The Information Society Library
GETTING THE BEST OUT OF CYBERSPACE
&
GKP Issues Paper
KNOWLEDGE FOR DEVELOPMENT SERIES

INTERNET GOVERNANCE

ISSUES, ACTORS AND DIVIDES

Eduardo Gelbstein • Jovan Kurbalija

DiPLO
www.diplomacy.edu

GKP

PREFACE

INFORMATION SOCIETY LIBRARY

There is no shortage of books on all matters relating to information management and information technology. This booklet adds to this large collection and attempts to do a number of things:

- offer non-technical readers an insight into the few principles that are important and reasonably stable;
- present the material in a context relevant to the work of those involved in international relations;
- awaken the curiosity of readers enough that they will progress beyond this booklet and investigate and experiment and thus develop knowledge and take actions that will meet their particular needs.

The format of these booklets and their contents evolved from courses given by the authors over the last few years in various environments and the feedback of the attendees. Readers' feedback on these booklets would be greatly appreciated by the authors so that future editions can be improved. The coordinates of the authors are given at the end of this booklet.

KNOWLEDGE FOR DEVELOPMENT SERIES

This publication is part of the Global Knowledge Partnership's 'Knowledge for Development Series', an overall effort to increase the availability of information and knowledge on various issues in the area of ICT4D.

ISBN 99932-53-09-X

Published by DiploFoundation and Global Knowledge Partnership

DiploFoundation

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

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

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

Global Knowledge Partnership Secretariat

Level 23, Tower 2, MNI Twins
11, Jalan Pinang, 50450 Kuala Lumpur
Malaysia

Email: gkp@gkps.org.my
Website: http://www.globalknowledge.org

Edited by Dejan Konstantinović and Steven Slavik
Illustrations: Zoran Marcetic - Marca
Cover Design by Nenad Došen
Layout & prepress by Lidija Tušek

CONTENTS

Introduction

The Evolution of Internet Governance 8
International Negotiations and Internet Governance 9
What does Internet Governance Mean? 10
Internet Governance Toolkit. 12
Approaches and Patterns 14
Guiding Principles 19
Analogies 22
The Classification of Internet Governance 26
"Building under Construction" 29

The Infrastructure and Standardisation Basket

Introduction 33
The Telecommunications Infrastructure 34
Technical Standards and Services (The Internet Infrastructure) 37
Transport Control Protocol/Internet Protocol (TCP/IP) 38
The Domain Name System (DNS) 41
Root Servers 45
Internet Service Providers (ISPs). 47
Internet Bandwidth Providers (IBPs) 49
Economic Model for Internet Connectivity. 50
Web Standards. 53
Open Source. 54
Convergence: Internet-Telecommunications-Multimedia 54
Internet Security 57
Encryption 60
Spam 62

The Legal Basket

Introduction 69
Legal Mechanisms 69
Legislation 70
Social Norms (Customs) 71
Self-Regulation 71
Jurisprudence 71
International Regulation 72
Jurisdiction 73
Arbitration 78

Intellectual Property Rights 80
Trademarks 80
Copyright 81
Patents 86
Cybercrime 86
Digital Signatures 88
Labour Law 90
Privacy and Data Protection 92

The Economic Basket

Introduction 101
E-Commerce 102
Consumer Protection 105
Taxation 106
Customs 107
E-Payments: E-Banking and E-Money 107

The Development Basket

Introduction 113
The Digital Divide 114
Universal Access 115
Strategies for Overcoming the Digital Divide 116
Developing Telecommunications and Internet Infrastructures 117
Financial Support 117
Socio-Cultural Aspects 118
Telecommunication Policy and Regulation 119

The Socio-Cultural Basket

Introduction 123
Content Policy 123
Human Rights 129
Multilingualism and Cultural Diversity 130
Global Public Good 131
Education 132

Annex

"The Blind Men and the Elephant" by John Godfrey Saxe 139
A Survey of the Internet Governance Evolution 140
A Map for a Journey through Internet Governance 142
Diplo`s Internet Governance Cube 143

About the Authors 144

SECTION 1

Introduction

Internet Governance is not a simple subject. Although it deals with a major symbol of the DIGITAL world, it cannot be handled with a digital - binary logic of true/false and good/bad. Instead, the subject's many subtleties and shades of meaning and perception require an ANALOG approach, covering a continuum of options and compromises.

Therefore, this booklet will not attempt to provide definitive statements on Internet Governance issues. Rather, its aim is to propose a practical framework for the analysis, discussion, and resolution of the key problems in this field.

INTRODUCTION

> In only a few years, the Internet has revolutionised trade, health, education, and, indeed, the very fabric of human communication and exchange. Moreover, its potential is far greater than what we have seen in the relatively short time since its creation. In managing, promoting, and protecting its presence in our lives, *we need to be no less creative than those who invented it.* Clearly, there is a need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different.
>
> Kofi Annan - Global Forum on Internet Governance
> (New York, 24 March 2004)

The Internet has, in a relatively short time, become an essential instrument for today's society. As of early 2005, the Internet is thought to include:

- an estimated 750 million users worldwide;
- an estimated electronic commerce turnover of US$1 billion, which is projected to rise rapidly;
- a major social impact in education, health, government, and other areas of activity;
- cybercrime, such as fraud, gambling, pornography, 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. The process of addressing legal issues and the social consequences of technological developments invariably lags behind technological innovation. This applies to the Internet, too.

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 misuses and abuse;
- encourage further development.

We are currently in the early phase of international negotiations on Internet Governance, which is characterised by the need to establish and agree on a basic framework and to select appropriate instruments for the discussion of the many arising issues. 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 our emerging Information Society? These are some of the key questions that need to be addressed within the framework of Internet Governance.

THE EVOLUTION OF INTERNET GOVERNANCE

One of the fascinating aspects of the Internet during its development and early growth was its unique governance. The Internet started as a government project. In the late 1960s, the US government sponsored the development of the Defense Advanced Research Projects Agency (DARPANet), a resilient communication facility designed to survive a nuclear attack.

By the 1980s, a wider international community was using the facilities of this network, which by this time was referred to as the Internet. In 1986, the Internet Engineering Task Force (IETF) was established. The IETF managed the further development of the Internet through a cooperative, consensus-based, decision-making process, involving a wide variety of individuals. There was no central government, no central planning, and no grand design.

At this point, life was relatively simple. However, in 1994 the US National Science Foundation decided to involve the private sector by subcontracting the management of the Domain Name System (DNS) to Network Solutions Inc (NSI). This was not well received by the Internet community, and a "DNS War" started.

This "DNS War" brought other players into the picture: the business sector, international organisations, and nation states. It ended in 1998 with the establishment of a new organisation, the Internet Company for Assigned Names and Numbers (ICANN).

Since 1998 and the establishment of ICANN, debate on Internet Governance has been characterised by the more intensive involvement of national governments, mainly through the UN framework.

INTERNATIONAL NEGOTIATIONS ON INTERNET GOVERNANCE

The World Summit on the Information Society (WSIS), held in Geneva in December 2003, officially placed the question of Internet Governance on diplomatic agendas. The Declaration of Principles and Action Plan adopted at WSIS proposed a number of actions in the field of Internet Governance, including the establishment of a Working Group.

Below is an excerpt on Internet Governance from the WSIS Declaration of Principles:

> 50. International Internet Governance issues should be addressed in a coordinated manner. We ask the Secretary General of the United Nations to set up a working group on Internet Governance, in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector, and civil society from both developing and developed countries, involving relevant inter-governmental and international organisations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005.

Following is an excerpt on Internet Governance from the WSIS Action Plan:

> 13. b) We ask the Secretary General of the United Nations to set up a working group on Internet Governance, in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector, and civil society from both developing and developed countries, involving relevant intergovernmental and international organisations and forums, to investigate and make proposals for action, as appropriate, on the governance of Internet by 2005. The group should, *inter alia*:
>
> i. develop a working definition of Internet Governance;
> ii. identify the public policy issues that are relevant to Internet Governance;
> iii. develop a common understanding of the respective roles and responsibilities of governments, existing inter-governmental and international organisations and other forums, as well as the private sector and civil society from both developing and developed countries;

iv. prepare a report on the results of this activity to be presented for consideration and appropriate action for the second phase of WSIS in Tunis in 2005.

