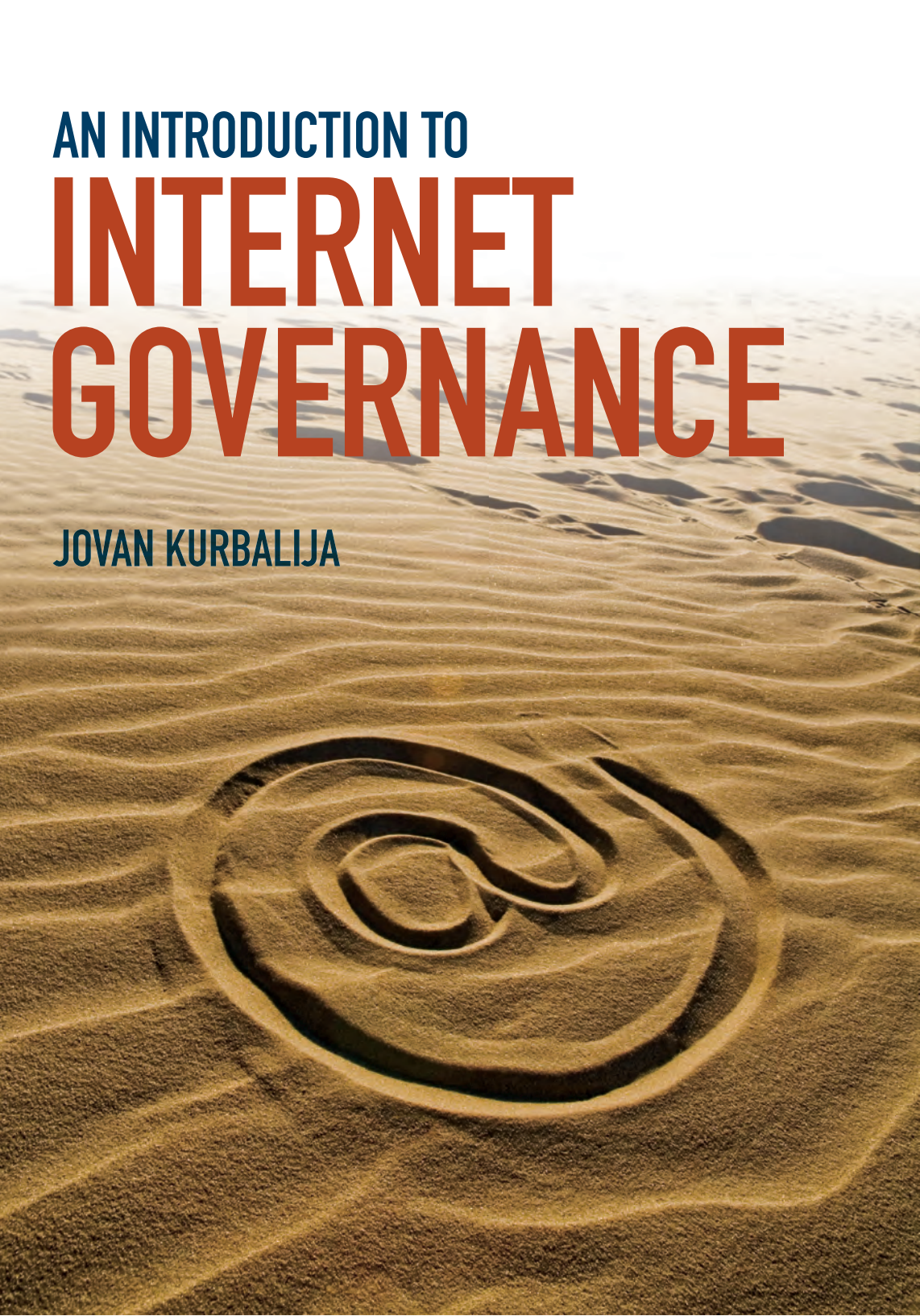
AN INTRODUCTION TO INTERNET GOVERNANCE

JOVAN KURBALIJA



PREFACE

The history of this book is long, in Internet time. The original texts and the overall approach, including the five-basket methodology, were developed in 1997 for a training course on Information and Communications Technology Policy for Commonwealth state officials. Since 1997, through subsequent courses and online programmes, Diplo has trained close to 600 diplomats, computer specialists, civil society activists and academics in the field of ICT/Internet Governance. With every delivery of the course, materials were updated and improved.

In 2004, for the first time, Diplo published a print version of its materials on Internet Governance, in a booklet entitled "Internet Governance – Issues, Actors and Divides." This booklet formed part of the Information Society Library, and was co-authored by Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija. Special thanks are due to Eduardo Gelbstein, who made substantive contributions in the sections dealing with cybersecurity, spam and privacy, and to Vladimir Radunovic and Ginger Paque who updated the course materials. Comments and suggestions of 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 version of the booklet was published in cooperation with NIXI-India on the occasion of the Internet Governance Forum 2008 held in Hyderabad, India.

This booklet has been prepared for the IGF 2009 (Sharm El Sheik, Egypt) in partnership with the Ministry of Telecommunication of Egypt and the Commonwealth Internet Governance Forum.

ISBN: 978-99932-53-22-8

DiploFoundation

Malta: 4th Floor, Regional Building
Regional Rd.
Msida, MSD 2033, Malta

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

E-mail: diplo@diplomacy.edu
Website: http://www.diplomacy.edu

Edited by Steven Slavik and Ginger Paque
Illustrations: Zoran Marcetic – Marča & Vladimir Veljašević
Cover: Rudolf Tusek
Layout & Prepress: Aleksandar Nedeljkov

© Copyright 2009, DiploFoundation

Any reference to a particular product in this booklet serves merely as an example and should not be considered an endorsement or recommendation of the product itself.

CONTENTS

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 Internet has, in a relatively short period, become an essential instrument of today's society. As of the end of 2009, the Internet is considered to include:

- an estimated 1.5 billion users worldwide;
- a major social impact on education, health, government, and other areas of activity;
- cybercrime, such as fraud, illegal gambling and ID theft;
- misuse and abuse in the form of malicious code and spam.

The growing awareness of the social, economic, and political impact of the Internet on society has brought the question of Internet governance into sharper focus. In the case of the Internet, governance is needed, among other things, to:

- prevent or, at least minimise, the risk of the fragmentation of the Internet;
- maintain compatibility and interoperability;
- safeguard the rights and define the responsibilities of the various players;
- protect end users from misuse and abuse;
- protect the public interest at the national and the global levels;
- encourage further development.

The Internet and statistics have not been easy companions. Since the earliest days of the Internet, identifying the exact numbers of users, website hosts, traffic volume, and precise financial information, to name but a few, has been difficult. In addition, numbers have often been used to hype the growth of the Internet, making them even less believable.[1]

The process of addressing the legal issues and social consequences of technological developments invariably lags behind technological innovation. This applies to the Internet, too. International negotiations on Internet governance have by now gone through a few important stages but are still very far from completion or even from a universal agreement on what Internet governance should look like. Who are the actors likely to influence the Internet's future development? What will their policies be with regard to connectivity, commerce, content, funding, security, and other issues central to Internet development? These are just some of the key questions that need to be addressed within the framework of Internet governance.

WHAT DOES INTERNET GOVERNANCE MEAN?

The controversy surrounding Internet governance starts with its definition. It is 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 the technical infrastructure. Computer specialists focus on the development of different standards and applications, such as XML or Java. Communication specialists stress the facilitation of communication. Human rights activists view Internet governance from the perspective of the freedom of expression, privacy, and other basic human rights. Lawyers concentrate on jurisdiction and dispute resolution. Politicians worldwide usually focus on media and issues that play well with their electorates, such as techno-optimism (more computers = more education) and threats (Internet security, protection of children). Diplomats are mainly concerned with the process and protection of national interests. The list of potentially conflicting professional perspectives on Internet governance goes on.

WSIS 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] The working definition is a good starting point for the debate on Internet governance. However, it did not clarify the question of different interpretations of two key terms "Internet" and "governance".

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 Communications Technology" are usually put forward as more comprehensive. They include areas that are outside of 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 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.

"I"nternet or "i"nternet and Diplomatic Signaling

Back in 2003, "The Economist" started writing Internet in lowercase. This editorial policy change was inspired by the fact that the Internet became an everyday item, no longer unique and special enough to warrant capitalization. The word Internet followed the linguistic destiny of (t)elegraph, (t)elephone, (r)adio and (t)elevison, among other inventions.

The question of writing Internet/internet with an upper or lowercase "i" re-emerged at the ITU Conference held in Antalya (November, 2006) – where a political dimension emerged 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 the ITU. Some interpreted it as a diplomatic signal of the ITU's intention to play a more prominent role in Internet governance.[3]

Governance

In the Internet governance debate, especially in the early phase of the WSIS-2003, controversy arose over the term "governance" and it's 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 the 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 by 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 Defence Advanced Research Project Network (DARPA Net), a resilient communication resource. By the mid-1970s, with the invention of TCP/IP protocol, this network evolved in what is known today as the Internet. One of the key principles of the Internet is its distributed nature: data packages 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 at 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 were no central government, no central planning, and no grand design.

This led many people into thinking that the Internet was somehow unique and that it could bring an alternative to the politics of the modern world. In his famous Declaration of the Independence of Cyberspace, John Perry Barlow addressed states thusly, "[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."

Prefixes: "e-" – "virtual" – "cyber" – "digital"

The prefixes "e-,", "cyber," "virtual" and "digital" are used to describe various ICT/Internet developments. Their use originates in the 1990s and implied different social, economic, and political influences in the development of the Internet. For example, academics and Internet pioneers used both "cyber-" and "virtual" to highlight the novelty of the Internet and the emergence of a "brave, new world." The prefix "e-" is usually associated with e-commerce and the commercialisation of the Internet in the late 1990s. "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 (Council of Europe, 2001). More recently, it has been used to describe cybersecurity issues. The ITU named its initiative in this field the "Global Cybesecurity 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. In the WSIS, "e-" was introduced at the Pan-European Bucharest Regional Meeting and became predominant in all WSIS texts, including the final documents. The WSIS implementation is centred on action lines including e-government, e-business, e-learning, e-health, e-employment, e-agriculture and e-science.

"DNS War" (1994-1998)

A detailed survey of the evolution of Internet governance is available on pp 187-189.

However, this decentralised approach to Internet governance soon began to change as governments and the business sector realised the importance of the global 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 "DNS War."

This "DNS 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.

WSIS (2003-2005)

The World Summit on the Information Society (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 being put forward by participants. In fact, during the first preparatory and regional meetings even the term "Internet," let alone "Internet governance," was not used.[5] Internet governance was introduced to the WSIS process during the West Asia regional meeting in January 2005 and 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). The 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 IG issues, and establishing the Internet governance Forum. The Forum, which held its first meeting in October 2006 in Athens and its second meeting in Rio de Janeiro in November 2007, provides a new way for discussing Internet governance issues. It is a multistakeholder body, convoked by the UN Secretary General. The forum's mandate will be revisited after five years.

Developments in 2006

After the Tunis Summit, which took place in November 2005, 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, the new MoU only made the umbilical cord between ICANN and the US government "thinner" but maintains the prospect of the eventual internationalisation of the status of ICANN.

The second event of 2006 was the Internet governance Forum 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. The Forum 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 2006. 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 in 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. Interventions by the US 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 2007 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 IG as well as other policy spheres, was the election of Barack Obama as the US President. During his presidential election campaign he used the Internet and Web 2.0 tools intensively. Some even argue that one of the reasons for his successful election was the use of the Internet. Among his advisors one can find many people from the Internet industry, including the CEO of Google. In addition to his techno-awareness, President Obama will promote multilateralism which will inevitably influence discussion on the internationalisation of ICANN and the development of the Internet governance regime.

In 2008, net neutrality emerged as one of the most important IG issues. It was mainly discussed in the United States between two main opposing blocks. The issue of net neutrality even featured in the US presidential campaign, with President Obama supporting net neutrality. Net 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 net neutrality might endanger their business. On the other side there are telecommunication companies, such as Verizon and AT&T, Internet service providers and the multimedia industry. For different reasons, these industries would like to see some sort of differentiation of packets travelling on the Internet.

Another major development was fast growth of Facebook and social networking. When it comes to Internet governance, the increased use of Web 2.0 tools opened 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 US President Obama's Internet-related policy. Obama's appointments to key Internet-related positions did not bring any major surprises. They follow Obama's support for an open Internet. His team also pushed for the implementation of the principle of net neutrality in accordance with promises made during his election campaign.

The highlight of 2009 has been the conclusion of the "Affirmation Commitments" between ICANN and the US Department of Commerce,

which should make ICANN a more independent organisation. While this move solves one problem in IG – the US supervisory role over ICANN – it opens 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 4th IGF will be held in Sharm el Sheik, Egypt. The Sharm discussion will be coloured by the "Affirmation of Commitments" as well as two important developments coming in 2010: a decision on the future of the IGF after 2011 and the next ITU Plenipotentiary Conference in Mexico. While 2009 was mainly dominated by developments in the USA after the election of Barack Obama, it is very likely that in 2010 the focus will shift to the international aspects of the Internet governance debate (international positioning of ICANN, future of IGF, ITU's strategic orientation).

THE INTERNET GOVERNANCE COGNITIVE TOOLKIT

The IG Cognitive Toolkit is a set of tools for developing policy and preparing policy argumentation. It has numerous practical functions for anyone involved in Internet governance. First, the Toolkit should help navigate the vast amount of information, documents and studies generated around the Internet governance process. Second, it can help in developing policy narrative and understanding the policy statements of others. Ultimately, the Toolkit should improve the quality of negotiations by increasing chances for compromises which are above the level of the "least common denominator".

The IG Cognitive Toolkit is part of the growing Internet governance regime which is in the very early stages of 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. The reference framework is highly relevant in political life. It shapes how we see particular issues and what actions we take.

In many cases, the common framework is influenced by the specific professional culture (the patterns of knowledge and behaviour shared

by members of the same profession). The establishment of a common framework usually helps in facilitating better communication and understanding. However, it is sometimes also used to protect one's "turf" and prevent outside influence. To quote the American linguist, Jeffrey Mirel, "All professional language is turf language."

Any Internet governance regime is complex as it will need to involve many issues, actors, mechanisms, procedures, and instruments.

The following illustration, inspired by the Dutch artist M.C. Escher, demonstrates some of the paradoxical perspectives associated with Internet governance.

The IG Cognitive Toolkit reflects the specificity of IG, as a so-called wicked policy problem. IG issues usually have a broad range of catalysts, making it difficult to assign causation to one specific reason. In many cases every problem is a symptom of another one, sometimes creating vicious circles of policy. Certain cognitive approaches such as linear, mono-causal and "either/or" thinking have a very limited utility in the field of Internet Governance. IG negotiations involve almost continuous balancing acts between different interests and approaches.

The IG Cognitive Toolkit contains a wide variety of tools. Some are used in addressing deeper policy controversies (narrow vs. broad approach to IG) while others are used as rhetorical devices for argumentation and building policy narrative (do not fix it if it is not broken).

An attempt to organise such tools, under the name "Internet governance Toolkit" would include:

- approaches and patterns;
- guiding principles;
- analogies.

Like the process of Internet governance, the toolkit is 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 system of references.

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 Internet governance process.

The "narrow" approach focuses on the Internet infrastructure (Domain Name System, IP numbers and root servers) and on ICANN's position as the key actor in this field. Whilst according to the "broad" approach, Internet governance negotiations should go beyond infrastructural points and address other legal, economic, developmental and socio-cultural issues. This latter approach is adopted in the WGIG Report and the WSIS concluding document. It is also used as the underlying principle of the Internet Governance Forum 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. The discussions at the Internet Governance Forum in Rio de Janeiro (November 2007) clearly highlight that the broad approach does not mean that discourse should be vague. The return of the question of core Internet resources (so called "ICANN issues") in the Forum agenda illustrates that the importance of the issues from the narrow approach will also remain.

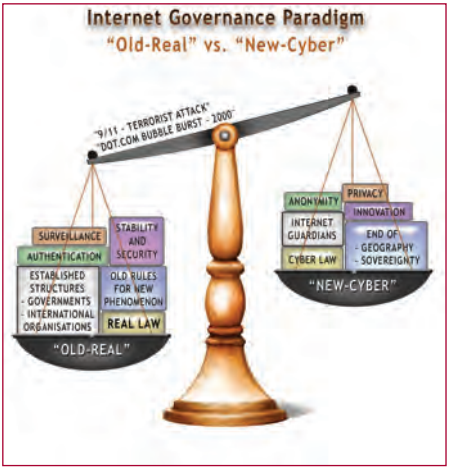
Technical & Policy Coherence

A significant challenge of 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 Internet Governance Forum debate.

"Old-Real" vs. "New-Cyber" Approach

There are two approaches to almost every Internet governance issue. The "old-real" approach – or "new wine in old bottles" – argues that the Internet has not introduced anything new to the field of governance. The Internet is just another new device, from the governance perspective, no different from its predecessors: the telegraph, the telephone, or 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 and "e-" commerce. Consequently there is no need for special legal treatment of "e-commerce."

The "new-cyber" approach – or "new wine in new bottles" – 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 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.

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 that 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, 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 enabled its rapid growth, and also fostered creativity and inclusiveness. How to protect the public nature of the Internet will remain one of the core issues of the IG 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 net 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," that governments had "no moral right to rule us [users]" nor "any methods of enforcement we have true reason to fear."

However, technological developments of the recent past, 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 Internet service provider (ISP) the Internet was accessed.

The more the Internet is anchored in geography, the less unique its governance will be. For example, with the possibility to geographically locate 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 affected the Internet governance agenda. For example, in 2002 when the WSIS process started, 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. Presently, 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 net neutrality, the convergence of different technologies (e.g., telephony, TV, and the Internet), and governances issues regarding social networking (Facebook and MySpace) as well as the role of Google and Wikipedia as "gate-keepers" to digitalised knowledge and information.

Policy Balancing Acts

Balance would be probably the most appropriate graphical illustration of Internet governance and policy debates. On many IG issues a balance has to be established between various interests and approaches. Establishing the balance is very often the basis for a compromise. There are a few areas of policy balancing, including:

- freedom of expression vs. protection of public order; the well-known debate between Article 19 (freedom of expression) and article 27 (protection of public order) of the Universal Declaration on Human Rights has been extended to the Internet. It is very often discussed in the context of content control and censorship on the Internet.
- 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 balance, depending on the overall global political situation. After 09/11 with the "securitisation" of the global agenda, the balance shifted towards cybersecurity.
- Intellectual property: protection of authors' rights vs. fair use of materials; another "real" law dilemma which took on a new perspective in the online world.

Balancing Act in History

Back in 1875, the International Telegraph Union (predecessor of the ITU) held a Conference in St. Petesburg, 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 the 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.

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

"Do not 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:

- those invented for the Internet (e.g. ICANN);
- those that require considerable adjustment in order to address Internet-related issues (e.g. trademark protection, e-taxation);
- 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 Internet protocols.

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).