WSIS and WGIG most likely comprise the first phase of the Internet Governance process, which should result in clarifying Internet Governance issues, setting the agenda, as well as introducing procedures and mechanisms.

The Multilateral Negotiation Process and Internet Governance

NEGOTIATION PHASE	WSIS ACTIVITY
Pre-negotiation	From 1998 until the WSIS Summit in Geneva (2003).
Agenda-setting and Issue Clarification	Started in December 2003 at the WSIS Summit in Geneva with the decision to establish the Working Group on Internet Governance (WGIG); to be concluded in Tunis.
The Search for Formulas	After Tunis 2005.
Negotiation on details	
Agreement	
Implementation	

WHAT DOES INTERNET GOVERNANCE MEAN?

At the Global Forum on Internet Governance, held at the United Nations in New York on 24-25 March 2004, several speakers told various versions of the story of the blind men and the elephant.

It was six men of Indostan
To learning much inclined,
Who went to see the Elephant
(Though all of them were blind),
……
And so these men of Indostan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right,
And all were in the wrong!

Excerpt from the poem "The Blide Men and the Elephant" written by American poet John Godfrey Saxe (1816-1887); the complete text is available in Annex I.

The moral of the poem makes it clear that a discussion of the meaning of "Internet Governance" is not merely linguistic pedantry. Different perceptions of the meaning of this term trigger different policy approaches and expectations.

Telecommunication specialists see Internet Governance through the prism of the development of the technical infrastructure. Computer

specialists focus on the development of various 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.

Each of the terms "Internet" and "governance" is the subject of controversial interpretation. Some authors argue that the first part, "Internet," does not cover all of the existing aspects of global ICT developments. Two other terms: "Information Society" and "Information and Communications Technology" are usually put forward as more comprehensive. They include areas that are beyond 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 TCP/IP as the main communications technical standard. The already ubiquitous Internet continues to expand at a rapid rate, not only in terms of the number of users but also in terms of the services that it offers, notably Voice over Internet Protocol (VoIP), which may displace conventional telephony.

The second part of the term, "governance," has been the cause of controversy in recent debates, especially during WSIS. Misunderstanding primarily stems from the use of the term governance as a synonym for government. When the term "Internet Governance" was introduced in the WSIS process, many, especially developing, countries linked it to the concept of government. One of the consequences of such an approach was the belief that Internet Governance issues should be addressed at the inter-governmental level with the limited participation of other, mainly non-state, actors.

What were the main reasons for this terminological confusion? Is it obvious that "governance" does not mean "government"? Not necessarily. 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.

Another potential source of confusion is the translation of the term "governance" into other languages. In Spanish, the term refers mainly to public activities or government (*gestión pública, gestión del sector públic* and *función de gobiern)*. The reference to public activities/government is also noticeable 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 (*gestăo pública* and *administração pública*). This discrepancy in the interpretation of the term "governance" might provide a linguistic explanation for why many delegations at WSIS linked the question of Internet Governance to the public sector, and centred their deliberations on the need for government intervention.

INTERNET GOVERNANCE TOOLKIT

An Internet Governance regime 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 tend to develop a common frame of reference, values, perception of cause-and-effect relationships, modes of reasoning, terminology, vocabulary, jargon, and abbreviations.

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 will be complex as it will need to involve many issues, actors, mechanisms, procedures, and instruments.

There are at least five dimensions to Internet issues: Infrastructure, Legal, Economic, Development, and Socio-cultural. Each one is discussed in the chapters that follow. Many actors, in the private and public sector, play roles in each of these dimensions. Most of them (root operators, ISPs, trademark lawyers, development specialists, civil society activists, etc.) have very specific and well developed professional cultures.

Each combination of issues and actors has its purpose, objectives, terminology, and spheres of collaboration and influence. It seems that many, if not most, of these combinations are currently working in relative isolation from the rest. Add to this the multiplicity of working languages reflecting the global nature of the problems, and the challenge of bringing these elements together into a coherent governance architecture will become clear, but with goodwill from all sides, no doubt manageable.

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

The complexity of implementing Internet Governance shows that linear, mono-causal and "either/or" thinking is not suited to addressing Internet Governance issues. Therefore there is a need for new cognitive tools that cater for this complexity and introduce common approaches and guiding principles.

The main purpose of such an Internet Governance Toolkit would be to:

- organise the tools currently used in the Internet Governance debate;
- create additional cognitive tools;
- facilitate the inclusive nature of the Internet Governance process by providing interested parties with the tools to understand the issues, positions, and developments.

The Internet Governance Toolkit consists of:

- patterns and approaches;
- 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 negotiation 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

"Narrow vs. broad" Internet Governance has been one of the main issues so far, reflecting the different approaches and interests in the Internet Governance process. The "narrow" approach focusses on the Internet infrastructure (Domain Name System, IP numbers, and root servers) and on ICANN's position as the key actor in this field.

According to the "broad" approach, Internet Governance negotiations should go beyond infrastructural issues and address other legal, economic, developmental, and socio-cultural issues. Distinguishing between these two approaches is particularly important in the early agenda-setting phase of Internet negotiations.

The broad approach is implicitly supported by the WSIS Declaration, which gave the WGIG the mandate "to identify the public policy issues

that are relevant to Internet Governance." This approach is generally supported by the policy and academic discussion following the WSIS Summit in Geneva.

The current debate has moved from the either/or stage towards identifying priorities and an appropriate balance between the "narrow" approach (ICANN-related issues) and the "broad" approach (other Internet Governance aspects).

Technical vs. Policy Aspects

A significant challenge of the Internet Governance process will be the integration of technical and policy aspects, as it is difficult to draw a clear distinction between them. 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 some cases, an initial policy goal for a technical solution changed. For example, the Internet architecture of end-to-end networking and packet switching was designed with the policy goal to create a robust network that could survive a nuclear attack. The same architecture later became the basis for the development of creativity and freedom of expression on the Internet.

Other technical solutions, such as electronic means for the protection of copyright, are intentionally created in order to replace or enforce certain policies (in this case stricter copyright protection).

In the case of the Internet, for a long time both technical and 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, that unity of technology and policy was broken. The reform of Internet Governance, including the creation of ICANN, was an attempt to re-establish the lost balance. This issue remains open, and most likely, will be one of the potentially controversial topics at WSIS/WGIG.

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

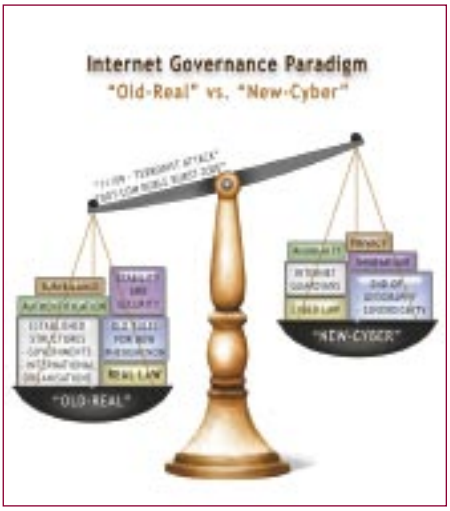
There are two approaches to almost every Internet Governance issue. The "old-real" approach – or "new wine in old bottles" – argues that the Internet does not introduce anything new to the field of governance. The

Internet is just another new device, from the governance perspective, no different to 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. As long as it involves communication between people, the Internet is no different from the telephone or the telegraph, and it can be regulated like other telecommunication devices. 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 "real" approach is also against e-tax moratoriums.

The "new-cyber" approach – or "new wine in new bottles" – argues that the Internet is a fundamentally different device from all previous ones. Thus, it requires fundamentally different governance. This approach was particularly popular in the early days of the Internet. There were even hopes that the innovative early method of governing the Internet – "rough consensus and running code" – might become the model for regulating other areas of human activities. The main premise of the "cyber" approach is that the Internet de-linked our social and political reality from the world of sovereign states. Cyberspace is different from real space and it requires a different form of governance.

The influence of this approach was noticeable in the process of the creation of ICANN, which, for example, minimised the influence of "real" world governments. The "cyber" approach was softened by ICANN's reform in 2002, which strengthened the role of governments and brought ICANN closer to political reality.



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.

Given the continuous interplay between these two approaches, the "old-real" versus "new-cyber" dilemma is likely to continue and strongly influence Internet Governance negotiations.

Decentralised vs. Centralised Structure of Internet Governance

Internet Governance is a multi-faceted phenomenon involving a wide range of government mechanisms and forums, including international organisations, national governments, as well as professional and private bodies.

According to the decentralised view, the current governance structure reflects the very nature of the Internet: a network of networks. Such a complex setup cannot be put under a single governance umbrella, such as an international organisation. Another argument is that the lack of centralised governance is one of the major factors allowing for 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.

Internet and the Public Good

Most of the technical infrastructure through which Internet traffic is channelled is owned by private and state companies, typically telecommunication operators. This is analogous to a shipping company transporting containers. However, shipping lanes are open and regulated by the Law of the Seas, which states that the open seas are *res communis omnium,* while the network backbones over which data is transported are owned by telecommunication companies. This raises a number of questions:

- What are the property rights on Internet backbones?
- Can private companies be requested to manage their private property – Internet backbones – in the public interest?
- Can the Internet, or parts of it, be considered a global public good?
- Could the old Roman concept of *res communis omnium* be applied to the Internet, as in the case of some parts of the Law of the Sea?

The main challenge in this public versus private dilemma will be, on the one hand, to provide the private sector with a proper commercial environment, but, on the other hand, to ensure further development of the

Internet as a public resource, consisting of knowledge and information commons. For more information please consult page 131.

Geography and the Internet

One of the early assumptions regarding the Internet was that it overcame national borders and eroded the principle of sovereignty. In his famous "Declaration of the Independence of Cyberspace," John Perry Barlow sent the following message to all governments: "You are not welcome among us. You have no sovereignty where we gather. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Cyberspace does not lie within your borders."

This declaration is an example of the predominant techno-optimism typical of the mid-90s. Since Barlow's declaration, there have been many developments, including more sophisticated geo-location software. 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. In addition, the latest national laws worldwide require ISPs to identify their users and, if requested, to provide necessary information about them to authorities.

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 more easily through existing laws.

"Walk the Talk" Approach

The "walk the talk" approach promotes the use of online tools for negotiating on the issues of the online world. The Internet Governance negotiation process presents a considerable challenge in multilateral diplomacy, which calls for both the use of well-proven and efficient negotiating techniques and the introduction of new innovative approaches. One of the main innovative techniques could be the use of online tools for negotiations.

Internet-based negotiations should facilitate the participation of a broader group of stakeholders, especially those who cannot afford to participate in traditional diplomatic conferences. One priority will be to assist developing countries to participate meaningfully in the Internet Governance process.

GUIDING PRINCIPLES

Guiding principles represent certain values and interests that should be promoted through 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.

"Don´t Re-Invent the Wheel"

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

a) those invented for the Internet (e.g. ICANN);
b) those that require considerable adjustment in order to address Internet-related issues (e.g. trademark protection, e-taxation);
c) 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 as a criterion for the evaluation of specified Internet Governance-related decisions (e.g. introduction of new protocols and changes in decision-making mechanisms).

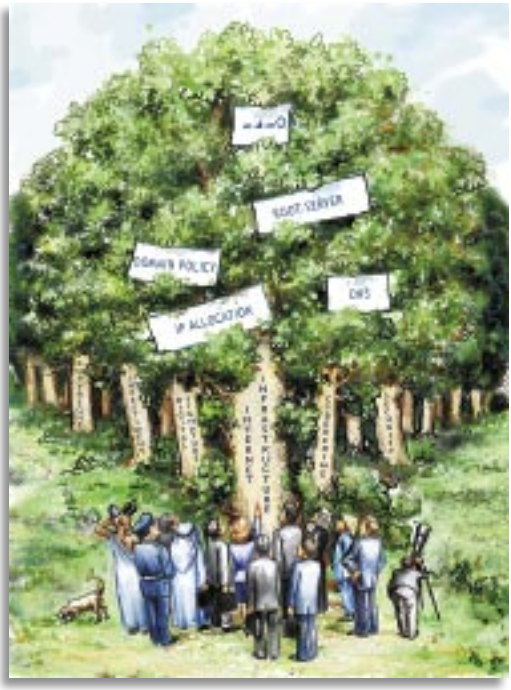
Internet Governance and Development

The current debate on Internet Governance highlights the high development relevance of the following Internet Governance issues: interconnection charges, distribution of IP numbers, investment, protection of intellectual property, and promotion of e-commerce. The Internet Governance process should be guided by overall WSIS development objectives and the UN Millennium Goals.

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).

ICANN's GUIDING PRINCIPLES

The USA White Paper on Internet Governance (1998) specifies the following guiding principles for the establishment of ICANN:

- Stability; the functioning of the Internet should not be disrupted, especially in the operation of its key structures, including "root domains";
- Competition; it is important to encourage creativity and flexibility, which will help in the further development of the Internet;
- Decision-making; the new system should accommodate some of the Internet's early rules and principles, including grassroots-style organisation, openness, etc.;
- Representation; the new framework should accommodate the main stakeholders: both geographical (different countries) and professional (different professional communities).

Make Tacit Technical Solutions Explicit Policy Principles

It is a common view that certain social values, such as free communication, are facilitated by the way the Internet is designed technically (the "end to end" principle). However, this is not necessarily correct. 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. Principles such as free communication should be clearly stated at the policy level, not tacitly presumed at the technical level.

The Principle of Technological Neutrality

This principle is closely linked with the previous one. According to technological neutrality, policy should not depend on 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).

Technological neutrality provides many governance advantages. First, it de-links governance from any particular technology and makes it ready for future technological developments. Second, technological neutrality is the most appropriate regulatory principle for the future convergence of the main technologies (telecommunication, media, Internet, etc.).

The European Union has introduced technological neutrality as one of the cornerstones of its telecommunications policy. While technological neutrality is clearly an appropriate principle, one can envisage many dif-

ficulties in the transition from existing telecommunication regulations to new ones. This is already obvious in areas such as Voice over IP.

Risk of Running Society through Programmers' Code

One key aspect of the relationship between technology and policy was identified by Lawrence Lessing, who observed that with its growing reliance on the Internet, modern society may end up being regulated by software code instead of laws. Some legislative functions of parliament and government could *de facto* be taken over by computer programmers and technical 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 a key mental process 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, the Internet is a broad term, which encompasses a variety of services, including e-mail (see analogy to telephony), web (see analogy to broadcasting services – television), and databases (see analogy to library). An analogy to any particular system may over-simplify the understanding of the Internet.

Second, with the increasing convergence of various telecommunication and media services, the traditional differences between them 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 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 (like 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 through chatting. 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 is analogous to the telephone, the content of communication cannot be controlled.

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.

Internet – Mail/Post

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

Differences: This analogy covers only one Internet service – e-mail. Moreover, the postal service has a much more elaborate intermediary structure between the sender and recipient 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: As with telephony, the Internet is a broader concept 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 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.).

Internet - VCR, Photocopier

Similarities: This analogy is used in cases involving the reproduction of copyright-protected materials. The Internet can be used in the process of reproducing and disseminating various materials.

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.

Internet - Highway

Similarities: This analogy is linked to American culture and the importance it places on highways and railroads, thereby revealing the national fascination with discovery and new frontiers.

Differences: Aside from the transportation aspect of the Internet, there are no other similarities between the Internet and highways. The Inter-

net 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."