"Not Seeing the Wood for the Trees"

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. The 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 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.). However, one can also envisage many shortcomings of this principle, especially in cases of transition from existing telecommunication regulations to new ones.

The Principle of Net Neutrality

Net neutrality is one of the Internet's core principles, enabling data transfer between Internet end points (users and services) without any discrimination. This principle is often quoted as the primary reason behind the rapid development of the Internet. Inventors of Google, Skype and Wikipedia, to name a few, had only to observe a few Internet-protocols to make their ideas reality. They did not need any permission or authorisation for using their inventions to create an Internet business.

Discussions around net neutrality have resulted from the high commercial potential of Internet services. Different actors, for various reasons, argue that some Internet traffic should be treated differently. The introduction of new and faster Internet services for multimedia and video content is one of the main commercial growth areas. The provision of such services requires the development of a new Internet layer, sometimes described as a "VIP Internet." The main proponents of this development, which may challenge the principle of net neutrality, are the major telecommunication companies, such as Verizon, AT&T, Comcast, the entertainment industry, and equipment providers.

Net neutrality has been strongly supported by Internet business sectors, including major companies such as Google, eBay, Yahoo, and Amazon; consumer rights associations; and civil society. Net neutrality has already been subject to debate in high political bodies, such as the US Congress, and the preservation of net neutrality is one of the first principles of the technology agenda of president-elect Barack Obama.

Make Tacit Technical Solutions Explicit Policy Principles

It is a common view within the Internet Community that certain social values, such as free communication, are facilitated by the way in which the Internet is technically designed. For instance, the principle of network neutrality, accord-

ing 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 wrong 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 the policy level, not tacitly presumed at the technical level. The technical 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*

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.

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 (see analogy to telephony), web services (see analogy to broadcasting services – television), and databases (see analogy to library). 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 Voice over IP it is increasingly difficult to make a clear distinction between the Internet and telephony.

In spite of these limiting factors, analogies are still powerful, and are still the main cognitive tool for solving legal cases and developing an Internet governance regime. Some of the most frequently used analogies are discussed below.

Internet – Telephony

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

A more recent analogy between the telephone and the Internet focusses on the possible use of the telephony numbering system as a solution for the organisation of the domain name system.

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.

Used by: Those who oppose the regulation of Internet content (mainly in the United States). If the Internet was analogous to the telephone, the content of Internet communication could not be controlled, as is the case with the telephone.

This analogy 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 the ITU.[6]

Internet – Mail/Post

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

Paul Twomy, former Chairman 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 focussing on just ensuring that the address works."

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 of mail than the e-mail system, where the active intermediary function is performed by the 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 wish 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 – "huge digital library," "cyber-library," "Alexandrian Library of the 21st 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:

a) traditional libraries aim to serve individuals living in a particular place (city, country, etc.), while the Internet is global;
b) books, articles, and journals are published using procedures to ensure quality (editors). The Internet does not always have editors;
c) libraries are organised according to specific classification schemes, allowing users to locate the books in their collections. Apart from a few directories, such as Yahoo! and Google, which cover only a small part of the information available throughout the Internet, no such classification scheme exists for the Internet;
d) apart from keyword descriptions, the contents of a library (text in books and articles) are not accessible until the user borrows a particular book. The content of the Internet is immediately accessible via search engines.

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 focusses 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 copyrights (developing software for breaking copyright protection, etc.). The counterargument in such cases was that software developers, like VCR and photocopy machine manufacturers, cannot predict whether their products will be used illegally. This analogy was used in cases against the developers of Napster-style software for peer-to-peer sharing of files, such as Grokster and StreamCast.

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."[7]

Internet – Highway

Similarities: This analogy is linked to the American'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-90s, after Al Gore introduced 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."

Internet – High Sea

Similarities: Initially, this analogy was driven by the fact that like high sea, 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 transporting 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 Organisation 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 sea. 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* on the Internet as it is used for regulating the high seas.

THE CLASSIFICATION OF INTERNET GOVERNANCE ISSUES

Internet governance is a complex new field requiring an initial conceptual mapping and classification. The complexity of Internet governance 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 difficulties grasping the complexity of Internet governance. A conceptual mapping, provided by various academic inputs and the Working Group on Internet governance (WGIG) Report, contributed towards more efficient negotiations within the context of the WSIS. The WGIG Report (2004) identified the following four main areas:

- issues related to infrastructure and the management of critical Internet resources;

- issues related to the use of the Internet, including spam, network security and cybercrime;
- issues relevant to the Internet but have an impact much wider than the Internet and for which existing organizations are responsible, such as intellectual property rights (IPRs) or international trade;
- issues related to the developmental aspects of Internet governance, in particular capacity-building in developing countries.

The agenda for the first Internet Governance Forum held in Athens (2006) was build around the following thematic areas: Access, Security, Openness and Diversity. At the second IGF in Rio de Janeiro (2007), the fifth thematic area – Managing Critical Internet Resources – was added to the agenda.

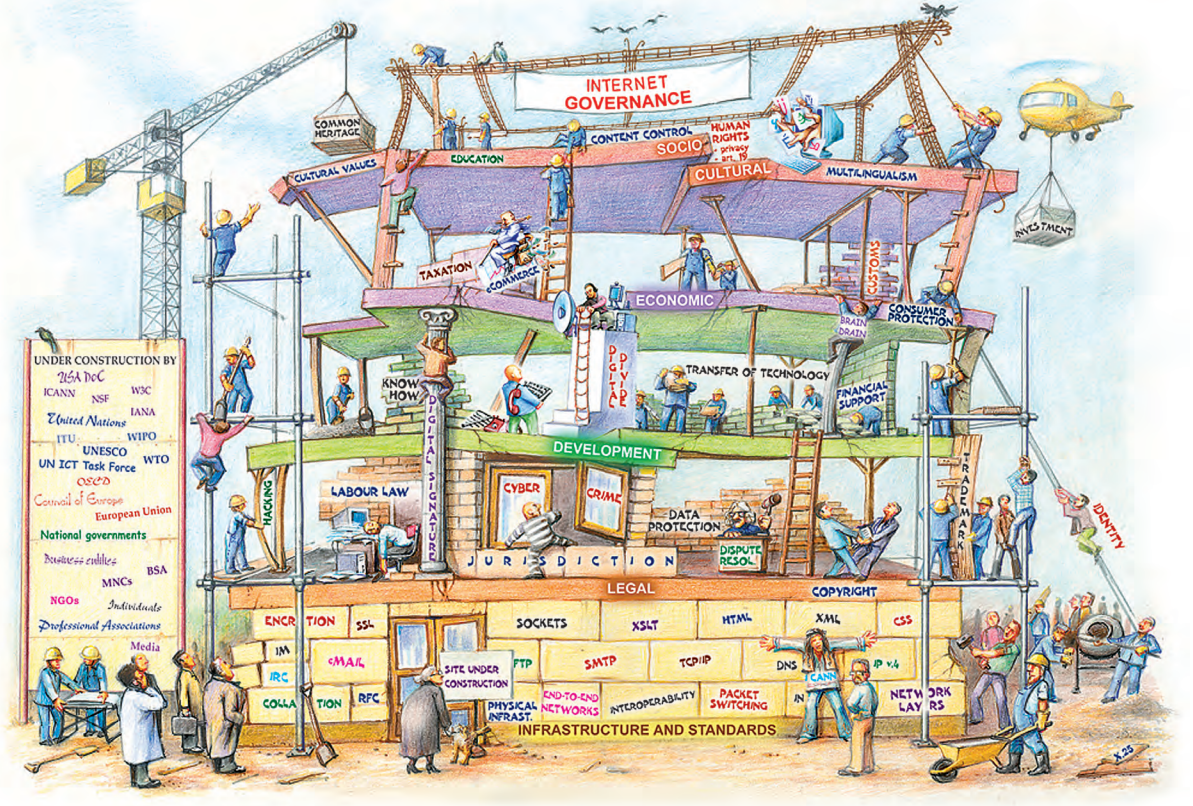
Although the classification changes, Internet governance addresses more or less the same set of 40-50 specific issues, with the relevance of particular issues changing. For example, while Spam featured prominently in the WGIG classification in 2004, its policy-relevance diminished at the IGF meetings,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

Diplo's classification of Internet governance groups the set of the main 40-50 issues into five clusters. Adapting the terminology to the world of diplomacy, Diplo has adopted the term "basket." (The term "basket" was introduced into diplomatic practice during the Organisation on Security and Cooperation in Europe (OSCE) negotiations.) The following five baskets have been used since 1997, when Diplo started developing its classification scheme:

1. infrastructure and standardisation;
2. legal;
3. economic;
4. development;
5. socio-cultural.

Diplo's classification reflects both the above-mentioned (WGIG, IGF) policy approaches as well as academic research in this field. It has been constantly adjusted through several iterations based on the feedback from students (alumni of 700 students as of 2009), research results and feedback from the policy process.

The five-basket classification of Internet governance is metaphorically presented through the "Building under Construction" image, developed by Diplo researchers.


INTERNET GOVERNANCE
COMMON HERITAGE
CONTENT CONTROL
SOCIO
HUMAN RIGHTS
privacy art. 19
CULTURAL
CULTURAL VALUES
EDUCATION
MULTILINGUALISM
INVESTMENT
TAXATION
E-COMMERCE
ECONOMIC
CUSTOMS
BRAIN DRAIN
CONSUMER PROTECTION
TRANSFER OF TECHNOLOGY
KNOW HOW
DIGITAL DIVIDE
FINANCIAL SUPPORT
DEVELOPMENT
HACKING
LABOUR LAW
CYBER
CRIME
DIGITAL SIGNATURE
DATA PROTECTION
DISPUTE RESOL.
TRADEMARK
IDENTITY
JURISDICTION
LEGAL
COPYRIGHT
UNDER CONSTRUCTION BY
DoC
ICANN
NSF
W3C
IANA
United Nations
ITU
WIPO
UNESCO
WTO
UN ICT Task Force
OECD
Council of Europe
European Union
National governments
Business entities
BSA
MNCs
NGOs
Individuals
Professional Associations
Media
ENCRYPTION
SSL
IM
eMAIL
IRC
COLLABORATION
RFC
SOCKETS
XSLT
HTML
XML
CSS
SITE UNDER CONSTRUCTION
FTP
SMTP
TCP/IP
DNS
IP v.4
ICANN
IN
NETWORK LAYERS
PHYSICAL INFRAST.
END-TO-END NETWORKS
INTEROPERABILITY
PACKET SWITCHING
X.25
INFRASTRUCTURE AND STANDARDS

"Building under Construction:" Internet Governance – Are We Building the 21st 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. (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. This comparison has prompted the authors to consider another building under construction – 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 in the picture on the previous page. Each floor in this building is discussed in the chapters that follow. It is important to realise that all of the floors in this building are linked, and that construction is on-going and never-ending.

NOTES

[1] Numbers related to Internet growth should be taken with a healthy dose of scepticism and caution. It is now widely documented that the telecommunication boom in the late 1990s and failure of many investments in this sector was caused by the completely unrealistic estimation that Internet traffic would double every three months. This completely wrong assumption was mentioned on a few occasions even by authorities in the field of communication, including Reed Hundt, the Chairman of the US Federal Communication Commission. A number of articles have been written about this phenomenon, including: Odyzko, "Internet Growth: Myth and Reality, Use and Abuse," **http://www.dtc.umn.edu/~odlyzko/doc/internet.growth.myth.pdf**, and "Internet as Hyperbole," **http://folk.uio.no/gisle/essay/diff.html** (accessed on 14 November 2008).

[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, Stephen (1983): "Introduction," in Stephen D. Krasner (ed.) International Regimes, Ithaca, NY: Cornell University Press)

[3] Shannon, Victoria (2006) "What's in an 'i'? Internet Governance", *International Herald Tribune,* 3 December, available from **http://www.iht.com/articles/2006/12/03/technology/btitu.php** (accessed on 14 November 2008).

[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" was directly related to core government functions.

[5] For the evolution of the use of the word "Internet" in the preparation for the Geneva summit consult, DiploFoundation (2003) *The Emerging Language of ICT Diplomacy – Key Words,* available from **http://www.diplomacy.edu/IS/Language/html/words.htm** (accessed on 14 November 2008).

[6] Volker Kitz provides an argument for the analogy between administration of telephony systems and Internet names and numbers. See Volker Kitz (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 from h**ttp://www.smu.edu/csr/articles/2004/Winter/Kitz.pdf** (accessed on 14 November 2008).

[7] Excerpts from the speech delivered at the ICANN Meeting in Cairo (6 November 2008); visit: **https://cai.icann.org/files/meetings/cairo2008/toure-speech-06nov08.txt**. (accessed on 14 November 2008).

SECTION 2

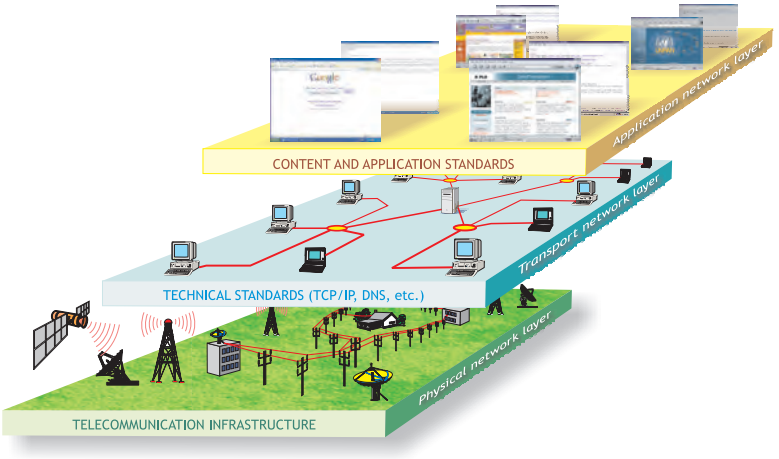
The Infrastructure and Standardisation Basket

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 putting 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 the following 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, DNS, SSL); and
3. the content and applications standards (e.g., HTML, XML).



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 utilizing power line 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 the national and international levels 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]

The roles of the WTO and the ITU are quite different. The ITU sets detailed voluntary technical standards, telecommunication-specific international regulations, and provides assistance to developing countries.[4] The WTO provides a framework for general market rules.[5]

ITU International Regulation (ITR) from 1988 facilitated the international liberalisation of pricing and services and allowed a more innovative use of basic services 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 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 "Last Mile" – "Local Loop"

The "local loop" (or "last mile") is the name given to the connection between Internet service providers and their individual customers. Problems with "local loops" are an obstacle to the more widespread use of the Internet in many, mainly developing countries. One possible, low-cost solution to the "local loop" problem may be found in wireless communication. Apart from increasingly available technical options, the solution to the problem of the "local loop" 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. However, many developing countries are faced with a hard choice: to liberalise and make the telecommunication market more efficient, or to preserve an important budgetary income from the existing telecommunication monopolies.[6] 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 (IEEE). 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.

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 antitrust 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.

(Source: Janet Abbate, *Inventing the Internet,* MIT Press)

TRANSPORT CONTROL PROTOCOL/ INTERNET PROTOCOL (TCP/IP)

THE CURRENT SITUATION

The Internet's main technical standard, specifying how data is moved through the Internet, is TCP/IP, which is based on three principles: packet-switching, end-to-end networking, and robustness. Internet governance related to TCP/IP has two important aspects: a) the introduction of a new standards; b) 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 the IETF. Any changes to TCP/IP require extensive prior discussion and proof that they are an efficient solution (the "running code" principle).

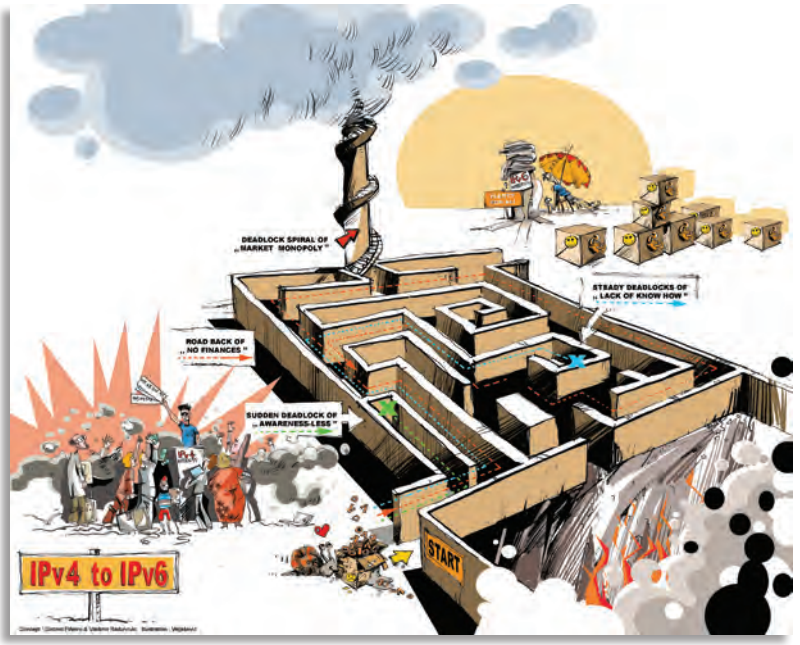
IP numbers are numeric addresses that all computers connected to the Internet must have. IP numbers are unique; two computers connected to the Internet cannot have the same IP number. This makes IP numbers a potentially scarce resource. The system for the distribution of IP numbers is hierarchically organised. At the top is IANA (the Internet Assigned Numbers Authority – a subsidiary of ICANN), which distributes blocks of IP numbers to the 5 regional Internet registries (RIRs).[7] RIRs distribute IP numbers to the 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 Internet Protocol 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:

- to rationalise the use of the existing pool of IP numbers through the introduction of Network Address Translation (NAT);
- to address the wasteful address allocation algorithms used by the RIRs by introducing Classless Inter-Domain Routing (CIDR);
- to introduce a new version of the TCP/IP protocol – IPv6 – which provides a much bigger pool of IP numbers (430,000,000,000,000,000,000).



The response of 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 the IPv6 was introduced back in 1996, its deployment has been very slow. With the approaching depletion of the pool of IPv4 numbers in 2011, the slow deployment of IPv6 is acquiring elements of a crisis in the making.

One of the main challenges for the deployment of IPv6 is the lack of backward compatibility between IPv6 and IPv4. The 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 is also delayed by the low interest on the part of Internet Service Providers (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 the ISPS are aware of the risk of depletion of IPv4, only 30% are preparing for transition to IPv6. In a such 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, financial support for the transition to IPv6 and the use of IPv6 for governments 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 networks based on IPv6 from the beginning. In this process developing countries will need technical assistance.[8]

Apart from the problem of transition, the policy framework for the 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, the Internet consisted of a closed network of research institutions. With the expansion of the Internet to over 1 billion users worldwide and its growing importance as a commercial tool the question of security was placed high up 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, the 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.[9]

Changes in TCP/IP and the Problem of Limited Bandwidth

To facilitate the delivery of multimedia content (e.g., Internet telephony, or 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 Internet protocol, including a potential risk for the principle of net neutrality.