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 need for an initial mapping of Internet Governance is both academic and practical. On the academic side, an increasing volume of research on Internet Governance is being produced, but it has focussed mainly on ICANN and other issues belonging to the so called "narrow" approach to Internet Governance. A broader theoretical framework is still lacking, in particular on the international aspects of Internet Governance. The practical need for classification was clearly demonstrated during the WSIS process. Many players, including nation states, had difficulties grasping the complexity of Internet Governance. A conceptual mapping of the field should contribute towards more efficient negotiations within the context of WSIS as well as other multilateral negotiation processes on Internet-related issues.

A classification may assist Internet Governance players with the following:

- clearer identification of the main issues requiring negotiation;
- reduction of negotiation "noise" caused by inconsistent interpretations of the main concepts;

- avoidance of duplicating efforts by addressing the same issues in multiple fora;
- maintenance of an appropriate balance between a broad perspective and specific issues, thereby avoiding the problem of being "unable to see the forest for the trees."

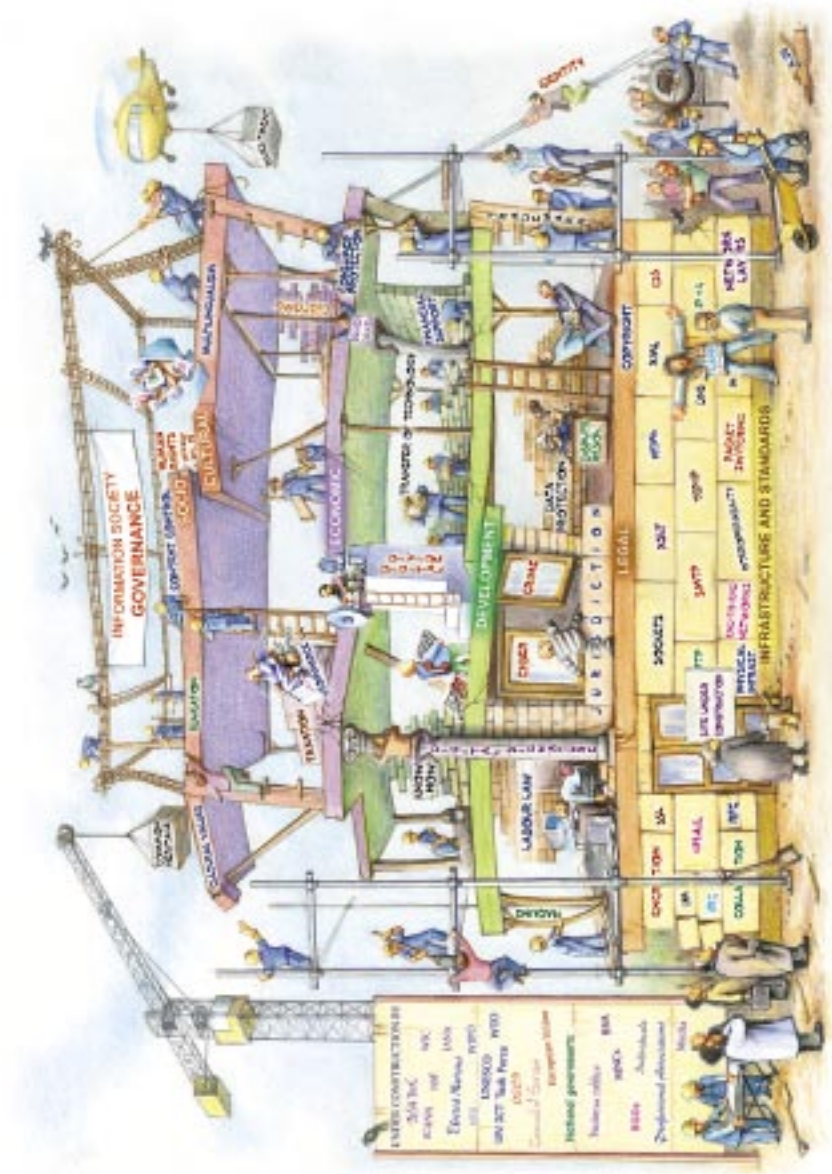
Ultimately, a careful mapping of Internet issues should make the process of negotiating Internet Governance more efficient. In economic terms, it should reduce the transaction cost – in other words, reduce the total time required for negotiations. This would be of particular benefit to countries with limited financial and human resources, thus enabling their increased participation. Unclear and confusing negotiating processes require disproportionately higher human resources and more time.

Diplo's classification of Internet Governance groups all issues in five classification clusters. Adjusting the terminology to the world of diplomacy, Diplo has adopted the term "basket." (The term "basket" was introduced in 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.

The five-basket model is metaphorically presented through the "Building under Construction" illustration on the next page.

Diplo's classification of Internet Governance is the conceptual basis for Diplo's overall approach to this field, including training/education, research, and the development of tools. Since its introduction in 1997, the classification has been used in courses attended by more than 300 students as well as by many researchers. Regular feedback on this classification scheme has been the basis for constant adjustments. The current classification, therefore, is based on numerous iterations as well as aggregated knowledge and experience.


INFORMATION SOCIETY
GOVERNANCE
ECONOMIC
DEVELOPMENT
LEGAL
INFRASTRUCTURE AND STANDARDS
COPYRIGHT
LABOUR LAW

"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 Internet – or, more specifically, at the structure of the emerging Information Society. 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.

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. In Diplo's "Building under Construction" illustration of Internet Governance, the ground floor represents infrastructure and standardisation (see page 28). The main criterion for placing 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. These issues are grouped into the following three layers:

One of the Internet's strengths is its layered architecture. The Internet Infrastructure layer remains independent of the telecommunications infrastructure (the layer below) and of the applications standards (the layer above).

1. the telecommunications infrastructure, through which all Internet traffic flows;

2. the 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 a secure and stable operation of the Internet infrastructure, including Internet security, encryption, and spam.

THE TELECOMMUNICATIONS INFRASTRUCTURE

THE CURRENT SITUATION

Internet data can travel over a diverse range of communication carriers: telephone wires, fibre-optic cables, satellites, microwaves, and wireless links. Even the basic electric grid can be used to relay Internet traffic. The fast growth of the Internet has triggered a considerable increase in telecommunication capabilities. It is estimated that since 1998, telecommunications capacity has increased 500 times due to a combination of technological innovation and investment in new telecommunication facilities.

Because the telecommunications layer carries Internet traffic, any new regulations linked to telecommunications will inevitably impact the Internet too. The telecommunications infrastructure is regulated at both the national and international levels by a variety of public and private organisations.

Traditionally, international telecommunications were coordinated by the International Telecommunication Union (ITU), which developed elaborate rules covering the relationship between national operators, the allocation of the radio spectrum, and the management of satellite positioning.

Eventually, the liberal approach prevailed over the telecommunication monopolies. Liberalisation was additionally formalised in 1998 through the World Trade Organisation (WTO) Agreement on Basic Telecommunication (ABT). Following the adoption of ABT, 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 ITU's International Regulation (ITR) from 1988 facilitated the international liberalisation of pricing and services, and allowed basic services, such as international leased lines, to be used more innovatively in the Internet field.

The WTO gradually moved into the centre of the international telecommunications regime traditionally governed by the ITU. 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. The WTO provides a framework for general market rules.

Following liberalisation, the ITU's near monopoly, as the principal standards-setting institution for telecommunications, was eroded by other professional bodies and organisations, such as the European Telecommunications Standardisation Institute (ETSI), which developed the GSM standards, the Institute of Electrical and Electronics Engineers (IEEE), which developed the WiFi standards, and the Internet Engineering Task Force (IETF), which developed TCP/IP and other Internet related protocols.

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 Governance.

THE ISSUES

The "Last Mile" – Unbundling Local Loops

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. The reason is usually an underdeveloped national telecommunications infrastructure. In some developing countries with large territories it is difficult to connect remote cities and villages through traditional terrestrial telecommunication links.

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 telecommunications market.

The Liberalisation of Telecommunication Markets

A considerable number of countries have liberalised their telecommunication markets. However, many developing countries with telecommunication monopolies are faced with a hard choice: How to liberalise and make their telecommunication markets more efficient, while preserving an important budgetary income from the existing telecommunication monopolies.

Foreign assistance, gradual transition, and linking the liberalisation process to the protection of the public interest might be one way 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 position 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)

TECHNICAL STANDARDS AND SERVICES – The Internet Infrastructure

The Internet takes shape on this layer. Most of the issues attached to it are the core Internet Governance issues, usually listed in the "narrow" definition of Internet Governance. They are divided into two groups. The first comprises the core issues related to **technical standards and services:** TCP/IP, DNS, and root servers, while the second covers **the commercial aspects of the Internet infrastructure**, including: the roles of the Internet service providers (ISPs) and the Internet broadband carriers as well as the economic aspects of Internet connectivity (Internet connectivity charges and IXPs – Internet eXchange Points).

ICANN is probably the most frequently mentioned organisation within the context of Internet Governance discussions. The reason is ICANN's central position in the management of Internet technical standards and services. Its function is to set policy as well as manage numeric addresses (IP numbers) and domain name systems.

Opposing Views about ICANN's Role in Internet Governance

NARROW – TECHNICAL	BROAD – POLITICAL
ICANN is simply a coordination body conducting technical administration in the field of IP numbers and domain names. According to this view ICANN simply coordinates, not governs, the Internet. View expressed by: ICANN, the Internet Society, the US government, the governments of other industrialised states.	ICANN's work involves more than simple technical coordination. While ICANN should be allowed to keep such core technical tasks as the management of root servers and the distribution of IP numbers, policy should be established by a legitimate international body representing all states. This might be done either within the UN or a newly-established international framework. View expressed by: many developing countries.

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.

Packet switching is the method used to transmit data over the Internet. All the data sent from one computer is split into packets that travel over the Internet and are then reassembled when they reach the destination computer.

End-to-end networking puts all sophistication, intelligence, and innovation at the edges of a network. This principle has made all the Internet-related innovations possible. The network between the end-points is neutral and does not prevent development and creativity at the end-points. This means that applications that run over the Internet can be designed without requiring permission from network operators or any other parties.

Robustness is achieved through dynamic routing. Initially, the Internet's predecessor, ARPANET, introduced dynamic routing in order to develop robust defence networks capable of surviving a potential nuclear attack. Dynamic routing was used to interconnect a diverse set of networks.

Internet Governance related to TCP/IP has two important aspects: a) the introduction of new standards; and b) the distribution of IP numbers.

Standards for TCP/IP are set by the Internet Engineering Task Force (IETF). Given the core relevance of TCP/IP for the Internet it is carefully guarded by the IETF.

IP numbers are numeric addresses that each computer 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 regional Internet registries (RIRs).

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), and RIPE NCC (Reseaux IP Européens Network Coordination Centre – covering Europe and the Middle East). An African Registry, AFRINIC, is currently being established.

RIRs distribute IP numbers to the main ISPs and large enterprises. Further down the ladder are smaller ISPs, companies, and individuals.

THE ISSUES

Are There Enough IP Numbers?

The current pool of IP numbers under IPv4 (Internet Protocol, version 4) contain2s some 4 billion numbers and could be depleted 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 two major actions.

- The first was the rationalisation of the use of the existing pool of IP numbers. This was achieved through the introduction of Network Address Translation (NAT), capable of connecting a private network (e.g. company or university) through just one IP. Without NAT, every computer on a private network would need to have its own IP number.
- The second action was the introduction of IPv6 (a new version of the TCP/IP protocol), 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. The "better safe than sorry" approach (known as the "precautionary principle" in the language of environmental diplomacy) was followed, even though it was uncertain how fast IPv4 numbers would be depleted.

However, there could be an "artificial" scarcity if those responsible for allocating IP numbers at the local level, such as an ISP, choose to abuse their power and link such allocation to, for example, the purchase of other services, thus affecting IP number availability and their price.

Changes in TCP/IP and Internet Security

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. Security was primarily provided by limiting physical access to the connected networks and computers. Computers were used by a small group of computer specialists. Data was exchanged without any particular protection.

The expansion of the Internet has seen its user base grow far beyond the expectations of its early community, to some 750 million users worldwide. The Internet has also become an important commercial tool.

All this places the question of security high up on the list of Internet Governance issues. Security has been progressively improved through various, mainly *ad hoc*, solutions. Some of them, such as firewalls as well as anti-virus and encryption software have been effective to a substantial degree.

Because the Internet architecture was not designed with security in mind, incorporating intrinsic security will require substantial changes to the very basis of the Internet, TCP/IP. A new protocol (IPv6) provides some security improvements, but still falls short of a comprehensive solution. Such protection will require considerable modifications to TCP/IP.

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 specifies a minimum rate of data delivery. It is particularly important for applications sensitive to delay, such as live event broadcasting. Frozen, or slow-motion, images and echo in sound are the consequences of bandwidth constraints. The introduction of QoS may require changes in the Internet protocols, including a compromise with one of the Internet's mantras, end-to-end networking.

POSSIBLE FUTURE DEVELOPMENTS

It is realistic to expect growing pressure to change current networking architecture. Some solutions aimed towards higher security and in-

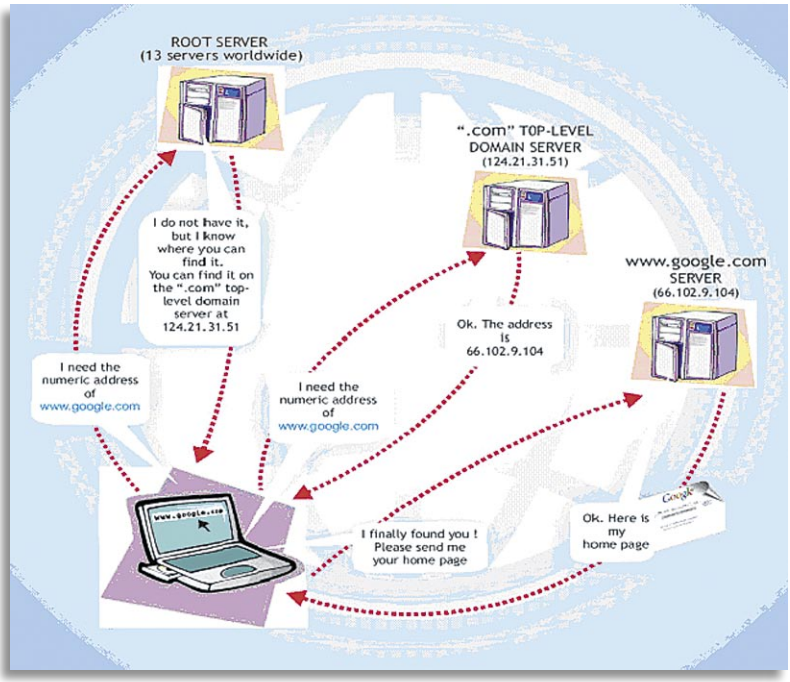
creased bandwidth cannot be achieved without fundamental changes to the Internet Protocol.

Another emerging solution is the construction of various network options on top of the current TCP/IP. It is very likely that private companies will continue to develop such initiatives, which will bypass both the limitations of the current Internet and the uneasiness of the Internet standardisation bodies to change the core Internet principles, mainly "end-to-end networking."

THE DOMAIN NAME SYSTEM (DNS)

THE CURRENT SITUATION

DNS handles Internet addresses (such as www.google.com) and converts them to IP numbers. Thus, to gain access to a particular website, a



computer first has to access a DNS server. This DNS server then finds the numeric address (196.23.121.5 in the case of Google) of that particular site. DNS consists of root servers, top domain servers, and a number of DNS servers located around the world. The management of DNS has been a hot issue in the Internet Governance debate. One of the main controversies is the hierarchical organisation of DNS and the ultimate authority the US government (via the Department of Commerce, DoC) has over it.

DNS is based on two types of top-level domains. One is generic; the other is based on country codes. The generic top-level domains (gTLD) include:

- .com, .edu, .gov, and .mil (in 1984);
- .net and .int (added in 1985); and
- .biz, .info, .name, .pro, .museum, .aero, and .coop (added in 2000).