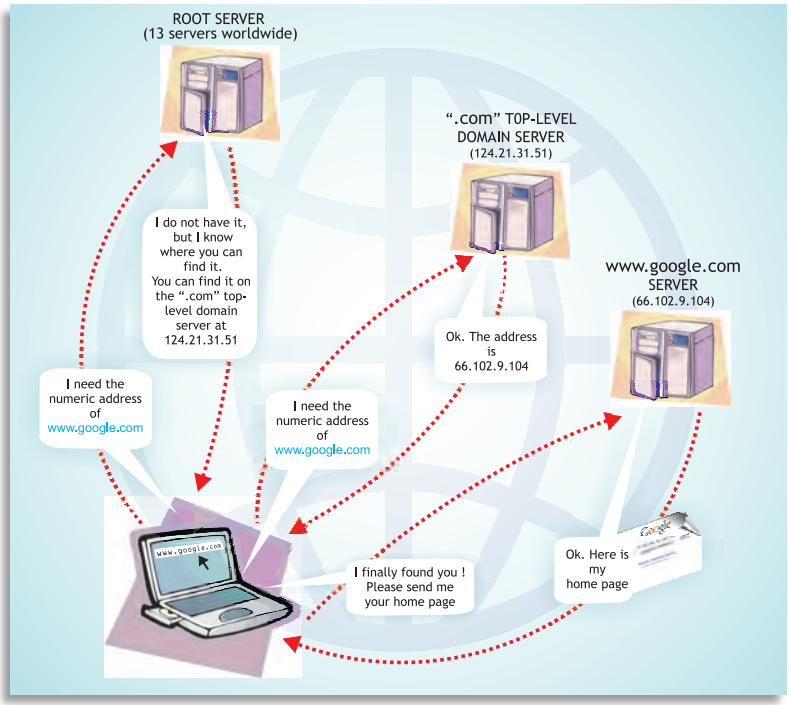
THE DOMAIN NAME SYSTEM (DNS)

THE CURRENT SITUATION

The DNS handles Internet addresses (such as **www.google.com**) and converts them to IP numbers (a simplified scheme of this process is presented in the drawing below). The DNS consists of root servers, top-level domain (TLD) servers, and a large number of DNS servers located around the world. The management of the 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, DOC) over root servers, the top tier of the hierarchically organised Domain Name System. 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 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.

The DNS is based on two types of top-level domains. One is generic; the other is based on country codes. For each generic top-level domain (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 (Internet Corporation for Assigned Names and Numbers) provides overall coordination of the DNS system 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 the management of the Domain Name System 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 cyber-squatting, the practice of registering domain names that could be resold later on. The Uniform Dispute Resolution Policy (UDRP) developed by ICANN and the World Intellectual Property Organisation (WIPO) provides mechanisms that have significantly reduced cyber-squatting.

Another important element in the survey of the current organisation of DNS governance is the management of country code Top-Level Domains (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, top-level domains is almost unlimited. However, the introduction of new, generic top-level domains (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 business sector, whose concern is that increasing the number of domains would complicate the protection of their trademarks.

Under pressure to introduce new gTLDs, ICANN initiated consultations to design a new policy in this field. The new policy should address how to resolve competing claims for gTLDs, questions of public morality, and registration fees, among others. The new policy for gTLDs should be introduced in 2009.

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 latest example was the proposal to introduce the "xxx" domain for pornographic websites. The board of ICANN 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 the introduction of the "xxx" domain.[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.

Regarding the merits of the "xxx" domain, some argued that an "adult zone" on the Internet would clearly identify controversial material and reduce the risk of children's access to this type of material. Others were against the introduction of the "xxx" domain based on various religious and cultural grounds. The decision by ICANN on the "xxx" case also re-opened the discussion about the role of ICANN 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] This precedent has triggered a new controversies. First, many language and cultural communities around the world are likely to request the same right. Second, in some cases language and cultural communities may have aspirations towards nationhood. This aspect may cause potential controversies and conflicts with existing states. In the case of the ".cat" domain, the Spanish government did not oppose this decision.

The Management of Country Domains

The management of country top-level domains 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 recent controversial issue was the allocation of a Palestinian Authority domain name. In justifying its decision to assign the "ps" top-level domain, the Internet Assigned Numbers Authority (IANA) reiterated the principle of allocating domain names in accordance with the ISO 3166 standard, as was proposed by Jon Postel, one of the founding fathers of the Internet.[14]

The second issue concerns who should manage country codes. 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 a consensus exists within the country, reached by all the interested stakeholders. Given the importance of this issue and the wide variety of approaches, there were two important initiatives at the international level to introduce a certain level of harmonisation. The first was the "GAC Principles," adopted by the ICANN Government Advisory Committee (GAC), which proposes policy and specifies 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 the regional level (Europe – CENTR, Africa – AFTLD, Asia – APTLD, North America – NATLD, and South America – LACTLD). At the 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 initially developed for communication in English. Through rapid growth, the Internet has become a global communication facility with an increasing number of non-English speaking users. The lack of multilingual features in the Internet infrastructure could prove one of the main limits in the future development of the Internet.

The technical community, organised in the IETF, has developed a solution for Internationalised Domain Names (IDN), which should facilitate the use of a wide variety of scripts (e.g. Chinese, Arabic, Cyrillic) for domain

names alongside English ones. The IDN technical solutions are currently undergoing testing with ICANN.

Apart from the technical difficulties, the next, probably more complex, challenge will be to develop policy and management procedures. There is increasing pressure for IDN to be managed by countries or groups of countries speaking the same language. For example, the Chinese government has indicated on a number of occasions that IDN in Chinese should be managed by China. A similar request has been made by Russia for Cyrillic script. The introduction of an IDN policy will be one of the main tests for the current Internet governance regime.

ROOT SERVERS

At the top of the hierarchical structure of the domain name system, 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 the 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, 3 elsewhere; of the 10 in the USA, several are operated by US government agencies), which is the maximal 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

the DNS system and the 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, DOC). Once the content is approved by the DOC, it is entered into the master root server operated by VeriSign under contract with the DOC.

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 concerning the content of root servers remains the responsibility of one country (United States). In the Internet governance negotiations there were various proposals, 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. One can notice some elements for a "solution-in-the-making" which would consist of two steps:

- 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.
- 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.

US Role in the Management of the Root Servers – The Paradox of Power

After the adoption of the "Affirmation of Commitments" the question of the paradox of US power over the root server 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 lingua franca, the 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.

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

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 inhibit 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 the operational level (e.g. by providing lower bandwidths or causing disruptions in services).

The Responsibility of ISPs over Copyrights

Common to all legal systems is the principle that an ISP cannot be held responsible for hosting materials that breach copyrights 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 requests the ISP 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).[19]

The Role of ISPs in Content Policy

Under growing public pressure ISPs are gradually, even though 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 on what is appropriate content themselves. This runs the risk of the privatisation of 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: a) an ISP must prohibit its users from spamming; b) an ISP must not peer with ISPs that do not accept a similar code of conduct.[20]

The problem of spam exposes ISPs to new difficulties. For instance, the Verizon company's anti-spam filtering led to a court case. Besides spam, Verizon's filter also blocked legitimate messages. This caused inconvenience to users who did not receive their legitimate e-mail, which led them to initiate a court case against Verizon.[21]

INTERNET BANDWIDTH PROVIDERS

The Internet access architecture consists of three tiers. ISPs that connect end users constitute Tier 3. Tiers 1 and 2 consist of the Internet bandwidth carriers. Tier 1 carriers are the major IBPs. They usually have peering arrangements with other Tier 1 IBPs.[22] 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.[23]

Tier 1 is usually run by large companies, such as MCI, AT&T, Cable Wireless, and France Telecom. In the field of Internet backbone carriers, traditional telecommunication companies have extended their global market presence to Internet backbones.

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, 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? Can those operators be requested to run the Internet as a public facility?

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 (the Internet cable near Taiwan and the main Internet cable for Pakistan). These incidents show clearly 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

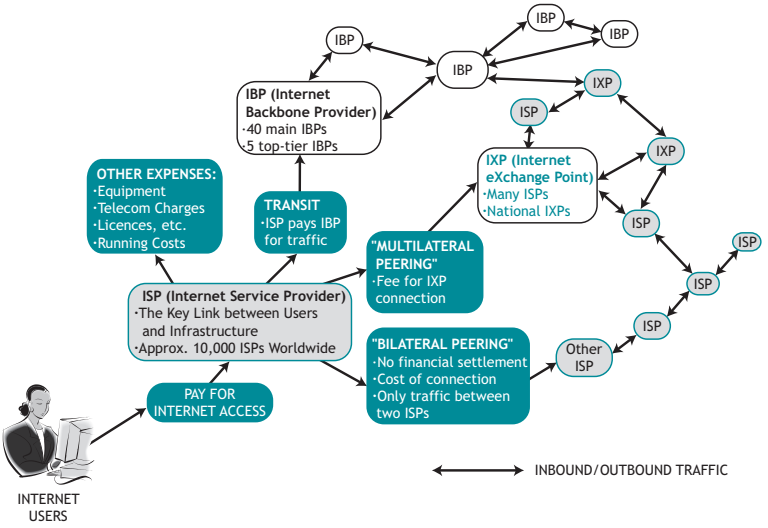
There are opposing views about the extent to which ISPs and IBPs should be subjected to existing international instruments. Developed countries argue that the liberalised rules granted by the WTO to telecommunication operators can also be extended to ISPs. A restrictive interpretation highlights the 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 CONNECTIVITY

"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.[24] Who pays for the Internet? Many 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?"[25] 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 regional Internet registries (RIR) or local Internet registries (LIR), 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,
- 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 legacies is current Internet 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:

- 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;
- 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.[26] Other authors 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. In 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.[27] 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.[28]

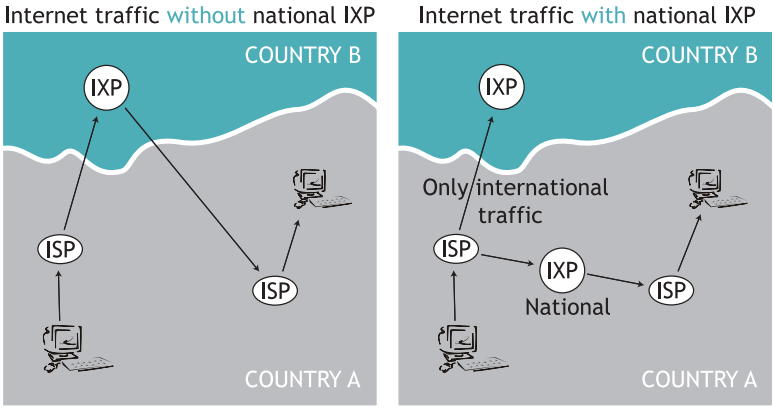
Who Should Cover the Cost of Links between Developing and Developed Countries?

> "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."[29]

Currently, developing countries cover the cost of links between developing and developed countries.[30] 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 the 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 end-points. 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.[31] 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.

The ITU initiated discussions on possible improvements to the current system for the settlement of Internet expenses, with the main objective of having 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.[32] Unsuccessful attempts were also made to introduce this issue during the WTO negotiations. The need for adjustments in interconnection charges was reiterated in the WSIS final documents and in the WGIG Report.



Reduction of Access Costs through the Use of Internet eXchange Points (IXPs)

IXPs are technical facilities through which different ISPs 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.[33]

IXPs could also play an important role in reducing the digital divide.[34] For example, in the case of a country without national IXPs, 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. The addition of national and regional IXPx could reduce Internet costs for developing countries.

WEB STANDARDS

By the late 80s, the battle over network standards was over. TCP/IP gradually became the main network protocol, marginalising other standards, such as the ITU-supported X-25 (part of the Open Systems Interconnection architecture) and many proprietary standards, such as IBM's SNA. While the Internet facilitated normal communication between a variety of networks via TCP/IP, the system still lacked common applications standards.

A solution was developed by Tim Berners-Lee and his colleagues at CERN in Geneva, consisting of a new standard for sharing information over the Internet, called HTML (HyperText Mark-up Language, really just a simplification of an existing ISO standard called SGML). 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 technologies 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 (eXtended Mark-up Language), 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 Mark-up 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, the W3C has not attracted much attention in the debate on Internet governance.

CLOUD COMPUTING

The term "cloud computing" is used to describe a new trend in the computer industry based on the use of computer applications as services delivered from huge "server farms". The first glimpse of cloud computing is already available with the move of e-mail from our hard-disks to mail servers (Gmail, Yahoo, Hotmail), the use of online word processors (wiki, Google services). Social networking applications such as Facebook and blogs further accelerated 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, who either already have or plan to develop big "server farms".

Historians of technology can notice that with cloud computing we close the circle. In the early days of computers, there were powerful main-frame computers and dumb workstations. The power was in the center. After that, for a long time, with PCs and Windows applications, computer power moved to the edges. Is the circle going to be closed with "cloud computing"? 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 need time. Currently, we can identify a few Internet governance issues which are very likely to emerge in parallel with the development of cloud computing.

First, with the more services delivered online, modern society will increase its dependence on the Internet. In the past, with the Internet 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 the text or do calculations. This higher dependence on the Internet will imply higher pressure on its robustness and reliability. It will inevitably lead towards stronger a Internet governance regime and higher involvement of governments.

Second, 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-mail and other data? May cloud operators use it without our permission? Who will have access to our data?

Third, 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.

Fourth, with diverse operators of cloud computing, the question of standards is becoming highly important. The adoption of common standards will ensure a smooth transfer of data among different clouds (e.g. from Google to Apple). One possibility which is being discussed is the adoption of open standards by the main players in cloud computing.

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

The broad and prevailing use of the Internet Protocols has aided in the convergence of technological platforms for telecommunication, broadcasting, and information delivery. Today, we can make telephone calls, watch TV, and share music on our computers via the Internet. Only a few years ago it was handled by different systems.

In the field of traditional telecommunication, the main point of convergence is the Voice over Internet Protocol (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 the 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 Internet service providers, 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 European Union, 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 US, where cable Internet is much more prevalent than ADSL, 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 net 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, giving them complete control over their subscribers' Internet access. They can block the use of certain applications and control the 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."

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 it is 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 of individuals, where security concerns, if they existed at all, were limited. The main Internet users, academic communities, developed strong, but informal rules to reduce security breaches.

Cybersecurity came into sharper focus with the rapid expansion of the Internet user base. The Internet proved what many had suspected for a long time: 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 an increased vulnerability of modern society. The Internet is a part of the global critical infrastructure. Critical infrastructures, including electricity grids, transport systems, and health services are all part of a global network, potentially exposed to cyber-attack. As attacks on these systems may cause severe disruption and have high financial consequences, critical infrastructures are frequent targets.

Cybersecurity issues can be classified according to three criteria: type of action, type of perpetrator, and type of target. Classification based on type of action may include: data interception, data interference, illegal access, spyware, data corruption, sabotage, denial-of-service, and identity theft. Possible perpetrators might include hackers, cyber-criminals, cyber-warriors, and cyber-terrorists. 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 the 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. The Department of Homeland Security is the main institution dealing with questions of

cybersecurity. It is difficult to find any of the developed countries without some initiative focussing on cybersecurity.

At the international level, the most active organisation is the ITU, which 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 (HTTPS). Recently, the ITU moved beyond strictly technical aspects and launched the "ITU Global Cybersecurity Agenda".[35] 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. The G8 has also formed a Subgroup on High Tech Crime to address the establishment of 24x7 communication between the cybersecurity centres of member states, the training of staff, and the improvement of state-based legal systems that will 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 in 1998, 54/49 in 1999, 55/28 in 2000, 56/19 in 2001, 57/239 in 2002 and 58/199 in 2003. Since 1998, all subsequent resolutions have included similar content, without any significant improvements. They do not reflect the considerable changes that have taken place in the field of cybersecurity since 1998.

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.[36] Some countries have established bilateral arrangements. The United States has bilateral agreements on legal cooperation in criminal matters with more than 20 other countries.[37] These agreements also apply in cases of cybercrime.

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

THE ISSUES

Influence of Internet Architecture on Cybersecurity

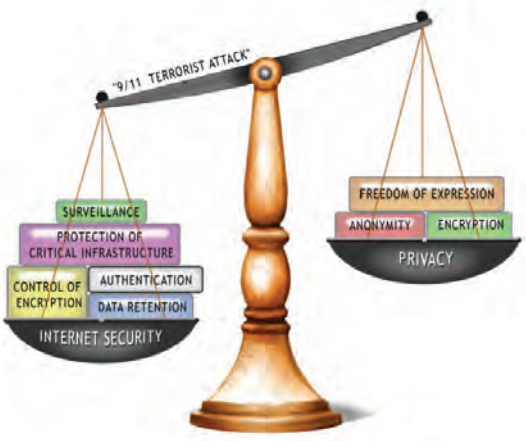
The very nature of Internet organisation affects its security. Should we continue with the current approach of building security on a pre-existing

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 the 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 the 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 improves only slowly (with, e.g. lack of standards), it is likely that the business sector will push for faster developments in cybersecurity. It may lead towards further challenges for the principle of net neutrality and the development of "a new Internet," which would facilitate, among other things, 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 communications of terrorists and criminals? The answers to these and other questions depend on the constantly shifting balance between cybersecurity and privacy.

In the aftermath of the terrorist attack in New York in September of 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 focussed on the dangers to privacy and to the concept of freedom of expression.

On the international level, the question of balancing the security of information and communication technology with privacy has been the focus of discussions regarding the extension of the Council of Europe Convention on Cybercrime to the global level. The main objection from human rights activists is that the Cybercrime 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 international distribution of encryption software. The US software companies initiated a strong lobbying campaign arguing that export controls do not increase national security but only 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" 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 US 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.

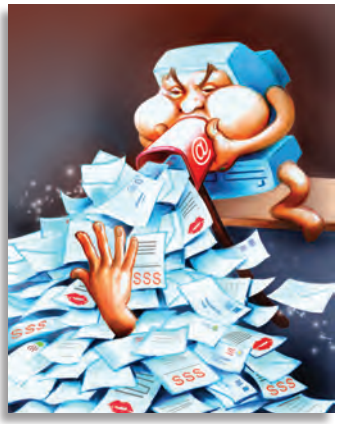
A few attempts to develop an international regime for encryption, mainly within the context of the Wassenaar Arrangement, did not result in the development of an effective international regime. It is still possible to obtain powerful encryption software on the Internet.

SPAM

THE CURRENT SITUATION

Spam is usually defined as unsolicited e-mail, which is sent to a wide number of Internet users. Spam is 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 affects almost everyone who connects to the Internet. According to the latest statistics, of every 10, 9.5 may be categorised as spam. Besides the fact that it is annoying, spam also causes considerable economic loss, both in terms of bandwidth used and time lost on checking/deleting it. Some recent studies on spam reported that the loss in terms of bandwidth capacity alone is in the range of €10 billion.

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 US, the Can-Spam Law involves a delicate balance between allowing e-mail based promotion and preventing spam.[39] 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" (by using 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.