For each gTLD there is one registry that maintains an address list. For example, the ".com" gTLD is managed by VeriSign. The "salesman" function is performed by registrars. ICANN provides overall coordination of 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 domains involves the protection of trademarks and dispute resolution. In the early days of the Internet, the registration of domain names was based on the principle "first come first served," where anyone could register any name.

The potential value of domain names triggered the phenomenon known as cyber-squatting, the practice of registering domain names that could be resold later on. The impossibility of having two domains with the same name led to a debate on registration rights. The problem was particularly relevant for domain names using famous brand names (e.g. Microsoft, Nike, Toyota, and Rolex).

The reform of DNS management, with the adoption of the Uniform Dispute Resolution Policy (UDRP), has introduced mechanisms that have significantly reduced cyber-squatting. UDRP is only available for .com, .net, and .org domains and does not cover country domains. UDRP jurisdiction is automatically acknowledged when an individual, company,

or organisation signs the domain name registration agreement. UDRP has a few advantages for the challengers of already registered names, usually the holders of traditional trademarks, such as the quick resolution of conflicts through arbitration and the simple implementation of arbitration decisions through direct changes in DNS (avoiding drawn-out court-based procedures).

Another important element in the survey of the current organisation of DNS governance is the management of country code top level domains (ccTLDs). Currently, country codes are managed by a variety of institutions that received accreditation in the early days of the Internet, when some governments were not all that interested in such matters. Such organisations include: academic institutions, technical associations, NGOs, and even private individuals. In many cases, responsibility for managing country codes was assigned on a "first come first served" basis.

THE ISSUES

The Creation of New Generic Domain Names

In the mid-90s, one of the founding fathers of the Internet, Jon Postel, unsuccessfully attempted to add a number of new domains to the existing basic list (.com, .edu, .org, and .int). The main opposition originated from the business sector, whose concern was that increasing the number of domains would complicate the protection of their trademarks. The restrictive approach prevailed, and only a few new domains were introduced by ICANN in 2000 (.biz, .info, .name, .pro, .museum, .aero, and .coop).

Another problem associated with new domains involves the linking of domain names to content. For example, 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 the part of the US country domain.

The Management of Country Domains

The management of country top level domains involves three important issues. The first concerns the very 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, resistance movements, etc.). Jon Postel advocated the allocation of national domain names in accordance with the ISO standard, which is one common source of two-letter abbreviations for countries and other entities. Postel's approach proved successful and continues to be practiced, despite the fact that the ISO list identifies "distinct economic areas" rather than sovereign nations.

The second issue concerns *who should manage country codes*. Many countries have been trying to gain control over their country domains, which are considered to be national resources. 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 quoted 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.

In some cases, country domains have been inappropriately used for the purpose of registering generic top domains, such as listed in the table below:

COUNTRY CODE	COUNTRY	DOMAIN AREA
Tv	Tuvaly	TV stations
Mu	Mauritius	Music
Md	Moldova	Medicine and health
Fm	Federation of Micronesia	Radio
Tm	Turkmenistan	Trademark

Most of the above mentioned countries have been trying to regain control of their country domains. For example, Mauritius initiated an intensive diplomatic lobbying campaign in this direction.

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. Some country domain operators have started creating their own regional organisations such as CENTR (the Council of European National TLD Registries).

The Problem of Languages: Multilingual Domain Names

One of the main limits to the future development of the Internet is the lack of multilingual features for running the Internet infrastructure. Domain names are registered and used in English. Even non-ASCII characters in French or German cannot be used for Internet addresses (e.g. café becomes cafe). The situation is even more complicated with non-Latin scripts such as Japanese, Arabic, and Chinese.

Among the various solutions for multilingual domain names, the most relevant are the Internationalised Domain Name (IDN) and the Native Language Internet Address (NLIA) systems. IDN, a technical solution proposed by IETF, is becoming the dominant solution. IDN translates native names into English domain names on the client machine and sends English domain names for resolving on the DNS. One of the main obstacles to the wider use of IDN is its technical integration within the main Internet browsers such as Internet Explorer.

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. The introduction of an IDN policy will be one of ICANN's main challenges and a test of its inclusive international approach.

ROOT SERVERS

Being 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 DNS can be illustrated by analysing the concern that the Internet would collapse if the root servers were ever dis-

abled. Firstly, 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). If one server crashes, the remaining 12 would continue to function. Even if all 13 root servers went down simultaneously, the resolving of domain names (the main function of root servers) would continue on other domain name servers, distributed hierarchically throughout the Internet.

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 more than 80 worldwide locations. This provides many advantages, including an increased robustness in the DNS system and the faster resolving 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 (six servers), commercial companies (three servers), and government institutions (three servers).

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 DoC, it is entered into the master root server operated by VeriSign under contract with 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 for many governments.

THE ISSUES

Should the Policy Supervision of Root Servers Be Internationalised?

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 the US Department of Commerce, and have suggested adopting a "Root Convention," which would put the inter-

national community in charge of policy supervision of the root servers or, at least, grant nation states rights over their own national domain names. It is not very likely that US institutions (mainly Congress) will accept such proposals. A potential compromise might be based on two elements:

- the transfer of control of root servers from the US Department of Commerce to ICANN, as was initially envisaged;
- the substantive reform of ICANN, leading to the creation of a *sui generic* international organisation, which would be an acceptable institutional framework for all countries.

What is the Likelihood of Creating Alternative Root Servers (e.g. an Internet B)?

As was previously discussed, 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 them 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.

INTERNET SERVICE PROVIDERS (ISPs)

Since IPSs connect end users to the Internet and host websites for many governments, they offer the most direct and straightforward option for the enforcement of government control and legal rules on the Internet. In this text, by ISPs we mean both companies that provide access to individual users and institutional Internet Service Providers (universities, government departments, etc.).

During the Internet boom of the 1990s, ISPs were guarded from any responsibility for content or copyright infringement. It was thought that additional pressure on ISPs might hinder the future development of the Internet. With the growing commercial relevance of the Internet and in-

creasing security concerns, many states have started concentrating their law enforcement efforts on ISPs.

THE ISSUES

The ISP Market and Telecommunications Monopoly

It is common in countries with telecommunications 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 it. 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 to avoid being prosecuted. US and EU legislation provides stronger protection to the holder of the copyright, offering no opportunity for the user of the material to present his case. 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 Role of ISPs in Content Policy

"Don't kill the messenger" is the response of ISPs to growing official pressure on them to enforce content policy. Reluctantly, Internet service providers are gradually becoming involved with content policy. 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.

In many countries, legislation has been adopted where ISPs are burdened with additional responsibilities related to content control; both with what

is available on websites hosted by them and with what is accessed by clients serviced by them. This approach could lead towards additional expenses for ISPs and, ultimately, the higher cost of Internet access for users.

INTERNET BANDWIDTH PROVIDERS (IBPs)

The Internet access architecture consists of three tiers. ISPs that connect end users constitute Tier 3. Tiers 1 and 2 consist of the Internet bandwidth carriers. Tier 1 (Internet backbones) 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. Tier 2 providers usually operate at the national or regional level.

THE ISSUES

Should the Internet Infrastructure Be Considered a Public Service?

Internet data can flow over any telecommunications medium. In practice, facilities such as Tier 1 backbones 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. Two related cases were mentioned in a recent OSCE (the Organisation for Security and Cooperation Europe) report.

In the first case, legal action was launched against a web page with questionable Nazi content hosted by Flashback in Sweden. The courts decided that the page did not violate Swedish anti-Nazi laws. Nevertheless, one committed anti-Nazi activist mounted a strong campaign against Flashback, thereby putting pressure on Flashcomm's ISP, Air2Net, and the main backbone operator MCI/Worldcom. Under pressure from this campaign, MCI/Worldcom decided to disconnect Flashcomm in spite of a lack of any legal basis for doing so. Flashcomm's attempts to find an alternative provider were unsuccessful, since most of them were also connected through the backbone operated by MCI/Worldcom.

The second case took place in The Netherlands where a small Dutch ISP provider, Xtended Internet, was disconnected by its US-based upstream provider under pressure from the Scientology lobby. Ultimately, the functioning of the Internet could depend on the decisions taken by the owners of central backbones. Does the global Internet community have any right to request assurances for the reliable functioning of the critical Internet infrastructure from the major telecommunication operators? Do those companies operate a public facility?

Telecommunications Liberalisation and the Role of ISPs

There are opposing views about the extent to which Internet service providers (ISPs) 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 telecommunications regime applies only to the telecommunications market. The regulation of the ISP market requires new WTO rules.

ECONOMIC MODEL FOR INTERNET CONNECTIVITY

THE CURRENT SITUATION

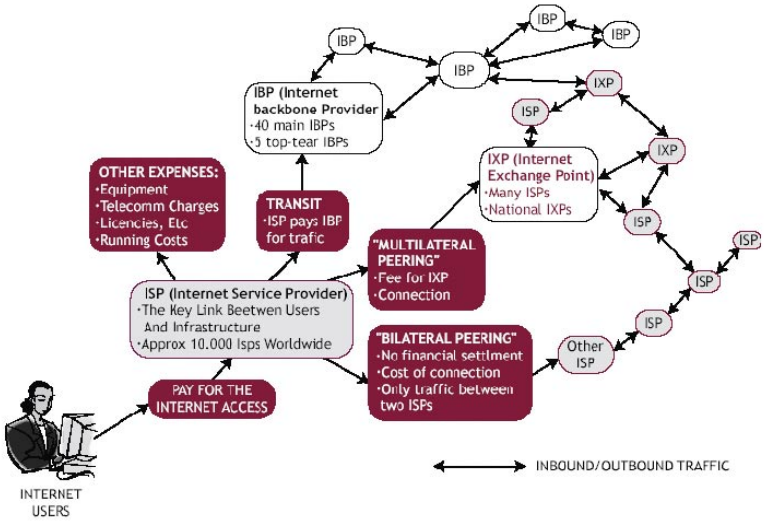
Very often, any discussion of governance-related issues ends up with an analysis of the distribution of money and the sources of income. What is the flow of funds on the Internet? Who pays for the Internet?

There are many financial transactions between the many parties involved with the Internet.

- Individual subscribers and companies pay the ISPs.
- ISPs pay for the services of telecommunications operators and for Internet bandwidth.
- ISPs pay the 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 not only the registrar but also IANA for its services.

- Telecommunication operators pay 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, the costs in this chain are covered by Internet end users, be they individuals or institutions.



THE ISSUES

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

Currently, the cost is covered mainly by the developing countries. Compared to the traditional telephony system, where the price of each international call is shared between two countries, the Internet model puts the entire burden on one side, developing countries, which have to connect to backbones, located mainly in developed countries. Paradoxically, by doing this it could be argued that small and poor countries subsidise the Internet system in developed countries.

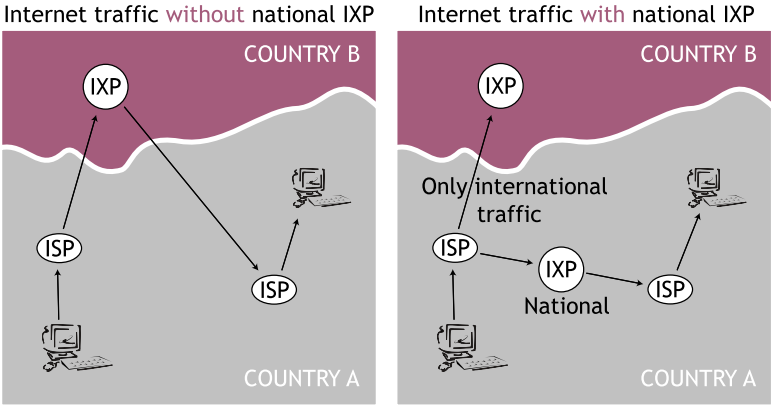
The problem of financial settlements is particularly relevant for the poorest countries, which rely on income from international telecommunications as an important budgetary source. The situation has been fur-

ther complicated with the introduction of Voice over IP (VoIP), Internet telephony, which shifts telephone traffic from national telecommunications operators to the Internet.

The ITU initiated discussions on possible improvements in 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, the adopted ITU Resolution, D. 50, is practically ineffective.

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

IXPs are technical facilities through which different ISPs exchange Internet traffic. 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.



IXPs can also play an important role in reducing the digital divide. For example, in the case of a country without national IXPs, a considerable part of traffic between the clients within the country needs to be routed through another country. This increases the volume of long distance international data traffic and the cost of providing Internet service.

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.

OPEN SOURCE

The code for open source software is made available free of charge. Open source applications are developed by programmers from around the world working on the same code.

When it was introduced, open source promised to be an efficient alternative to expensive proprietary software. Linux is the most well-known open source initiative. The proliferation of open source software has been slower than expected, mainly due to the lack of solid technical support. The latest decision by some key players, such as IBM and Intel, to use Linux, the main open source platform, could lead towards the successful development of this approach.

Moreover, there is a renewed interest in open source under a new name and slightly modified concept, titled Free/Libre Open Source Software (FLOSS). The main difference between open source and FLOSS is that FLOSS enables free access to code without any registration.

Open source is often put forward as the solution to the development of ICT capabilities in developing countries. At the WSIS, an attempt by civil society and some developing countries to introduce open source and FLOSS in the final document as a solution for overcoming the digital divide was watered down with a general reference to "different software models, including proprietary, open-source, and free software."

CONVERGENCE: INTERNET-TELECOMMUNICATION-MULTIMEDIA

The broad and prevailing use of the Internet Protocols has triggered the process of the convergence of telecommunication, multimedia, and entertainment systems. Today, it is possible to make telephone calls, listen to radio, watch TV, and share music, over the Internet. In the field of traditional telecommunications, the main point of convergence is the Voice

over Internet Protocol (VoIP). The growing popularity of VoIP is based on lower price, the possibility of integrating data and voice communication lines, as well as the use of advanced PC-based tools. TCP/IP is also becoming dominant in the field of multimedia and entertainment. While technical convergence is going ahead at a fast 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 previously operating in separate domains into direct competition. It remains to be seen who is going to take the lead in this increasingly convergent market, telecommunications companies such as MCI or ICT companies such as IBM.

The same applies to the multimedia market, although in this field a few companies have reacted to the challenge posed by convergence by developing both IT and media/entertainment or forming partnerships. Sony is one company that has developed both ICT and media/entertainment capabilities. The merger of America Online and Time Warner was aimed at combining telecommunications 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 of these segments: telecommunications, media/entertainment, and ICT, 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 fields such 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 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 end-to-end networking principle.

The main difference between traditional dial-up 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 "telecommunications service." If it is the latter, it will have to be regulated through common carrier rules.

INTERNET SECURITY

THE CURRENT SITUATION

Internet security came into sharper focus with the rapid expansion of the Internet user base. The Internet has proven what many have 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.

The side-effect of the fast integration of the Internet in almost all aspects of human activities increases the vulnerability of modern society. 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 are known to cause severe disruption and have potentially high financial impact, critical infrastructures are frequent targets.

Information security is discussed in more detail in three other booklets in this series:

- Good Hygiene for Data and Personal Computers
- Information Security and Organisations
- Hacktivism, Cyber-terrorism and Cyber-war

Internet security issues can be classified according to three criteria: type of action, type of perpetrator, and type of target.

A classification based on type of action would include: data interception, data interference, illegal access, spyware, and identity theft. Possible perpetrators might include hackers, cyber-criminals, cyber-warriors, or cyber-terrorists.

The potential targets are numerous, from individuals, private companies, and public institutions to critical infrastructures, governments, and military assets.

POLICY INITIATIVES IN THE FIELD OF INTERNET SECURITY

There are many national, regional, and global initiatives focussing on Internet security.

At the national level is a growing volume of legislation and jurisprudence dealing with Internet security. The most prominent are US initiatives linked to the broader authority of the state in its fight against terrorism. The Department of Homeland Security is the main institution dealing with questions of Internet security. It is difficult to find any, mainly developed, country without some initiative focussing on Internet security.