Spam and "Policy Fashion"

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

Since 2005, the volume of spam has tripled, according to conservative estimates (2005: 30 billion messages per day; 2008: 100 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 Internet Governance Forum in Hyderabad, spam was mentioned only in the title of one of workshop (out of 91 proposed workshops). The main reason for this change in the global policy relevance of spam remains to be discovered.

In July 2003, the European Union 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 towards a reduction in spam.[39] In 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.

THE INTERNATIONAL RESPONSE

Both of the anti-spam laws adopted in the US and 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, recently stated that the problem cannot be solved on a "country by country" basis. A similar conclusion was reached in a recent study on the EU anti-spam

law carried out by the Institute for Information Law at the University of Amsterdam: "The simple fact that most spam originates from outside the EU restricts the European Union's Directive's effectiveness considerably." A global solution is required, implemented through an international treaty or some similar mechanism.

A Memorandum of Understanding 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. The ITU has also been proactive by organising the Thematic Meeting on Countering Spam (2004) for considering various possibilities of establishing a global Memorandum of Understanding on Combating Spam. At the regional level, the EU established the Network of Anti-Spam Enforcement Agencies and APEC 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 US, a general concern about the protection of the freedom of speech and the First Amendment affect the anti-spam campaign as well. 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 email" regardless of its content. Since most spam is generated from the US, 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. The 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

As was stated above, 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 Memorandums of Understanding (MOU), 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.

NOTES

[1] The terms Internet and WWW are sometimes used interchangeably, however, there is a difference. The Internet is a vast network of networks and 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 the HyperText Transfer Protocol (HTTP).

[2] Internet transfer via an electric grid is called Power Line 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, please consult: "Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication" (Internet Society, ISOC Member Briefing No. 13; available at **http://www.isoc.org/briefings/013**; accessed on 14 November 2008).

[3] The liberalisation of telecommunication markets of WTO members was formalised in 1998 in the so-called 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 entering into force on 5 February 1998); **http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm** (accessed on 13 November 2008).

[4] One of the controversies surrounding the WSIS was the ITU's intention to become more involved in the Internet governance process, especially within a domain handled by ICANN. For more information about ITU's Internet policy, please consult: **http://www.itu.int/osg/spu/ip/** (accessed on 14 November 2008).

[5] For more information about the WTO's role in the field of telecommunication, please consult **http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm** (accessed on 14 November 2008).

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

[7] 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** (accessed on 14 November 2008).

[8] For a detailed discussion on IPv6, please consult the research project: "IP Allocation and IPv6" by Jean Philémon Kissangou, Marsha Guthrie, and Mwende Njiraini, a part of the 2005 Internet Governance Capacity Building Programme: **http://textus.diplomacy.edu/Textusbin/portal/Ghome.asp?IDspace=84** (accessed on 14 November 2008).

[9] For a comprehensive and highly technical survey of TCP/IP Security, please consult: Chris Chambers, Justin Dolske, and Jayaraman Iyer, TCP/IP Security, Department of Computer

and Information Science, Ohio State University: **http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html** (accessed on 14 November 2008).

[10] An overview of the gTLDs with a link to the list of all the TLDs is available at **http://www.icann.org/registries/about.htm** (accessed on 14 November 2008).

[11] One previous example of content-related domains is "kids.us" domain. The US Congress adopted a law introducing the domain, "kids.us," 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 been used only 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: **http://www.icann.org/tlds/stld-apps-19mar04/cat.htm**. (accessed on 14 November 2008).

[14] The IANA Report on the county code top-level domain for Palestine is available at: **http://www.iana.org/reports/ps-report-22mar00.htm** (accessed on 14 November 2008).

[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, please consult: Alfonso, Carlos, BR: CCTLD An Asset of the Commons, in: MacLean, Internet Governance: A Grand Collaboration (UN ICT Task Force, New York, 2004), pp. 291-299; Norbert Klein, Internet Governance: Perspectives from Cambodia in "Internet Governance: A Grand Collaboration" edited by Don MacLean (United Nations, 2004), p. 227-237.

[16] "Principles for the Delegation and Administration of Country Code Top-Level Domains," currently being redrafted: **http://www.icann.org/committees/gac/gac-cctldprinciples-23feb00.htm** (accessed on 14 November 2008).

[17] The list of root zone servers, their nodes and positions, and managing organisations is available at **http://www.root-servers.org/** (accessed on 14 November 2008)

[18] See: **http://www.icann.org/en/announcements/announcement-30sep09-en.htm**

[19] A summary of these and other court cases is available at: **http://www.diplomacy.edu/ig/resources/booklet/isp/** (accessed on 14 November 2008).

[20] Frances Williams, "ISPs should be liable for spam, says UN report" (Financial Times, 8 November 2006).

[21] "The End user: Junk Payout in Spam Case" (International Herald Tribune, 13 April 2006): **http://www.iht.com/articles/2006/04/12/business/PTEND13.php** (accessed on 15 November 2008)

[22] 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 HSCGroup (**www.hscgroup.co.uk**). The peering arrangement is a mutual benefit, and is also common among the ISPs, as well as telecom operators.

[23] Tier 2 Internet Bandwidth Providers are usually called ICP (Internet Connection Points) or Internet Gateways.

[24] 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. For more information, please consult: Andrew Odlyzko, "Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation" **http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf** (accessed on 14 November 2008)

[25] Shawn O'Donnel, 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. **http://itc.mit.edu/itel/docs/2002/Internet_Map.pdf**; link was suggested by Djordje Marinkovic, Diplo's Internet Governance Portal).

[26] Thuy T. T. Nguyen and Grenville J. Armitage, "Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model," ETRI Journal, vol.27, no.1, Feb. 2005, pp. 64-74.

[27] See the website, which is an "online market" of Internet resources, offering bandwidth, Internet access and other Internet resources: **http://www.bandwidthmarket.com/** (accessed on 14 November 2008).

[28] Geoff Huston, "Where's the Money? – Internet Interconnection and Financial Settlements," The ISP Column, Internet Society (January 2005), **http://ispcolumn.isoc.org/2005-01/interconns.pdf** (accessed on 14 November 2008).

[29] "The Halfway Proposition: Background Paper on Reverse Subsidy of G8 Countries by African ISPs," Conference of African Ministers of Finance, Planning and Economic Development, Johannesburg, South Africa, 19 October 2002.

[30] For a comprehensive survey of interconnection costs, please consult: B. Esmat and Juan Fernandez, "International Internet Connections Costs" in William J. Drake, "Reforming Internet Governance: Perspectives from the Working Group on Internet Governance (WGIG)," New York: 2005, pp. 73-86. Mike Jensen, in "Interconnection Costs" (APC: 2005), provides a comprehensive analysis of the topic at: **http://rights.apc.org/documents/interconnection_costs.pdf** (accessed on 14 November 2008).

[31] Geoff Huston, "Where's the Money? Internet Interconnection and Financial Settlement," The ISP Column, January 2005, Internet Society, pp. 7-9.

[32] 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.

[33] Please consult the list of regional and national IXPs: **http://en.wikipedia.org/wiki/Internet_Exchange_Point#List_of_IXPs_and_IXP-operators** (accessed on 14 November 2008).

[34] For the potential of IXPs in Africa, please consult: "Internet Exchange Points: Their Importance to the Development of the Internet and Strategies for Their Deployment

– The African Example," by Global Internet Policy Initiative: **http://www.internet-policy.net/practices/ixp.pdf**.

[35] For more information on the ITU Global Cybersecurity Agenda please consult: **http://www.itu.int/osg/csd/cybersecurity/gca/** (accessed on 14 November 2008).

[36] The convention text is available at: **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm** (accessed on 14 November 2008).

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

[38] More references to Can-Spam can be obtained from: **http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm** (accessed on 14 November 2008).

[39] 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 the ITU.

SECTION 3

The Legal Basket

THE LEGAL BASKET

THE LEGAL BASKET – INTRODUCTION

Almost every aspect of Internet governance includes a legal component, yet the shaping of a legal framework to mould the rapid development of the Internet is still in its early stage. The two prevalent approaches are:

a) 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]
b) A "cyberlaw" approach is based on the presumption that the Internet introduces new types of social relationships in cyberspace. Consequently, there is a need to formulate new "cyberlaws" 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

There is a wide variety of legal instruments that has 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 (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 field of the Internet. This is especially the case within 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.

Regardless of whether the "real" or "cyber" approach is more appropriate, the general principle remains that **laws do not make prohibited behaviour impossible, only punishable.** The fact that fraud is prohibited in both the "cyber" and "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.

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 of the Internet, its 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.

Self-Regulation

The US government 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-regulation 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 increasing pressure from government authorities to enforce rules related to content policy. ISPs are increasingly using self-regulation as a method of imposing certain standards of behaviour and, ultimately, of preventing government interference in their activities.

While self-regulation can be a useful regulatory technique, some risks remain in using it for regulating 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 is acceptable content? Other issues need to be addressed too: 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. A list of analogies is available on pages 21-26.

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 international private law are stipulated in national legislation, not in international treaties.[2] 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 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, international trade treaties). In this part, 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*.

International Conventions

The main set of conventions on Internet-related issues was adopted by the 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 Cybercrime Convention. 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 over the Internet root. The US government 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 the awareness by 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 (.com, .org, .edu, .net), which do not involve other countries.

Soft Law

"Soft law" has become 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. Since it is not legally binding, it cannot be enforced through international courts or other dispute resolution mechanisms.

Soft law instruments contain principles and norms rather than specific rules. It is usually found in international documents such as declarations, guidelines, and model laws.

The main 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.[3]

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 adjustment 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."[4] Professor Brownlie lists the following examples of *ius cogens* rules: 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.[5] 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:

- an inability of the state to exercise its legal power as a responsible entity in regulating social relations within its territory;
- 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?[6]

JURISDICTION – BASIC TECHNIQUES

Three main considerations are important when thinking about jurisdiction:

- Which court or state authority has the proper authority (procedural jurisdiction);
- Which rules should apply? (substantive jurisdiction);
- 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.[7] "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."[8] Universal jurisdiction covers such crimes as piracy, war crimes, and genocide.

CONFLICT OF JURISDICTION

The principles for establishing jurisdiction (territoriality, 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.[9]

One of the most illustrative and frequently quoted cases that exemplify the problem of jurisdiction is the 2001 Yahoo! Case in France.[10] The Yahoo! Case prosecuted in French courts reiterated the high relevance of the problem of multiple jurisdictions.[11] The Yahoo! Case 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 US, 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 access from France and block their access to the webpages with Nazi materials.

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

The harmonisation of national laws could result in the establishment of one set of equivalent rules at the 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.[12] Another potential consequence of a lack of harmonization 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.

ARBITRATION

Arbitration is a dispute resolution mechanism available in place of traditional courts. In arbitrations, decisions are made by one or more independent individuals 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 is available, specifying such issues as place of arbitration, procedures, and choice of law.

Below is 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 (*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

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.[13] 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 rather than regular court judgments.

The main limitation of arbitration is that it cannot address issues of higher public interest, which 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 UNCITRAL *Model Law on International Commercial Arbitration* (1985), supplemented by other UNCITRAL instruments.[14] 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), or 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 Universal Domain Name Dispute Resolution Policy (UDRP), which was developed by WIPO and implemented by ICANN as the primary dispute resolution procedure.[15]

The Universal Domain Name Dispute Resolution Policy 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 as well. Its unique aspect is that arbitration awards are applied directly through changes in the Domain Name System without resorting to enforcement through national courts.

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 no agreement between parties has 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 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 socio-cultural aspects are at issue, where a national legal system reflects specific cultural content.

INTELLECTUAL PROPERTY RIGHTS

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

IPRs have 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 IPRs include copyright, trademarks, and patents.[16]

COPYRIGHT

Copyright protects only 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 by copyright. 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 the 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" texts 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.

These developments endanger the delicate balance between authors' rights and the public interest, which is the very basis of the 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 however has gradually been changing, mainly through numerous global initiatives focusing on the open access to knowledge and information.

THE CURRENT SITUATION

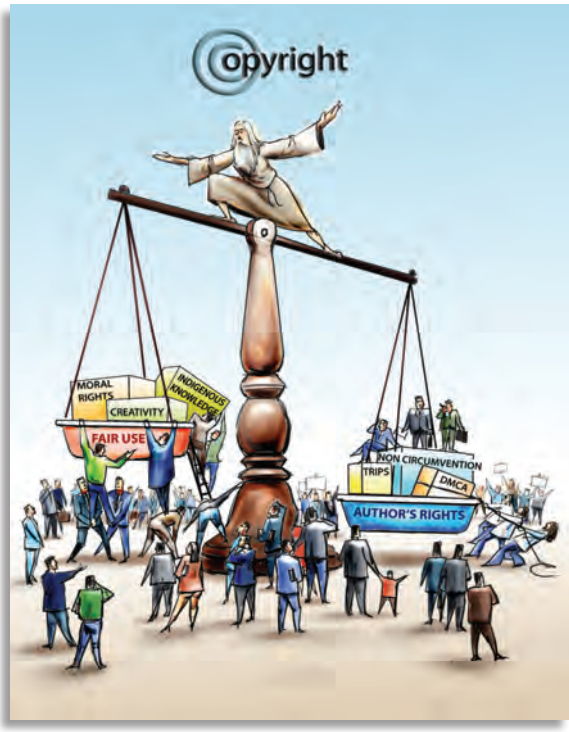
Stricter Copyright Protection at the National and the International Levels

The recording and entertainment industries have been lobbying intensively at the national and international levels to strengthen copyright protection. In the United States, stricter protection of copyright was introduced through the US Digital Millennium Copyright Act (DMCA) of 1998. At the international level, the protection of digital artefacts was introduced in the World Intellectual Property Organization (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 the file-sharing activities of their subscribers, and more than 500 lawsuits against individuals were launched. A particularly relevant case to the future of copyrights on the Internet is the case against Grokster and StreamCast, two companies that produce P2P

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 the infringement of copyrights. 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 misuses 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 *International Herald Tribune* listed the following software-based tactics, used by recording/entertainment companies to protect their copyrights:

- a Trojan Horse, which redirects users to websites where they can legitimately buy the song they tried to download;
- "freeze" software that blocks computers for a period of time and displays a warning about downloading pirated music;
- "silence," where hard disks are scanned and an attempt is made to remove any pirated files found;

- "interdiction," preventing access to the Net for those who try to download pirated music.

Professor Lawrence Lessig, of the Stanford Law School, has warned that such measures might be illegal. He noted that among the measures passed to deal with copyright infringement, those specified above 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 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 the international level (WIPO Copyright Treaty) and in the DMCA Act. Moreover, the DMCA Act 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 ICT and Internet developments? One answer suggested by the US government White Paper on *Intellectual Property and the National Information Infrastructure* 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 Property 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 public interests. 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 usually defined as use for academic research and other non-commercial purposes.

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

Two main international regimes exist for intellectual property rights. The World Intellectual Property Organisation (WIPO) manages the traditional IPR regime, based on the Bern and the Paris conventions. Another emerging regime is run by 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. The 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, intellectual property rights. So far, the main focus of the WTO and TRIPS has been on various interpretations of IPRs for pharmaceutical products. It is very likely that future discussions will extend to IPRs 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 copyrights, if the material is not removed upon notification of infringement. This has made the previously vague IPR regime directly enforceable in the field of the Internet.

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 cyber-squatting, 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 Universal Dispute Resolution Procedure (UDRP). [17]

PATENTS

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

Some patents have been granted for business processes, and some of these were 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.[18] If British Telecom had won this case, Internet users would have to pay a fee for each hypertext link created or used. It is important to stress that the practice of granting patents to software and Internet-related procedures has not been accepted in Europe and other regions.[19]

CYBERCRIME

A dichotomy between "real" 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 are different. The cyberlaw 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.[20]

THE ISSUES

Definition of Cybercrime

The definition of cybercrime is one of the core issues of cyberlaw, 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 Cybercrime

Convention: 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.[21] 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 the 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 reviewed short-term contracts. This introduces a lower level of social protection of the workforce.

- Teleworking is becoming increasingly relevant with the further development of telecommunications, 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 Great Britain, 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.

NOTES

[1] One of the strongest supporters of the "real law" approach is Judge Frank Easterbook 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.; **http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf**. Judge Frank Easterbrook's argument provoked several reactions, including one from Lawrence Lessig in *The Law of the Horse: What Cyberlaw Might Teach*; **http://www.lessig.org/content/articles/works/finalhls.pdf** (accessed on 14 November 2008).

[2] 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.

[3] There is a high frequency of the use of the word "should" in the WSIS documents, one of the features of soft law instruments. For more information consult: Jovan Kurbalija, *The Emerging Language of ICT Diplomacy—Qualitative Analysis of Terms and Concepts,* DiploFoundation,

[4] Article 53 of the 1969 Vienna Convention on the Law of Treaties.

[5] Ian Brownlie, *Principles of Public International Law,* 5th Ed. (Oxford: Oxford University Press, 1999), p. 513.

[6] For more information see:

- Richard Paul Salis, *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**.
- Jonathan Zittrain, *Jurisdiction in Cyberspace,* Internet Law Program, available at: **http://cyber.law.harvard.edu/ilaw/mexico_2006_module_9_jurisdiction**.
- 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 City, May 8, 2002): **http://www.howardrice.com/uploads/content/jurisdiction_internet.pdf**. (accessed on 14 November 2008).

[7] Among the most important resources in this field is the *Princeton Principles on Universal Jurisdiction* (2001): **http://www1.umn.edu/humanrts/instree/princeton.html** (accessed on 14 November 2008).

[8] Peter Malanczuk, *Akehurst's Modern Introduction to International Law* (London: Routledge, 1997), p. 113.

[9] For an overview of cases involving extraterritorial jurisdiction related to Internet content, see Yulia A, Timofeeva, Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis, *Connecticut Journal of International Law,* 20, p. 199, 2005, available at: **http://ssrn.com/abstract=637961** (accessed on 14 November 2008).

[10] Other court cases include the German Federal Court of Justice case against Fredrick Toben, former German national with Australian nationality who had posted at an Australian-based website, materials questioning the existence of the holocaust: **http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html** (accessed on 14 November 2008).

[11] For a following of the case development, see: **http://www.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/** (accessed on 14 November 2008).

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

[13] The full text of the convention is available at: **http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html** (accessed on 14 November 2008).

[14] 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).

[15] *Uniform Domain Name Dispute Resolution Policy,* The Internet Corporation for Assigned Names and Numbers, 26 August 1999: **http://www.icann.org/udrp/udrp-policy-24oct99.htm** (accessed on 14 November 2008).

[16] Other IPRs include: designs, utility models, trade secrets, geographical indications and plant varieties.

[17] For a comprehensive survey of the main issues involving UDRP please consult: "WIPO's Overview of WIPO Panel Views on Selected UDRP Questions" at: **http://arbiter.wipo.int/domains/search/overview/index.html** (accessed on 14 November 2008).

[18] CNET News.com. Loney, M., "Hyperlink patent case fails to click" at: **http://news.com.com/2100-1033-955001.html** (accessed on 14 November 2008).

[19] For more information about the debate in Europe on software patentability, please consult: http://swpat.ffii.org and **http://www.eubusiness.com/Rd/patents.2006-02-02**

[20] For the text of the convention, please consult: **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm** (accessed on 14 November 2008).

[21] For critical views about the Cybercrime Convention expressing the concern of civil society and human rights activists, please consult:

- The Association for Progressive Communication Report on the Cybercrime Convention: **http://rights.apc.org/privacy/treaties_icc_bailey.shtml**.
- TreatyWatch.org website at **http://www.treatywatch.org/** (accessed on 14 November 2008)

SECTION 4

The Economic Basket

THE ECONOMIC BASKET

E-COMMERCE

E-commerce has been one of the main engines promoting the growth of the Internet over the last ten years. The importance of e-commerce is illustrated by the title of the document that initiated the reform of Internet governance and established ICANN: "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

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 WTO defines e-commerce more precisely as: "the production, distribution, marketing, sale, or delivery of goods and services by electronic means." The World Customs Organisation defines e-commerce as: "a way of conducting business by utilising computer and telecommunications technology to exchange data between independent organisational computer information systems in order to complete a business transaction."

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 the international level, an increasing number of initiatives and regimes is related to e-commerce.

THE WTO AND E-COMMERCE

The key policy player in modern global trade, the World Trade Organization (WTO), regulates many relevant e-commerce issues, including telecommunication liberalisation, intellectual property rights, and some aspects of 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.[2]
- Dispute resolution mechanism. E-commerce was particularly relevant in the USA/Antigua Online Gambling case.[3]

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) or goods (regulated by GATT)?

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 implication, because of the different regulatory mechanisms for goods and services.

What should be the link between TRIPs and the protection of IPRs on the Internet?

Since the WTO's TRIPS agreement (Trade-Related Aspects of Intellectual Property Rights) provides much stronger enforcement mechanisms for IPRs, 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 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 European Union has carried out a broad set of actions in the field of e-commerce, its main focus being on small and medium enterprises (SMEs).[4] The OECD's activities touch on various aspects related to e-commerce, including customer protection and digital signatures. The OECD emphasises promotion and research regarding e-commerce through its recommendations and guidelines.

UNCTAD is particularly active in research and capacity-building, focussing 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, 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 the international and the national context.

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 cyber security. 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.

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. Jurisdiction 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.

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 OECD established the main principles, now adopted by other business associations, including the International Chamber of Commerce 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 the 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 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

After Faraday discovered the basic principle of electricity in 1831 (electromagnetic induction), a sceptical politician asked him what electricity was good for. Faraday responded with, *"Sir, I do not know what it is good for. But of one thing I am quite certain, some day you will tax it."*[5]

The Internet governance dilemma of whether cyber-issues should be treated differently from real-life issues is clearly mirrored in the question of taxation.[6] Since the early days, the US has been attempting to declare the Internet a tax-free zone. In 1998, the US Congress adopted the Tax Freedom Act, which was 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.[7]

The OECD and the EU have promoted the opposite view, 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, the EU introduced a new law in 2003 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 US 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 US. 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 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.[8]

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, New Zealand, and Australia.

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 the two above-mentioned approaches.[9] It has a minimalist provision for the recognition of signatures supplied via an electronic medium. The maximalist approach is also recognised through grant-

ing that "advanced electronic signatures" will have stronger legal effect in the legal system (e.g. easier to prove these signatures in court cases). The EU regulation on digital signatures was one of the responses at the multilateral level. While it has been adopted in all EU member states, a difference in the legal status of digital signatures still remains.

At the 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. The International Chamber of Commerce (ICC) issued a "General Usage in International Digitally Ensured Commerce" (GUIDEC), which provides a survey of the best practices, regulations, and certification issues.[10] Directly related to digital signatures are Public Key Infrastructure (PKI) initiatives. Two organisations, the ITU and the IETF, 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. Digital signatures are just one of the important techniques (but not the only one) for the identification of individuals on the Internet.[11] For instance, SMS authentication via mobile phones is used by banks for approving the online transactions of customers, in some countries where the digital signature legislation or standards and procedures have not been set up yet.

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 (the ITU) and professional associations (the IETF and the EESSIO).

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 a 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 pre-condition 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, while 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 $1 in traditional banking, cost only $0.02 in Internet banking.[12] 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, already discussed during the course, is customer protection at the 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 its early stages of development. It has not been widely used, because of limited security and lack of privacy. E-money 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 micro-payments. 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 (BIS) 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. In the context of the recent financial crisis and attempts to re-gain control of financial system by governments, it is not very likely that experiments with e-money will be encouraged.

THE ISSUES

1. 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.[13] 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.

2. Cybersecurity is one of the main challenges to the wider deployment of e-payments. How can one ensure the safety of financial transactions via the Internet? Cybersecurity has been discussed in another part of this publication. 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.[14]

3. 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.

4. 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.[15] 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." Governments are also concerned about the potential use of e-money for money laundering.

5. 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 Euros/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, the main Web standardisation body, has ceased its e-commerce/micropayment activities, which was a setback to the global efforts towards standardisation in this field.[16]

6. 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 the 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 which are key issues for the introduction of e-money.[17]

7. 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.*[18] What the law enforcement authorities could not achieve through legal mechanisms, they could accomplish through the control of electronic payments.

NOTES

[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**; accessed on 14 November 2008).

[2] This section of the WTO website focuses on e-commerce: **http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm** (accessed on 14 November 2008).

[3] For more information about the USA/Antigua Online Gambling Case, please consult: **http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm** (accessed on 14 November 2008).

[4] For more information about EU's e-commerce initiatives, please consult: **http://europa.eu.int/information_society/eeurope/2002/action_plan/ecommerce/index_en.htm** (accessed on 14 November 2008).

[5] Source: Maastricht Economic Research Institute on Innovation and Technology (MERIT) **http://www.merit.unimaas.nl/cybertax/** (accessed on 14 November 2008).

[6] For a discussion on various aspects of taxation policy and the Internet, please consult:
- Arthur J. Cockfield, Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 MINN. L. REV. 1171, 1235-36 (2001);
- Edward A. Morse, State Taxation of Internet Commerce: Something New under the Sun?, 30 CREIGHTON L. REV. 1113, 1124-27 (1997);
- W. Ray Williams, The Role of Caesar in the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 WM. MITCHELL L. REV. 1703, 1707 (2001).

[7] "Making the 'Internet Tax Freedom Act' Permanent Could Lead to a Substantial Revenue Loss for States and Localities" by Michael Mazerov: **http://www.cbpp.org/7-11-07sfp.htm** (accessed on 14 November 2008).

[8] For a more detailed explanation of these three approaches, please consult: Survey of Electronic and Digital Signature Initiatives provided by the Internet Law & Policy Forum: **http://www.ilpf.org/groups/survey.htm#IB** (accessed on 14 November 2008).

[9] Directive 1999/93/EC by the European Parliament and Council on 13 December 1999 on a Community Framework for Electronic Signatures.

[10] GUIDEC (General Usage for International Digitally Ensured Commerce) by the International Chamber of Commerce: **http://www.iccwbo.org/home/guidec/guidec_one/guidec.asp** (accessed on 14 November 2008).

[11] Gavin Longmuir, "Privacy and Digital Authentication" (**http://caligula.anu.edu.au/~gavin/ResearchPaper.html** (accessed on 14 November 2008). This paper focuses on the personal, communal, and governmental aspects of the need for authentication in a digital world.

[12] Saleh M. Nsouli and Andrea Schaechter, "Challenges of the 'E-Banking Revolution'," Finance and Development (September 2002, Volume 39, Number 3), International Monetary Fund: **http://www.imf.org/external/pubs/ft/fandd/2002/09/nsouli.htm** (accessed on 14 November 2008).

[13] This article provides an introduction to online banking and a survey of the advantages and disadvantages in comparison to traditional banking: **http://www.bankrate.com/brm/olbstep2.asp** (accessed on 14 November 2008).

[14] For more information, please consult: Edwin Jacobs, "Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union": **http://www.arraydev.com/commerce/JIBC/2005-08/security.htm** (accessed on 14 November 2008).

[15] 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.

[16] For arguments against micro-payments, please consult: "The Case against Micropayments" by Clay Shirky: **http://www.openp2p.com/pub/a/p2p/2000/12/19/micropayments.html** (accessed on 14 November 2008).

[17] 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." Please consult: **http://www.bis.org/publ/cpss62.pdf** (accessed on 14 November 2008).

[18] For more information, please consult: **http://www.oag.state.ny.us/press/2002/aug/aug21a_02.html** (accessed on 14 November 2008).

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 the 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 the North and the 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. For example:

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

This chapter will focus exclusively on the core development issues, such as the digital divide and universal access, issues frequently raised in the development debate. It will be followed by an analysis of the main factors influencing the Internet and development: infrastructure, financial assistance, policy issues, and socio-cultural aspects.

How Does ICT Affect the Development of Society?

The main dilemmas about ICT and development were summarised in an article in *The Economist* ("Falling through the Net?," 21 September 2000).[1] The article proposes pro and con arguments for the thesis that ICT provides specific impetus for development.

ICT does NOT facilitate development	ICT facilitates development
• The "network externalities" help first-comers 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: "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 UNDP Human Development Report and the ILO's World Employment Reports.

Some opposing views argue that statistics on the digital divide are often misleading and that the digital divide 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 India and China.

UNIVERSAL ACCESS

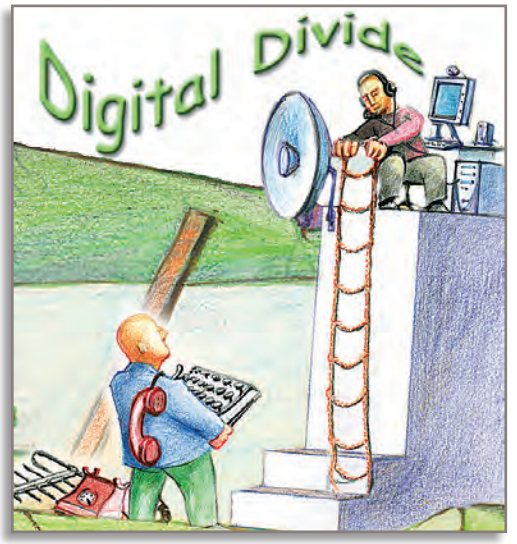
In addition to the digital divide, another frequently mentioned concept in the development debate is universal access, that is, access for all. Although it should be the cornerstone of any ICT development policy, differing perceptions and conceptions of the nature and scope of this universal access policy 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 the global level remains largely a policy issue, ultimately dependent on the readiness of developed countries to invest in the realisation of this goal.

Unlike universal access at the 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 self-sufficient precondition for development. Other elements include a regulatory framework, financial support, available human resources, and other socio-cultural conditions. Even if all of these ingredients are present, the key challenge remains of how and when they should be used, combined, and interplayed.



DEVELOPING TELECOMMUNICATIONS AND INTERNET INFRASTRUCTURES

The possibility of establishing connectivity is a precondition for bringing individuals and institutions to the Internet and ultimately overcoming the digital divide. Various possibilities for providing and improving connectivity are available.

The rapid growth of wireless communication provides many developing countries with a new chance. 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. Traditionally, the infrastructural aspect of the digital divide has been the focus of the International Telecommunication Union.

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 telecommunications market, a tendency for developing telecommunication infrastructures through foreign direct investment has grown. Many developing countries continuously struggle to attract private investment.

Currently, most Western telecommunication companies are in a consolidation phase, after accumulating huge debts for over-investing in the 1990s. While they are still reluctant to invest, it is widely expected that in the medium-term they will invest in developing countries, since the market in the developed world is over-saturated with huge capacities built up in the late 1990s.

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 an UN-administered Digital Solidarity Fund to help technologically disadvantaged countries build telecommunication infrastructures. However, the proposal to establish a Digital Solidarity

Fund did not garner broad support from the developed countries, which favoured direct investment instead of the establishment of a centralised development fund. After the WSIS, the Digital Solidarity Fund was established in Geneva as an independent foundation mainly supported by cities and local authorities worldwide.

SOCIO-CULTURAL ASPECTS

The socio-cultural aspect of digital divides encompasses a variety of issues, including literacy, ICT skills, training, education, and language protection.

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 brain drain, developing countries lose out in a number of ways. The main loss is in skilled labour. Developing countries also lose the investment in training and education of the migrating skilled labour. It is likely that brain drain will continue, given the various employment/emigration schemes that have been introduced in the US, 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 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 the 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 Diasporas in the field of ICT.

TELECOMMUNICATION POLICY AND REGULATION

Telecommunication policy issues are closely linked in many respects with overcoming the digital divide. First, both private investors and, increasingly, public donors are not ready to invest in countries without a proper institutional and legal environment for Internet development. Second, the development of national ICT sectors depends on the creation of necessary regulatory frameworks. Third, the existence of national telecommunication monopolies is usually indicated as one of the reasons for the higher cost of Internet access.

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 copyright, privacy, e-commerce, etc.), and the granting of access to all without political, religious, and other restrictions.

Debate about the impact of the liberalisation of the telecommunication market on development is centred on two dominant points of view. The first is that liberalisation has not benefited developing countries. With the loss of telecommunication monopolies, governments in the developing world lost an important source of income for their budgets. The lower budgets affected all the other sectors of social and economic life. According to this view, the losers are the governments of developing countries and the winners are the telecommunication companies from the developed world. The second view is that the opening of the telecommunication markets led towards more competition, bringing a higher quality of service and lower costs. Ultimately, this will lead to an efficient and affordable telecommunication sector, a pre-condition for the overall development of society.

NOTES

[1] "Falling through the Net?", The Economist, 21 September 2000

[2] 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. 11 May 2001 (available online at **http://www.g8italia.it/_en/docs/STUWX141.htm**; accessed on 14 November 2008).

[3] For more information regarding Network Neutrality, please consult the following study: Romina Bocache, Andrei Mikheyev, Virginia Paque: "The Network Neutrality Debate and Development." Internet Governance and Policy Discussion Papers, DiploFoundation, March 2007: **http://www.diplomacy.edu/poolbin.asp?IDPool=453** (accesed on 14 November 2008).

[4] European Union. Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) (available online at **http://ec.europa.eu/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00510077.pdf**; accessed on 14 November 2008).

[5] See: United Nations. Press Release PI/1490. Development Potential of Wireless Internet Technology Explored at Headquarters Conference Resolution adopted by the General Assembly 56/183. World Summit on the Information Society. 27 June 2003 (available online at **http://www.un.org/news/Press/docs/2003/pi1490.doc.htm**; accessed on 14 November 2008);
Larry Press. Wireless Internet Connectivity for Developing Nations// First Monday. Volume 8, number 9 (September 2003). (available online at **http://www.firstmonday.org/issues/issue8_9/press/**; accessed on 14 November 2008).

[6] More information about the Digital Diaspora Network initiative is available on UN ICT Task Force website at **http://www.unicttaskforce.org/stakeholders/ddn.html** (accessed on 14 November 2008).

SECTION 6

The Socio-Cultural Basket

THE SOCIO-CULTURAL 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 our social life that is not affected by the Internet. The Internet introduces new patterns of social communication, breaks down language barriers and creates new forms of creative expressions – to name but a few of its effects. Today, the Internet is increasingly becoming more of a social, as opposed to a technological, phenomenon. The socio-cultural basket includes IG issues such as content policy and multilingualism, reflecting the most prevalent national, religious and cultural differences of modern times.

HUMAN RIGHTS

The Internet has brought new forms of communication and interaction to society and ultimately has influenced traditional concepts of 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, among others. It is not surprising that human rights related issues have been very often hotly debated both in the WSIS and IGF processes. While human rights are usually explicitly addressed, they are also involved in cross-cutting issues appearing when dealing with issues such as net neutrality (right to access, freedom of expression, anonymity), cybersecurity (observing human rights while carrying out cybersecurity and protection activities), content control, etc. The WSIS recognized the importance of human rights, in particular the right to development and the right to the freedom of expression.

"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 "cyberlaw", 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. "New" human rights such as the right to communicate are being discussed as well.

Survey of Initiatives on Human Rights and the Internet

The main "cyber rights" initiative taking place currently is the Internet Bill of Rights (IBR), championed by Italy and civil society. The Internet Bill of Rights project triggered the process which is currently supported by the Internet Rights and Principles Dynamic Coalition (IPR, previously IBR http://internetrightsandprinciples.org/) and includes other developments such as Internet rights watch. The IBR has been discussed at all previous IGFs. In an attempt to delineate "cyber rights", the Association for Progressive Communication (APC) drafted an Internet Rights Charter.[1] Another predominantly academic initiative is the Networked Communications Freedom Charter proposed by the Faculty of Law at the University of Toronto.

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 the major Internet companies can directly affect the way human rights are protected.[2]

Right to Access the Internet
Finland is the first country to legally guarantee the right to access the Internet. As of July 2010 all citizens in Finland will have the right to a one-megabit broadband connection.

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 Council of Europe (CoE). The CoE is the core institution dealing with pan-European human rights, with the European Convention for the Protection of Human Rights and Fundamental Freedom (195)[3] as its main instrument. Since 2003 the Council of Europe has adopted several declarations highlighting the importance of human rights on the Internet.[4] 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.

The 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 the 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 UN Universal Declaration of Human Rights, the 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.

The freedom of expression is the particular focus of human rights 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 telecommunications 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 vigor, diversity, and activism of the new media domain in each country, regardless of—or despite—state efforts to restrict usage.[5]

Other Human Rights

The right to privacy is discussed on pages 135–139.

The rights of persons with disabilities are discussed on pages 142–143.

CONTENT POLICY

One of the main socio-cultural 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.

The first group consists of content that has a global consensus for its control. Included here are child pornography, justification of genocide, and incitement or organization of terrorist acts, all prohibited by international law *(ius cogens)*.[6]

The second group consists of 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.[7]

The third group consists of political censorship on the Internet. In 2007 "Reporters without Borders" reported that 13 countries perform political censorship on the Internet.[8]

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.[9] If a website is in the "Internet Index," access will not be granted. Technically speaking, filtering utilises mainly router-based IP blocking, proxy servers, and DNS redirection.[10] Filtering of content occurs in many countries. 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.[11]

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 and other like-minded institutions made proactive moves proposing the implementation of user controlled *rating and filtering systems*.[12] In these systems, filtering mechanisms are built-in to Internet browsers. A label indicates the accessibility of particular content in a particular website.

The use of this type of filtering is especially favoured in accessing "child friendly" websites.

Geo-Location Software

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.[13] 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.[14] With the introduction of IPv6 addressing formats, where each device connected to the Internet has its own address, geo-location will become even easier.

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.[15] The response of the Chinese information department ran thus: "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".[16]

To adjust to local laws, Google decided to restrict some materials on Google's 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.[17]

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. Manual review and labelling of content is impossible: it has been estimated that by mid-2006 YouTube contained over 6 millions videos, while the total time that people spent in watching these materials was over 9000 years![18]

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 what 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 ISPs, enforcement agencies and other players. In recent years, many countries have introduced content policy legislation.

International Initiatives

At the 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 on the Cybercrime Convention.

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 included 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.[19]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 the freedom of expression. This is especially important in the US, 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 US has signed the Cybercrime Convention, 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 US will not step beyond the line which may compromise the 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" and the "cyber" worlds. 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 the rules themselves.

The Effectiveness of Content Control

In discussions on Internet policy, one of the key arguments is that the decentralised nature of the Internet can bypass censorship. The Internet includes many techniques and technologies that can provide effective control. However, technically speaking, 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 R.H. Coase, "A regulation need not be absolutely effective to be sufficiently effective".

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. Lessing provides a concise statement of this problem: "*A regulation need not be absolutely effective to be sufficiently effective.*"

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. Internet service providers, 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). 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, Scienositter, to members, preventing access to websites critical of Scientology.[20]

PRIVACY AND DATA PROTECTION[21]

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 her own personal information and to decide about them (to keep or disclose information). Privacy is a fundamental human right. It is recognized in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and in many other international and regional human rights conventions.

National cultures and the way of life influence the practice of privacy. Although this issue is important in Western societies, it may have lesser importance in other cultures. Modern practices of privacy focus on communication privacy (no surveillance of communication) and information privacy (no handling of information about individuals). Privacy issues, which used to focus on governmental activities, has been extended and now includes the business sector, as depicted in *Figure 1.*[22]

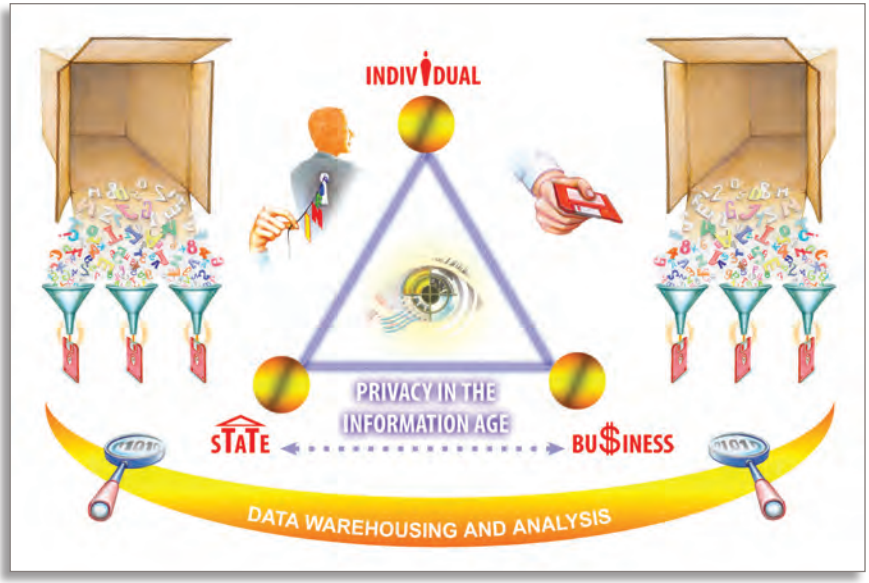


Figure 1. Privacy Triangle

Privacy Protection: 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, among others). 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 September 11, 2001 in the US, the US "Patriot Act" and comparable legislation in other countries broadened governments' authority to collect information, including a provision for lawful interception of information.[23] The concept of lawful interception in gathering evidence is also included in the Council of Europe's Convention on Cybercrime (Articles 20 and 21).

Privacy Protection: Individuals and Businesses

In the privacy triangle *(see Figure 1),* the second, and increasingly important relationship is that between individuals and the business sector. A person discloses her personal data when she opens a bank account, when she books a flight or a hotel, when she makes an online payment on her credit card, when she browses or searches on 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 corner-stone of their business model. The success and sustainability of electronic 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.[24] 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.

Privacy Protection: 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. However, in some situations, such as those to which the European Directive on Data Protection applies, the state supervises and protects data about individuals held by businesses.

Privacy Protection: Individuals and Individuals

The last aspect of privacy protection, not represented within the triangle of Figure 1, 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 "democratized 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.[25] 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 vast 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 Development and Co-Operation, "Guidelines on Protection of Privacy and Transborder Flows of Personal Data," from 1980. These guidelines and the organisation'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 diffeence is in the way they are implemented. The main difference is between the European and USA 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 (the Graham-Leach-Bliley Act)[26] and children's privacy (The Children's Online Privacy Protection Act)[27], and medical privacy (the proposed Health and Human Services regulations)[28].

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. Individuals are seldom aware of the importance of options offered by privacy policies and commonly agree to them without informing themselves.

Safe Harbour Agreement between USA and EU

These two approaches – USA 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 US's) is data transferred through a company's network from the EU to the US 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-regulation 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 Harbour" 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 US.

When it was signed in 2000 "Safe Harbour" 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 protecting sufficiently 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 Harbour Framework, only 348 meet the basic requirements (e.g. privacy policy).[29] Given the high importance of privacy and data protection in the European Union, it is likely to expect higher pressure to find some solution for the dysfunctional "Safe Harbour" 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.[30] 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

First, 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 and IETF took an important step in promoting Internationalised Domain Names (IDN). IDN should facilitate the use of domain names written in Chinese, Arabic and other non-Latin alphabets.

Second, 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.

Third, the promotion of multilingualism requires appropriate governance frameworks. The first element of governance regimes has been provided by organizations such as UNESCO. 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 Web2.0 tools, allowing ordinary users to become contributors and content developers easily, 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".[31]

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 harmonization 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" 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 standardization, 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) 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[32]

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 criterion: non-rivalrous consumption and non-excludability.

RIGHTS OF PERSONS WITH DISABILITIES[33]

The UN estimates that there are 500 million persons 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.[34] 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.[35]

Awareness of the need for technological solutions that include the persons with disabilities is increasing with the work of organizations that teach and foster support for the disabled community, such as the IGF Dynamic Coalition on Accessibility and Disability[36] and the Internet Society Disability and Special Needs Chapter.[37]

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

design and development of equipment, software and content,, and second, to 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 the Word Wide Web Consortium (W3C) which calls them "Web Content Accessibility Guidelines (WCAG)"[38]

One policy action that should increase the access of people with disabilities is ISOC's "Universal Design for the Internet", which is defined as:

"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."[39]

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 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 the 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 WTO negotiations is the interpretation of Articles 1 (3) (b) and (c) of the General Agreement on Trade in Services, which specify exceptions from the free trade regime for government provided services. According to one view, supported mainly by the US and 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 organizations, will focus on the dilemma of education as a commodity or a public good. If education is considered a commodity, the 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

Recognition of degrees has become particularly relevant within the online learning environment. When it comes to online learning, the main challenge is the recognition of degrees beyond the regional context, mainly at the 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 Standardization of Online Learning

The early phase of online learning development was characterized 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 standardization is performed in the US by private and professional institutions. Other, including international, initiatives are on a much smaller scale.

CHILD SAFETY ONLINE[40]

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

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

Abuse and Sexual Exploitation. The 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, the "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 the abuse and exploitation of children, paedophilia and 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 becoming dominant over the "passively" violent movies.

The impact of the violence of these games on the behaviour of young people is being 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, were 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 on how to use ICT - they know more, yet they understand less. Close peers-parents-educators-community cooperation is thus of the utmost importance. Parents, policy-makers and the wider community worldwide are, nevertheless, slowly becoming aware of the situations mentioned above, and increasingly creating initiatives for safeguarding children in computer-mediated environments.

To raise the awareness among the stakeholders, the European Commission has launched the InSafe project as 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 cyber-bullying resulted in sets of video clips and an e-Learning course on Internet safety for kids. NetSafe initiative in New Zealand, founded in 1998, is among the first national initiatives on Internet safety, which gathers the key stakeholders including ministries, business sector and media.

Certainly among the most successful models of national awareness and training campaigns is the Cyber-Peace Initiative (CPI) of Egypt, under the auspices of the Suzanne Mubarak Women's International Peace Movement. A group of young enthusiasts titled "Net-Aman", as well as a group of parents' representatives, have been formed and 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, they have reached out to tens of thousands of youth and parents around the country within the past few years. Additionally, they have produced several awareness and educational kits for kids, parents and educators, translated into Arabic. Having the forthcoming IG forum meeting in Egypt in 2009, it is likely that the model might get more visibility and get replicated to other countries as well.

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, non-governmental organisations etc.. Various international organisations are currently discussing possible models of cooperation in establishing such programmes, among which also are the Council of Europe, the International Telecommunications Union (ITU), CPI and DiploFoundation.

On a longer time scale educational curriculum updates would be needed as well, to include in school programmes Internet safety issues such as: protecting personal privacy and security, minding 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 as well. A very recent example is a successful pan-European "Prague Declaration for a Safer Internet for Children" adopted at the Ministerial Conference (Prague, April 2009). The Global Cybersecurity Agenda (GCA) of the ITU presents the Child Online Protection (COP) initiative as its integral part. Besides, there are many other international *fora* where child protection is a debated issue high on the agenda, including the IG Forum with its Dynamic Coalition on Child Online Safety.

International cooperation in the field of child protection has already been successful for a long time 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 non-government organisations 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.

NOTES

[1] The ACP 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. For more information visit: **http://www.apc.org/en/node/5677**

[2] For more information see: **http://www.globalnetworkinitiative.org**

[3] (**http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm**)

[4] 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 (28th May 2003, The Declaration on Human Rights and the Rule of Law in the Information Society (13th May 2005)

[5] For more information consult: **http://www.freedomhouse.org/uploads/specialreports/NetFreedom2009/FreedomOnTheNet_FullReport.pdf**

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

[7] For a discussion of Internet gambling, see: Jenna F. Karadbil (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.

[8] See "Internet Under Surveillance:" **http://www.rsf.org/rubrique.php3?id_rubrique=433** (accessed on 14 November 2008).

[9] Jonathan Zittrain and Benjamin Edelman, Documentation of Internet filtering worldwide (Open Net Initiative): **http://cyber.law.harvard.edu/filtering/** (Accessed on 14 November 2008).

[10] Chinese authorities use IP blocking. Official Saudi filtering is provided through "a proxy farm system." For more information, see: **http://www.isu.net.sa/saudi-internet/contenet-filtring/filtring-mechanism.htm** (accessed on 14 November 2008).

[11] See: Electronic Frontiers, Australia, "Internet censorship in Australia" (20 December 2002), **http://www.efa.org.au/Issues/Censor/cens1.html** (accessed on 14 November 2008).

[12] For more information about Platform for Internet Content Selection (PICS), see: **http://www.w3.org/PICS/iacwcv2.htm** (accessed on 14 November 2008).

[13] 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" (source: "Welcome to the world wide web, passport, please?" (*New York Times,* 15 March 2001; **http://www.quova.com/page.php?id=33&coverage_id=86** (accessed on 14 November 2008).

[14] 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 its 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" (source: "Rise of internet borders prompts fears of web's future" by Arianna Eunjung Cha, *Washington Post,* January 4, 2002, p. E01).

[15] For a survey of articles about the Google-China Case, see: **http://searchenginewatch.com/sereport/article.php/2165031** (accessed on 14 November 2008).

[16] Published in the *New Scientist* Internet edition: **http://www.newscientist.com/news/news.jsp?id=ns99992797** (accessed on 14 November 2008).

[17] See Jonathan Zittrain and Benjamin Edelman, Localised Google search result exclusions: statement of issues and call for data: **http://cyber.law.harvard.edu/filtering/google/** (accessed on 14 November 2008).

[18] The *Wall Street Journal* article on "Will all of us get our 15 minutes on a YouTube video?" by Lee Gomes: **http://online.wsj.com/public/article/SB115689298168048904-5wWyrSwyn6RfVfz9NwLk774VUWc_20070829.html?mod=rss_free** (accessed on 11 April 2008).

[19] EU Information Society, "Safer internet action plan:" **http://europa.eu.int/information_society/programmes/iap/index_en.htm** (accessed on 14 November 2008).

[20] See: Church of Scientology censors net access for members at **http://www.xenu.net/archive/events/censorship** (accessed on 14 November 2008).

[21] Valuable comments and inputs were provided by Katitza Rodriguez.

[22] A report issued by the American Civil Liberties Union: Jay Stanley. (2004). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society. This report explains the problem of the privatisation of surveillance and new challenges linked to the protection of privacy: **http://www.aclu.org/FilesPDFs/surveillance_report.pdf** (accessed on 14 November 2008).

[23] See the text of the Patriot Act at: **http://www.epic.org/privacy/terrorism/hr3162.html** (accessed on 14 November 2008).

[24] For a discussion of customer trust in business privacy protection, see: Rick Whiting (August 19, 2002). Wary customers don't trust business to protect privacy, *Information Week:* **http://www.informationweek.com/shared/printableArticle.jhtml?articleID=6503045** (accessed on 14 November 2008).

[25] Gramm-Leach-Bliley Act, *Public Law* (1999): **http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106** (accessed on 14 November 2008).

[26] Children's Online Privacy Protection Act of 1998: **http://www.ftc.gov/ogc/coppa1.pdf U.S.C. §§ 6501-6505** (accessed on 14 November 2008).

[27] 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, **http://www.epic.org/privacy/medical/HHS_medical_privacy_regs.html** (accessed on 14 November 2008).

[28] Council of Europe, Convention for the protection of individuals with regard to the automatic processing of personal data, ETS No. 108: **http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm** (accessed on 14 November 2008).

[29] Galexia, the US Safe Harbour – Fact or Fiction?, 2008

[30] For more information regarding multilingualism on the Internet please consult the following study: Qusai AlShatti, Raquel Aquirre and Veronica Cretu. *Multilingualism – the communication bridge.* DiploFoundation's Internet Governance Research Project, 2006/2007 (**http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241**; accessed on 15 April, 2008).

[31] On English content on the Internet, Wikipedia: **http://en.wikipedia.org/wiki/English_on_the_Internet#Internet_content** (accessed on 15 April, 2008)

[32] For more information regarding the Internet as a global public good, please consult the following study: Seiiti Arata and Stephanie Psaila. *Protection of Public Interest on the Internet.* DiploFoundation's Internet Governance Research Project, 2005/2006: **http://www.diplomacy.edu/ig/Research/display.asp?Topic=Research%20Themes%20II#Protection**

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

[34] **http://www.hrea.org/index.php?base_id=152**

[35] See: **http://www.un.org/disabilities/**

[36] See: **http://www.intgovforum.org/cms/index.php/dynamic-coalitions/80-accessibility-and-disability and http://www.itu.int/themes/accessibility/dc/**

[37] See: **http://www.isocdisab.org**

[38] See: **http://www.w3.org/TR/WCAG10/**

[39] See: **http://www.isoc.org/briefings/002/isocbriefing02.txt**

[39] 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 its multistakeholder participation. This multistakeholder facet is natural in discussions on Internet governance, since non-state actors played predominant roles in the development and the management of the Internet. Civil society and, particularly academia, were vital players in the Internet field, including the development of Internet protocols, creating content and developing online communities. The business community developed the technological infrastructure, including computers, networks, and software in response to emerging needs. Governments were newcomers to the field of Internet governance.[1]

The major difference between Internet governance negotiations and other global negotiations, such as environmental negotiations is that, while in other negotiations, inter-governmental regimes gradually opened to non-governmental players, in Internet governance negotiations, governments had to enter an already existing non-governmental regime, built around ICANN. Once Internet governance became a global issue, there was a need to converge these two regimes (non-governmental and traditional diplomatic regimes) 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 WSIS process (2003-2005). The WGIG was more than an expert, advisory group, but less than a decision-making body.[2] It did not produce official UN documents, but it substantially influenced WSIS negotiations on Internet governance. The WGIG was a compromise in which pro-ICANN governments let Internet governance issues officially emerge on 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 the WGIG.

As follow-up to the WSIS, Internet governance will remain on the global agenda through the Internet Governance Forum, whose fourth meeting will be held in November 2009 in Sharm el Sheikh, Egypt. The first was held in Athens, Greece, in 2006, the second in Rio de Janeiro, Brazil in 2007 and the third in Hyderabad, India in 2008.

The IGF follows the WGIG participation structure. Both the WGIG and the IGF will remain useful examples for the future development of multi-stakeholder partnerships on the international level.

In the following text, the role of the main stakeholders will be discussed. It will start with actors who were officially recognised by the WSIS and WGIG process, including governments, international organisations, civil society, and the business sector. The survey will also briefly analyse the role of other key stakeholders, mainly the Internet community and ICANN.

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:[3]

- 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."

GOVERNMENTS

The last six 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 posed numerous challenges, such as management of the multidisciplinary nature of Internet governance (technological, social, economic, and social aspects) and involving a wide variety of actors. On the go, while they were grasping the new issue, many governments had to train officials, develop the policy, and actively participate in various Internet governance *fora*. In this section, we will address the main challenges for governments in the field 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 is more than "wires and cables", governments started involving officials from other, less technical ministries, such as those of culture, media and justice. The multi-faceted nature of Internet governance also implied a wide diversity of bodies addressing Internet governance issues, such as ICANN and technical standardisation organisations.

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 that had 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.[4]

Policy Coherence

Given the multi-disciplinary nature of Internet governance and the high diversity of actors and policy fora, it is particularly challenging to achieve policy coherence. It is a management challenge that will require 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 strong hierarchy, could be an obstacle for the development of such flexible coordination.

"Cable Geo-Strategy" & 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 main reason for this was 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."[5]

Apart from management challenge, the achieving of 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, net 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 of net neutrality and the telecommunication/entertainment sector (Verizon and AT&T, Hollywood lobby), which sees net neutrality 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. Many diverse policy fields (telecommunication, broadcasting) will have to converge in order to follow technological convergence.

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, the base for the ITU, which played the main role in the processes. The first WSIS Summit 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 Geneva.

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 the WSIS along with other issues such as human rights, health, trade, and labour.

"Diplomatisation" of Internet Governance Process

Also relevant to the positions of governments at the WSIS was that this summit put the Internet on the global diplomatic agenda. Prior to the WSIS, the Internet had been discussed primarily in non-governmental circles or at the 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.[6]

The diplomatisation process had certain positive effects on the discussions at the WSIS. For example, diplomats provided non-partisan contributions to long-standing debates on issues related to the Internet Corporation for Assigned Names and Numbers (ICANN) (domain names, Internet numbers, and root servers). The contributions of diplomats were particularly noticeable in the WGIG debate. The diplomatic leadership of the WGIG (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 the future discussion by establishing the Internet Governance Forum.

POSITION OF THE UNITED STATES GOVERNMENT

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 Defence, 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 United States to Geneva. This process was stopped by a famous, at least in the history of the Internet, diplomatic note sent by US Secretary of State Madeleine Albright to the Secretary General of the ITU.[7] 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 an intention to withdraw from the supervision of ICANN, once ICANN achieves institutional and functional robustness. This withdrawal process was initiated at the beginning of October 2009 with signing of the "Affirmation 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 contract – will be reviewed in 2011.

On the global scene, during the WSIS process, the US opposed a possible take-over of ICANN's functions by an inter-governmental body. However, in the WSIS process the US government made the first steps towards internationalisation of the role of ICANN by recognising the right of

national governments over their respective domain names and accepting the continuation of international discussions through the establishment of the Internet Governance Forum.

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 inter-governmental organisation, such as the ITU, should govern the Internet. This was the initial position of many developing countries. The most vocal in advocating a prominent role for the ITU were China, Iran, Russia, and Brazil. Some of developing countries argued for creating a new international organisation to replace the ITU, including the establishment of a new treaty-based organisation, such as the International Organisation on the Internet. 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 gradually taken by the European Union. On the other side of the policy spectrum the US argued that nothing in the current ICANN-based regime needed change. Canada, Australia, and New Zealand offered similar views, additionally arguing for greater internationalisation of ICANN. Those countries, together with the European Union, Switzerland, and a few developing countries have been significant in achieving compromise solutions on Internet governance during the WSIS process.

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" structure for Internet governance issues.[8] 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[9]

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 cyber-squatting 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, the protection of trademarks was immediately addressed after the creation of ICANN.[10]

Today, with the growth of the Internet, the interest of business in Internet governance has become wide and diverse, with the following main groups of business companies: domain name companies, Internet service providers, telecommunication companies, software developers, and Internet content companies.

The International Chamber of Commerce (ICC), well known as the main 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 processes. The ICC was actively involved in the early WGIG negotiations and the WSIS, and continues to be an active contributor in the current IGF process as well.

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 to reduce the risk of a potential take-over of ICANN's role by other players, mainly national governments and international organisations.

Internet Service Providers (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 on the national level in dealing with government and legal authorities. On the global level, some ISPs particularly from the US and Europe have been active in the WSIS/WGIG/IGF processes individually, even more so through the ICC and its BASIC initiative, and through national and regional or sector-specific business organisations such as ETNO, ITAA and others.

Telecommunication companies facilitate Internet traffic and run the Internet infrastructure. The main players include companies such as Verizon and AT&T. Traditionally, telecommunication companies have been participating in international telecommunication policy through the ITU. They have been increasingly involved in the activities of ICANN and 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 such as Microsoft, Adobe, and Oracle are mainly involved in the activities of different standardisation bodies (W3C, 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. As one of the representatives of the business sector indicated, business was involved in "damage control." After it was clear that the WSIS would not move in the IPR-field, the software companies' interest in participating in the WSIS process diminished. This trend has continued after the WSIS.

The last group of players is labelled *"Internet content companies"* and it includes the main Internet brand names such as Google, Yahoo! and Facebook. 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 the global Internet governance processes.

CIVIL SOCIETY

Civil society has been the most vocal and active promoter of a multi-stakeholder approach to Internet governance. The usual criticism of civil society participation in previous multilateral fora 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,

WSIS has relatively low participation of the main NGOs (registered with the UN ECOSOC). Out of close to 3000 NGOs with the consultative status with the UN ECOSOC, only 300 NGOs participated in the WSIS.

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.

At the WGIG, civil society attained a high level of involvement due to its multistakeholder nature. Civil society groups proposed eight candidates for the WGIG meetings, all of whom were subsequently appointed by the UN Secretary General. In the Tunis phase (the second phase of the WSIS, after Geneva), the main policy thrust of civil society organisations shifted to the WGIG, where they influenced many conclusions as well as the decision to establish the Internet Governance Forum as a multistakeholder space for discussing Internet governance issues. Civil society has continued to be actively involved in the IGF activities.

INTERNATIONAL ORGANISATIONS

The ITU was the central international organisation in the WSIS process. It hosted the WSIS Secretariat and provided policy input on the main issues. The ITU involvement in the WSIS process was part of its on-going attempt to define and consolidate its new position in the fast-changing global telecommunications arena, increasingly shaped by the Internet. The ITU role has been challenged in various ways. The ITU 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 IP) further reduced the ITU's "regulatory footprint" in the field of global telecommunications.

The possibility that the ITU might have emerged from the WSIS process as the *de facto* "International Internet Organisation" caused concern in the US and some developed countries, while garnering support in some developing countries. Throughout the WSIS, this possibility created underlying policy tensions. It was particularly clear in the field of Internet governance, where tension between ICANN and the ITU had existed since the establishment of ICANN in 1998. The WSIS did not resolve this tension. With the increasing convergence of various communica-

tion technologies, it is very likely that the question of the more active role of the ITU in the field of Internet governance will be re-emerging in policy discussion.

Another issue concerned the anchoring 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, which addresses issues such as multilingualism, cultural diversity, knowledge societies, and information sharing. The balance between the ITU and other UN organisations was carefully managed. The WSIS follow-up processes also reflect this balance, with the main players including the ITU, UNESCO, and the United Nations Development Programme (UNDP).

OTHER PARTICIPANTS

In addition to the formal stakeholders at the WSIS, other players – the Internet community and ICANN – who were not officially recognised as stakeholders participated in the process mainly through the civil society and business sectors.

THE INTERNET COMMUNITY

The Internet community consists of institutions and individuals who 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 commu-

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.

nity.[11] 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 it did not have any strict regulation and formal structure, the early Internet communities were governed by strong custom and peer-to-peer pressure. Most of participants in this process shared similar values, appreciation systems, and attitudes.

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 understandings of the Internet and its governance, which led to increasing tension. For example, in the 1990s, Internet communities and Network Solution were involved in a so-called DNS war, a conflict over the control of the root server and domain name system.

Today, the Internet community is represented through the Internet Society (ISOC) and the Internet Engineering Task Force (IETF). The Internet Society (ISOC) has played a vital role in Internet standardisation and the promotion of the Internet 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 one of the important actors in the process of both establishing and running ICANN. One of the founders of the Internet, Vint Cerf, was the Chair of the ICANN Board. Members of the Internet community hold important positions in various ICANN decision-making bodies.

Another criticism focuses on the fact that, with 1.5 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 only Internet-users, frequently described as the Internet community. Particularly 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 challenge. It is very likely that the members of the Internet community will gradually integrate into the core stakeholders 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 that the Internet community has been promoting: openness, knowledge sharing, and the protection of the interests of Internet users.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS

The Internet Corporation on Assigned Names and Numbers (ICANN) is the main Internet governance institution. Its responsibility is to manage the Domain Name System (DNS), 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 World Summit on Information Society (WSIS), held between 2003 and 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." The 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 of the digital divide.

ICANN is a non-profit corporation registered in California. Its functional authority rested on a Memorandum of Understanding between the US Department of Commerce (DOC) and ICANN, initially signed in 1998 and extended twice, the second time from September 2006 to September 2009. As of October 1, 2009 the formal basis for ICANN's function is the "Affirmation 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. The first group consists of actors that have been involved since the days when ICANN was established. It includes the Internet community, the business community, and the US government. The second group consists of international organisations, with the most prominent role played by the International Telecommunication Union (ITU) and the World Intellectual Property Organization (WIPO). The third group of ICANN actors consists of national governments whose increasing interest in having a bigger role in ICANN started in 2003 with the WSIS process. The fourth group includes Internet users (at-large community). ICANN has experimented with various approaches in order to involve Internet users. In the early days of ICANN, the first attempt was to involve Internet users through direct elections of their representatives at the 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 going on now.

The decision-making process in ICANN 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 users of the Internet. 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 check-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 the activities of ICANN. 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.[12]

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. The debate over whether the "xxx" (adult materials) domain should be introduced clearly indicated that ICANN will have to deal with public policy aspects of technical issues.

International Status of ICANN

The special ties between ICANN and the US government have been the major focus of criticism, which takes two main forms. The first form rests on principle considerations, stressing that the vital element of the global Internet infrastructure, which could affect all nations, is 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 US 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 internationalisation of Internet governance.

The second group of arguments for the internationalisation of the ICANN status 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 the 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 "Affirmation Commitments" by US Department of Commerce and ICANN. It provides the basis for an independent ICANN and opens a new set of issues about the 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 in ICANN's status 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.

NOTES

[1] The exception was the government of the United States and a few developed countries (Australia, New Zealand and, at that time, the European Commission).

[2] The selection of the members of the WGIG 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, the selected members were supposed to be knowledgeable about the subject in order to contribute substantially to the WGIG discussion.

[3] See: World Summit on the Information Society, "Declaration of Principles," WSIS-03/GENEVA/DOC/4-E, 12 December 2003, Article 49.

[4] 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 IGF-2007, which was hosted in Rio de Janeiro.

[5] Charles Lesage, La rivalite franco-britannique. Les cables sous-marins allemands (Paris, 1915) p. 257-258; quoted in: Daniel R. Headrick, The Invisible Weapon: Telecommunications and International Politics 1851-1945 (Oxford University Press: 1991), p. 110.

[6] Cukier, K. N. (2005). The WSIS wars: an analysis of the politicization of the Internet. In: D. Stauffacher and W. Kleinwächter (eds). *The World Summit on the Information Society: moving from the past into the future.* New York: United Nations ICT Task Force, p. 176.

[7] In a telegram, the US government criticised ITU involvement in the establishment of CORE: "without authorization of member governments to hold a global meeting involving an unauthorized expenditure of resources and concluding 'international agreements.'"

[8] The convenience of "one stop shopping" was one of the arguments for establishing the ITU as the central Internet governance player.

[9] Valuable comments were provided by Ayesha Hassan.

[10] Establishment of the Universal Dispute Resolution Procedures (UDRP).

[11] 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." (Peter Haas (1990), *Saving the Mediterranean: the politics of international environmental co-operation* (New York: Columbia University Press, p. 55).

[12] See: **http://cyber.law.harvard.edu/is99/governance/introduction.html#_ftn10** (accessed on 14 October 2009)

SECTION 8

Annex

ANNEX I

FOURTEEN LESSONS FROM THE INTERNET GOVERNANCE FORUM

The Internet Governance Forum (IGF - the principal global body in the field of Internet governance) has introduced some innovative approaches in managing global policy processes. Some of these may be useful for other policy areas which involve many stakeholders (for example, climate change, migration, trade, human rights). When discussing lessons learned from the IGF experience, it is important to keep in mind one significant difference between Internet governance (IG) and other global policy processes. While other policy processes such as climate change have gradually opened to non-governmental players, in the case of Internet governance, governments were obliged to enter an already existing non-governmental, ICANN-based regime. The IGF has been one of the important elements in this process. Relevant experience from the IGF process is summarised in the following fourteen insights.

1. Lead Effectively: "Sage on the Stage & Guide on the Side"

One of the main reasons for the success of the IGF is the exceptional leadership of Nitin Desai, Chair of the IGF, and Markus Kummer, Executive Coordinator of the IGF Secretariat. Mr Desai and Mr Kummer make a highly efficient team,

Nitin Desai and Markus Kummer

complementing each others' approaches and skills. Both have considerable diplomatic experience: Mr Desai was in charge of the preparation of several major UN summits; Mr Kummer has had a successful career in Swiss diplomacy. While Mr Desai was managing "the stage" of the IGF main events, Mr Kummer has been building understanding and inclusiveness through timely online, off-stage communication and participation in the 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 implement the effective, although unwritten, *modus operandi* of the IGF. Mr Desai explains one element of the IGF's success as follows: "For the dialogue to work all the participants have to recognize that the value of this forum is the presence of the others; but to realize this value everyone must adjust their expectations of how others should behave and, above all, listen rather than just talk."

As newcomers in the IG field, Mr Desai and Mr Kummer provide a non-partisan contribution to long-standing debates on issues related to ICANN (domain names, Internet numbers and root servers). Their success has also challenged the "urban diplomatic myth" that technical issues must be managed by technical experts. **Sometimes, as this case shows, the "diplomatisation" of dealing with technical issues can help overcome traditional disputes in specialised technical communities and move the policy process forward.**

2. Build Trust through Proper Timing and Sequencing

The IGF process has gathered people from vastly diverse professional and cultural backgrounds around the same table. Participants do not have a previous history of working for the same institutions, attending the same universities, moving in the same social circles, and other basic elements of trust-building. Trust had to be built in an atmosphere where suspicions were already present either due to past disputes (such as that between ITU and ICANN), to a general feeling of "geo-suspicion" caused by the Iraq War, or to the simple human reaction of "us" versus "them".

Trust-building requires patience and careful sequencing of activities. Each phase of the IGF process was aimed at increasing mutual understanding, and bringing new knowledge and information. The result was a gradual building of trust as well as a highly informed debate. Some proposals, such as an early call to adopt the Framework Convention on the Internet, were rightly declined: the time was not ripe for further formalisation of the Internet governance field. As the recent decision of the US government on the future of ICANN illustrates, some issues can be ameliorated by the passage of time, if they are handled carefully and not allowed to degenerate into a policy crisis. The IGF has been very

successful in this respect. **Diplomats and policymakers can learn from the IGF about effective trust-building through time and careful sequencing, and also about time and timing in policy processes in general.**

3. Let the Policy Process Evolve

Closely related to timing is the importance of letting processes evolve through their own momentum rather than relying too much on detailed planning. Today, there is an obsession for creating logically consistent schemes and measuring input/outcome. Over-managing processes in this way can be counter-productive, because social reality is too complex to be forced into a Procrustean bed of models and schemes. The recent global financial crisis provides an example of how a system based mainly on science and modelling can lead to collapse, if it does not consider the complexity of human beings, with all their weaknesses and strengths.

Relaxed Protocol at the Congress of Vienna (1814)

In diplomacy, the risk associated with over-managing policy processes is well illustrated with 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, without a major war for almost 100 years. The Treaty of Versailles, on the other hand, was dead only a few years after it was signed. In Vienna, the negotiators had plenty of time for their work, but were still able to enjoy the social aspects of their interactions.

Slowly, and without a predetermined grand design, they created an effective peace deal. The genius of Metternich and Talleyrand helped achieve this. In Versailles, however, diplomats engaged in a highly organised process in which hundreds of scientists, statisticians and cartographers collaborated to create a "scientifically constructed peace". They even tried to quantify justice, and ultimately created the mess that led to the Second World War. Of course, many other factors influenced the fate of these two agreements, however the stark differences in the very way they were conceptualised provides a convincing argument against over-management of diplomatic processes.

While the IGF cannot be compared to these grand events, its principles are closer to the Vienna Congress approach. Unfortunately, there have not been as much entertainment as in Vienna, but the common factor is an attempt not to predetermine processes beyond a minimum of planning. **The IGF processes unfold and take an optimal shape through the collective moulding of all of those involved, including significantly different views.**

4. Harness 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 harnessing a wide variety of policy inputs that would normally be lost through the various filters of traditional inter-governmental operations. **Individuals and groups have been able to voice their opinions directly to the IGF through personal participation in events, web-communication and remote participation.** These new ideas and insights, which would not reach the top global fora in most policy processes, considerably enrich the IGF process. One of the lessons from the IGF is that the first step towards a more inclusive policy process is the invitation for open participation. The full benefit of open and inclusive participation is achieved if a wide variety of contributions are collected, considered and, whenever possible, included in policy documents. Inclusiveness increases the legitimacy of the process and the feeling of ownership among the various stakeholders.

5. Enhance National "Diplomatic Footprints" through Multistakeholderism

Traditionally, since the establishment of nation states and diplomatic services in the 18th century, governments have represented their populations abroad. When Richelieu established the first foreign ministry in France, it took one month to deliver a letter from Paris to Moscow. Today, a message can cover the same distance in a fraction of a second. This leads us to ask whether the mode

of diplomatic representation can remain the same, in spite of such dramatic changes in communications over the centuries.

Some aspects of representation will certainly remain the same. States are, and will remain, the principal way of organising human society, with citizens living in defined territories and sharing common national identities. Diplomacy will remain the main channel for the representation of these societies.

In other respects, representation will need to adapt. With more players and more complex issues to deal with, the traditional diplomatic approach shows serious limitations. Even the most efficient diplomatic services cannot provide enough "bandwidth" (i.e., qualified human resources) for exchanges with foreign entities. Better "diplomatic broadband" can be provided through the inclusion of actors from civil society, the business sector, local authorities and other entities in global policy processes. Already, many non-state actors run their "small diplomacies" – maintaining contacts with foreign entities, participating in international meetings and shaping the global policy discourse, among other activities.

Some states, such as Canada, Switzerland and the Scandinavian states, recognised this evolution early and have integrated non-state actors in their foreign policy activities through approaches such as "Team Canada" and ambassadors working with non-governmental actors. Unfortunately, this practice is not common in many developing countries, where the "diplomatic bandwidth" is usually very low and restricted to small diplomatic services with limited financial and human resources. In many developing countries, national multistakeholder structures have appeared only during the last few years.

The Internet Governance Forum contributed in a practical manner 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 dedicating more resources. Multistakeholder national IGF bodies are appearing and governments coordinate more with business and civil society. Some small and developing states are represented in IG policy processes by non-state actors.

Sometimes, fostering such inclusiveness is mainly a matter of coordination, identifying skilled compatriots and creating a national multistakeholder framework. Dedicated capacity building through training programmes involving various stakeholders from the same state also helps: co-participant in a training programme tend to develop trust and a team spirit.

6. Increase Policy Coherence through Multistakeholderism

One of the main challenges for any global policy process today, including fields such as climate change and migration, is to achieve policy coherence in dealing with multidisciplinary issues. In the field of Internet governance, the IGF serves as an umbrella where 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 part of Internet governance. In some issue areas, such as multilingualism, the IGF helped very diverse organisations including governments, ICANN, UNESCO and ITU to focus in coordinated way on the same topic. As a decision-*shaping* body the IGF influences policy coherence more than some decision-*making* bodies. **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, where different organisations end up dealing with the same issues.**

7. Develop Functional Interplay among National, Regional and Global Policy Levels

In increasingly integrated world, it is difficult to maintain the traditional architecture of international policy consisting of international organisations on regional and global levels. Instant communications and the growing influence of non-state actors blur the line between the national, regional and global policy spaces. In this globally unified policy space, issues move quickly between different levels and fora. Some players, especially NGOs, use "forum shopping" in order to insert their policy initiatives on the most favourable policy level. Some governments, for example, in the EU, use so-called "policy laundering:" If an initiative is not adopted on the national level it is "recycled" through the regional level and re-imported as a country's "international obligation".

In the field of Internet governance, the network of policy *fora* is highly complex. A wide variety of *fora* existed long before the IGF was created (international organisations, ICANN, ISOC, various standardisation bodies). In addition, the IG policy actors are highly agile, moving easily from one policy layer and fora to another using modern communications technologies. **The IGF has attempted to maximise the benefits and reduce the risks of multi-level policy processes. The IGF coordinates global, regional and national activities through both bottom-up (in the preparation of IGF) and top-down approaches (dissemination of knowledge from IGF). The high transparency of the IGF makes the process**

less open to "forum shopping" and other policy manipulations. Although the IGF made breakthroughs in this process, much more needs to be done.

8. Develop Communication among Different Professional and Organisational Cultures

Hundreds of books have been written on the theme of how to communicate with people from different national cultures: Arabs, Chinese, Americans, etc. However, experience from the IGF shows that in a policy process, often the main challenge is to facilitate exchange among different professional cultures (e.g., lawyers, engineers) and different organisational cultures (e.g., international organisations, governments, companies). In today's globalised world, with instant communication, it is often easier for us to communicate within the same professional circles, even across national borders. For example, an American computer engineer may find that he or she has better communication with another engineer in China, than with an American diplomat.

As global issues become increasingly technical (for example, climate change and health), effective inter-professional communication becomes more and more important. Improvements in inter-professional communication can be achieved through training, education and exposure to other cultures. Better inter-professional communication may also contribute to better policy coherence among different ministries and international organisations. **The IGF has made positive steps in inter-professional communication through facilitating effective exchange of ideas among specialists from a variety of professions.** A good example of this is the wide professional and institutional diversity of panellists involved in workshop session discussions.

9. Recognize that Technical and Scientific Issues are Not Policy Neutral

The IGF process has clearly shown that any technical issue has a policy aspect, empowering some groups and interests. At some point, technical issues evolve into policy issues; policy issues in turn require decisions about values and interests.

This evolution from technical issues to policy issues is happening in other policy fields as well. As the Copenhagen Climate Change Summit approaches, national delegations are more likely to be populated with diplomats and policy makers and less with scientists specialising in climate change. As diplomatic processes increasingly overlap with scientific and technical fields, the question of the delimitation between these two fields will be increasingly important.

10. Recognize that Text Remains Central for Diplomacy

Despite all the promises of virtual conferencing and other technologies, today – even more than in the past – text remains the central tool of diplomacy.[1] Text is central to the IGF process, even though the IGF does not produce in any official final document (e.g., convention, treaty or declaration). Most exchanges between preparatory sessions are done via mailing lists and email. The IGF website is text-intensive, with little use of photos or images. Text also emerges as the key to two other developments which are discussed separately below: verbatim reporting and remote participation. The IGF experience is that the multistakeholder nature of its processes did not reduce the importance of text. In fact, it has become clear that the main processes must be built around text. This fact should be reflected in the training and preparation of stakeholders for participation in global policy processes.

11. Appreciate the Influence of Verbatim Reporting on Diplomacy

Verbatim reporting – the simultaneous transcription and display of each oral intervention in a meeting as it is presented – is a technical and procedural innovation that could have substantive influence on the way multilateral diplomacy is performed. Learning from ICANN practice, the Secretariat of the Working Group on Internet Governance (WGIG) introduced verbatim reporting in April 2005. The practice has been continued by the IGF and recently introduced by the ITU. All oral 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, transcriptions of their speeches appear on the screen.

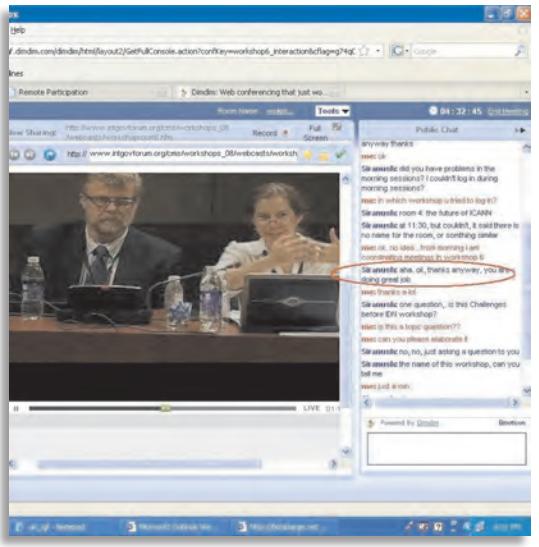
Verbatim Reporting Screen at the IGF-Rio – Photo by Charles Mok

Verbatim reporting has had an important effect on the diplomatic *modus operandi*. The awareness that what is said will remain in writing makes many delegates careful in choosing the level and length of their verbal interventions. Verbatim reporting has also increased the transparency of diplomatic meetings.

12. Increase Inclusiveness and Openness through Hubs for Remote Participation[2]

One of the main objectives of the IGF has been inclusive participation involving various countries and stakeholder groups. It was natural for a forum that discusses governance of the Internet, to use the Internet to extend participation in IGF meetings beyond those who could physically attend. During the first IGF meeting in Athens, the IGF Secretariat introduced video, audio and text broadcasting for both preparatory and main events. This footage was viewed mainly by individuals who already had a strong interest in the IGF. It led to a relatively modest level of remote participation and did not reach all stakeholders concerned with the topics discussed at the IGF.

A solution was introduced in the form of "remote hubs". Hubs are defined as local meetings that take place during and parallel to the IGF meetings, hosted by universities, ICT centres, NGOs and other players which 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 at the IGF. As part of a remote hub, remote participants can send text and video questions to be answered by the IGF panellists in real time interventions. In addition, hubs host panels and roundtable discussions correlating to the themes of the IGF from a local perspective. Through these activities, the local hubs enable enriching coordination between global and local policy processes. For example, during the IGF 2008, the remote hub in Madrid followed the session on cybersecurity during the IGF and continued their discussion on cybersecurity in the specific Spanish context. A total of eight remote hubs operated in parallel with the IGF 2008 (Madrid, Lahore, Barcelona, Belgrade, Buenos Aires, Sao Paulo, Bogota and Pune). More than 450 event hours were broadcast for remote participation and a total of 522 attendees joined the meeting remotely during the four-day event.[3]



Remote Participation at IGF-2008

After the successful test implementation in 2008, the concept of remote hubs was adopted by

the IGF Secretariat. It is expected that remote participation will increase significantly during the next IGF in Sharm El Sheikh (November 2009).

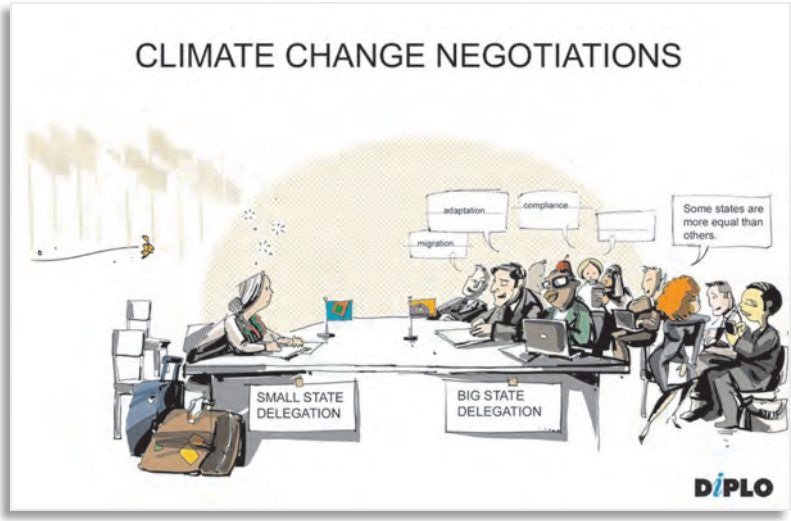
The experience from the IGF shows that remote participation significantly increases the inclusiveness and openness of international meetings. It creates a link between the global and local scenes, which is often missing in international diplomacy.

13. Recognize the Interplay between Formal Protocol (or Lack of) and Equal 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 three 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 may also pose a few challenges. The informal atmosphere may make participants from national cultures with strong respect for social hierarchy feel uncomfortable and hesitant to contribute. Furthermore, in diplomatic, legal and some other professional cultures, participation in debates is structured by professional protocols. Therefore, 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 various settings where different stakeholders can participate at ease.** For example, the IGF increased the level of protocol of some, mainly plenary, sessions, adding more of the typically diplomatic rules of procedure (e.g., speaking slots, asking questions) and organised special sessions for parliamentarians.

14. 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 the wider society through business, civil society and academic communities. Therefore, it is not surprising that small and developing states may 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 formally equal status, regardless of size or power.



Formal vs. Functional Equality in Negotiations

At the beginning of the World Summit on the Information Society (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 shopping approach" to Internet governance which would provide them with one, preferably intergovernmental "address", where they could discuss all issues related to Internet governance.[4]

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.

a) On the formal level, the IGF ensures that all sessions and panels have adequate participation from the various stakeholders from developing states. The increasing level of participation from developing countries was visible at IGF-Rio and IGF-Hyderabad.

b) 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 IG expertise, working at Internet organisations or universities around the world. Especially for small states taking advantage of experts working abroad is essential.

c) 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 1000 officials and professionals from small and developing states have been involved in training and other capacity building activities. This capacity building went beyond traditional academic courses by providing a unique blend of teaching, policy research and policy immersion aiming to help participants understand IGF dynamics and gain confidence for full and meaningful participation in policy processes. The involvement of various stakeholders (diplomats, officials, engineers) in the training process provided participants with an understanding of the advantages of a multistakeholder approach and the confidence to participate in meetings with other professional communities.

d) 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, 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 IG policy process.

By increasing participation levels, encouraging capacity building, and fostering the development of networks and communities, the IGF has helped developing countries move from formal/passive to functional/active participation in Internet governance.

NOTES

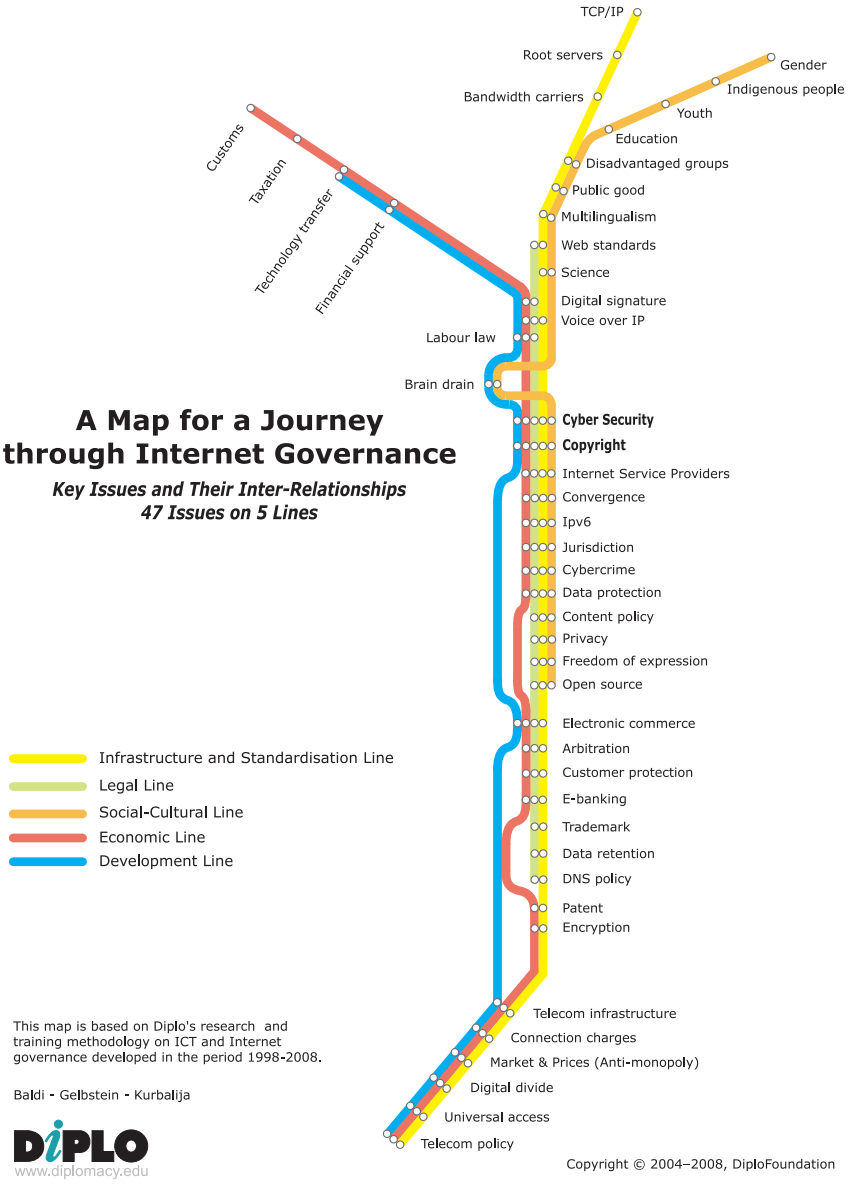
[1] An interesting parallel is the use of SMS services on mobile phones, through which text remains essential in human communication in spite of powerful voice and video based tools.

[2] Meaningful and substantive comments were provided by Ginger Paque and Marilia Marcel, who are also the driving force behind the remote participation working group (**www.igfremote.com**).

[3] A detailed report about remote participation at IGF 2008 is available at **http://www.igfremote.com/ReportRPIGF-final.pdf**.

[4] 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" IG-related aspects from other policy processes (privacy, intellectual property, human rights, development, e-commerce, etc.).

ANNEX II


A Map for a Journey through Internet Governance
Key Issues and Their Inter-Relationships
47 Issues on 5 Lines
Infrastructure and Standardisation Line
Legal Line
Social-Cultural Line
Economic Line
Development Line
TCP/IP
Root servers
Bandwidth carriers
Gender
Indigenous people
Youth
Education
Disadvantaged groups
Public good
Multilingualism
Web standards
Science
Digital signature
Voice over IP
Customs
Taxation
Technology transfer
Financial support
Labour law
Brain drain
Cyber Security
Copyright
Internet Service Providers
Convergence
Ipv6
Jurisdiction
Cybercrime
Data protection
Content policy
Privacy
Freedom of expression
Open source
Electronic commerce
Arbitration
Customer protection
E-banking
Trademark
Data retention
DNS policy
Patent
Encryption
Telecom infrastructure
Connection charges
Market & Prices (Anti-monopoly)
Digital divide
Universal access
Telecom policy
This map is based on Diplo's research and training methodology on ICT and Internet governance developed in the period 1998-2008.
Baldi - Gelbstein - Kurbalija
DiPLO
www.diplomacy.edu
Copyright © 2004–2008, DiploFoundation

ANNEX III – A SURVEY OF THE EVOLUTION OF INTERNET GOVERNANCE UNTIL 2003

Actor / Period	United States	Internet "Guardians"	International Organisations	Private Sector	Countries	Civil Society
	The Department of Defence (DoD) runs DNS					
1986	The National Science Foundation (NSF) takes over from the DoD					
1994				NSI signs a contract with the NSF to manage DNS for the period 1994-1998		
THE START OF "THE DNS WAR" After the NSF outsources the management of DNS to NSI (a private company), the Internet community (mainly ISOC) tries for many years to return DNS management to the public domain. It succeeds after 4 years. Here is a survey of this process, which involved a lot of diplomatic techniques, such as: negotiation, coalition building, using leverage, consensus building, etc.						
June 1996		IANA/ISOC – Plan to take over from NSI after the end of its contract; the introduction of additional domains; a strong opposition from the trademark sector against new top domains; also a strong opposition from the ITU				
Spring 1997		An IAHC (International Ad Hoc Committee) Proposal Participants in the IAHC: 2 representatives from the trademark interest groups, WIPO, ITU and NSF; and 5 representatives from the IETF Conclusion of gTLDMoU specifying: DNS as a "public resource"; seven new domains; strong protection for trademarks" Establishment of CORE (Council of Registers – signing ceremony in March 1997 at the ITU, Geneva); CORE collapsed immediately Strong opposition from the USA Government, NSI and EU				

Actor / Period	United States	Internet "Guardians"	International Organisations	Private Sector	Countries	Civil Society
1997	USA government transfers the 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: IFDT (International Forum on White Paper), ORSC (Open Root Server Confederation), and BWG (Boston Working Group)				
		Instead of drafting a new paper, the ISOC focuses on: – Building a broad coalition involving international organisations (from the IAHC initiative), the private sector (IBM) and key countries (EU, Japan, Australia). – Creating a new organisation				
Second part of 1998		September 1998 – An ISOC-NSI Joint Draft Agreement October 1998 – ISOC abandons agreements and creates ICANN				
15 Nov 1998	DOC transfers authority to ICANN	ICANN acquires two new crucial functions: – Authority to accredit registers for the gTLD – 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 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	30 countries establish GAC in order to gain more influence in managing national domains ICANN reacts by establishing the DNSO subcommittee – ccTLDs	

Actor / Period	United States	Internet "Guardians"	International Organisations	Private Sector	Countries	Civil Society
THE END OF "THE DNS WAR" The "war" was 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.						
2000-2003			Emergence of a greater focus on the Internet in ITU, WIPO, UNESCO, OECD, the Council of Europe, and the World Bank	Strong push of the private sector for a regulated Internet (copyright laws, e-commerce, etc.)	Development of Internet legislation, court cases, etc.	NGOs' involvement in the digital divide, human rights, gender issues on the Internet
			Multisectoral and global initiatives focusing on Internet development, governance, etc.: G-8 Dot Force, World Economic Forum, UN ICT Task Force, World Summit on Information Society, Global Knowledge Partnership			
June 2002 – November 2003	The first PrepComm for the WSIS was held in June 2002; Internet governance emerged as an issue during the Regional Prepcom for West Asia in Beirut (January 2003); The Geneva ea decision on Internet governance at the Tunis Event (2005) Multisectoral and global initiatives focusing on Internet development, governance, etc.: G-8 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. The WGIG was a mutistakeholder body consisting of representatives of governments, the business community and civil society. The WGIG held 4 preparatory meetings and produced the Report which was the basis for the decision on Internet governance at the WSIS – Tunisia (2005) At the WSIS 2005 in Tunisia the "Tunis IG Compromise" introduced the Internet Governance Forum a compromise between those who opposed any change in the ICANN-centered regime and those who argued that the Internet should be governed through an inter-governmental regime.					
2006–2009	Following the conclusion of the WSIS-Tunis (2005), the Internet Governance Forum (IGF) was established in order to continue the policy process on Internet governance. So far three IGFs have been held: Athens – 2006, Rio de Janeiro – 2007 and Hyderabad – 2008. The next IGF will be held in November 2009 in Sharm el Sheik (Egypt). On the 30th of September 2009 the Government of the US and ICANN signed the "Affirmation of Commitments" which ends the US supervision of ICANN, one of the most controversial issues of Internet governance. ICANN enters a new phase as an independent organisation with more questions than answers about its future position and role.					

ANNEX IV – THE INTERNET GOVERNANCE CUBE

The WHAT axis is related to the ISSUES of Internet governance (e.g. infrastructure, copyright, privacy). It conveys the **multi-disciplinary** aspect of this approach.

The WHO axis of the cube focusses 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 **multi-layered** 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 the national level (where).

Separate from the Internet governance Cube is a fifth component – WHEN.

ABOUT THE AUTHOR

Jovan Kurbalija

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 – 2009). 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

Arab Republic of Egypt
Ministry of Communications
and Information Technology
www.mcit.gov.eg

Ministry of Communications and Information Technology (MCIT)
Egypt's Ministry of Communications and Information Technology (MCIT) was established in October 1999 to facilitate the country's assimilation into the global information society. Its mandate is to support the development of the local ICT industry, thereby boosting exports and creating jobs; promote the use of ICT nationwide as a means to achieve national development goals; and build the foundations of the knowledge society in Egypt in close cooperation with other governmental, civil society and private sector entities.

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 all 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 on 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 Commonwealth Internet Governance Forum provides a focal point for stakeholders and users from the 53 Commonwealth member states to come together to discuss issues relating to Internet governance. It aims to promote awareness of opportunities and solutions, to share best practice and to increase participation in regional initiatives and the global IGF.
www.commonwealthigf.org