At the international level, the most active organisations have been the OECD, which produced its Guidelines on Information Security, and 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).

The G8 has also proposed a few initiatives in the field of Internet security, such as improving cooperation between law enforcement agencies. The G8 also formed a Subgroup on High-Tech Crime to address the establishment of 24x7 communication between the cyber-security centres of member states, the training of staff, and the improvement of the legal systems of nation states in order to combat cybercrime and promote cooperation between the ICT industry and law enforcement agencies.

The United Nations General Assembly has passed several resolutions on a yearly basis on "Developments in the field of information and telecommunications in the context of international security," specifically resolutions 53/70 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 had similar content without any significant improvements. They do not reflect the considerable changes that have been taking place in the field of Internet security since 1998.

A major international legal instrument related to Internet security is the Council of Europe Convention on Cybercrime, which entered into force on 1 July 2004.

Some countries have established bilateral arrangements. The US has bilateral agreements on legal cooperation in criminal matters with more than 20 other countries. These agreements are also used in cases of cybercrime.

One attempt by academics and non-state actors to draft an international agreement is the Stanford Draft Convention on Protection from Cyber Crime and Terrorism. This draft recommends the establishment of an

international body, named the Agency for Information Infrastructure Protection (AIIP)

THE ISSUES

Internet Architecture and Security

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

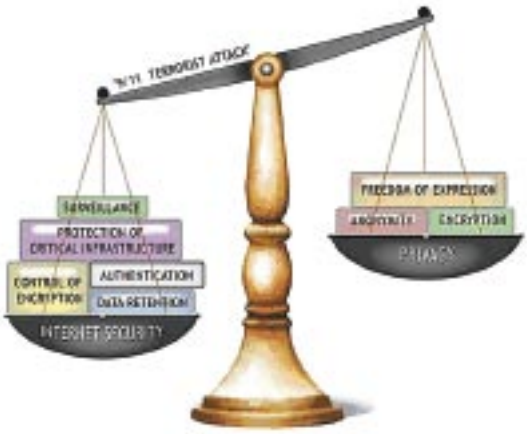
It is unclear whether the IETF will be able to change e-mail standards in order to provide proper authentication and, ultimately, reduce the misuse of the Internet (e.g. spam, cybercrime). Given the controversy surrounding any changes to the basic Internet standards, it is likely that security-related improvements of the basic Internet Protocol will be gradual and slow. The business sector and other parties interested in faster solutions may start developing new layers, "the smart Internet," which would facilitate, among other things, more secure Internet communication.

E-commerce and Internet Security

Security is very often mentioned as one of the preconditions for the faster growth of e-commerce. Without a secure and reliable Internet, customers will continue to be reluctant to provide confidential information online, such as credit card numbers. The same applies for online banking and the use of electronic money.

Privacy and Internet Security

Another debated issue is the link between security and human rights. Does more Internet security require some loss of privacy? How should the use of encryption software be regulated, which can be used both for the legitimate protection of privacy of communication and for the protection of the illegal communications of terrorists and criminals? This balance between Internet security and human rights is constantly shifting.



In the aftermath of "9/11," 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.

The question of balance between IT security and privacy was highlighted in discussions about the possibility of extending the Council of Europe Convention on Cybercrime to the global level. The main objection from human rights activists is that the convention addresses Internet security 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 and intelligence agencies to monitor potential criminal and terrorist activity remains an issue.

The international aspects of encryption policy are relevant to the discussion of Internet Governance 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 of introducing 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 was 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 was 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 impacts 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 13 e-mail messages sent, 10 may be categorised as spam. Besides the fact that it is annoying, spam also causes considerable economic loss, both in terms of used bandwidth and time lost on checking/deleting it. A recent EU-commissioned study 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 impact and have to be complemented with specific 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 bal-

ance between allowing e-mail based promotion and preventing spam. 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 do not evidence a decrease in the number of spam messages.

In July 2003, the European Union introduced its own anti-spam law as part of its directive on privacy and electronic communications. In spite the EU's requirement for member states to implement this anti-spam law by the end of 2003, nine member states did not observe this deadline. The EU law encourages self-regulation and initiatives by the private sector that would lead towards a reduction in spam.

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 for some countries such as Canada, which, according to the latest statistics, receives 19 out of 20 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 the 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 international treaty or some similar mechanism.

Spam and Development

Spam is causing serious, but still manageable, difficulties in developed countries while crippling the Internet infrastructure of many developing countries. Given the low-speed and underdeveloped Internet infrastructure, spam threatens the basic access to the Internet for many users from developing countries. Those countries usually lack the technical resources and expertise to combat spam. Consequently, spam widens the existing digital divide between the developed and the developing countries.

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 (7-9 July 2004) and 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 Telecomm, Comcast, EarthLink, Microsoft, and Yahoo!. They established the Anti-Spam Technical Alliance (ASTA), whose main task is coordinating technical and policy anti-spam activities.

THE ISSUES

Different Definitions of Spam

Different understandings on what spam is 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 e-mail" regardless of its content. Since most spam is generated from the US, this difference in definitions seriously limits any possibility for introducing an effective international anti-spam mechanism.

Spam and E-mail Authentication

One of the structural generators 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 standards for e-mail. The IETF is working on introducing changes in 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 curbing of anonymity on the Internet.

The Need for Global Action

As was stated above, most spam originates from abroad. It is a global problem requiring a global solution. There are various initiatives that

could lead towards better global cooperation. Some of them, such as bilateral Memorandums of Understanding (MOUs), have already been mentioned. Others include such actions as capacity building and information exchange. A more comprehensive solution would involve some sort of global anti-spam instrument. Some participants at the latest ITU meeting proposed the adoption of a multilateral MOU or the adoption of an instrument in the context of WSIS. 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.

SECTION 3

The Legal Basket

THE LEGAL BASKET

Almost every aspect of Internet Governance has a legal component, yet the shaping of a legal response to the rapid development of the Internet is still in its infancy. The two prevalent approaches to the legal aspects of the Internet are:

a) A "real law" approach, where the Internet is essentially treated no differently from previous telecommunication technologies, from smoke signals to the telephone. Though faster and more comprehensive, the Internet still involves communication over distance between individuals. Consequently, existing legal rules can be applied to the Internet.
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" for 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 have valid elements, the real law approach is gaining predominance in both theoretical analysis and policy. The general thinking is that a considerable part of existing legislation can be applied to the Internet. In certain cases, however, such as trademark protection, the rules of real laws would have to be adapted in order to apply to the cyber world. Other cases, such as spam, must be regulated by newly designed rules. The closest real world analogy to spam, junk mail, is not illegal.

This discussion about legal concerns is divided into two parts: legal mechanisms and legal issues.

LEGAL MECHANISMS

The following legal mechanisms have either already been applied or could be applied to Internet Governance:

- Legislation;
- Social norms (customs);
- Self-regulation;
- Regulation through code (software solution);
- Jurisprudence (court decisions);
- International law.

Legislation

Every piece of legislation consists of rules and sanctions. Rules stipulate certain 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).

Regardless of the "real" or "cyber" reality, 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.

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

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

Information Society Governance

The law always lags behind technology

Social Norms (Customs)

Like legislation, social norms prescribe 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, as well as other documents, 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 control. 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 tool in this field, some risks remain in using it for regulating areas of high public interest, such as content control. 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, or court decisions, is an important element of the Anglo-Saxon 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 23-26.

International Regulation

One common view about Internet Governance is that the global nature of the Internet requires global regulation. The need for a global approach is frequently confirmed by the lack of effectiveness of national measures against spam or cybercrime and other undesirable activities. The civil aviation regime is usually mentioned as an example of a successful universal regime for combating crime. "Since the adoption of the civil aviation treaties, sabotage and acts of unlawful interference have steadily declined." One of the main reasons is that with universal legal coverage of civil aviation, criminals can no longer easily find a "safe haven." At the same time, the importance of a global approach does not mean that some issues cannot or should not be regulated at the national and regional levels.

Global regulation will require a universal consensus, achievable only through a long negotiation process, if at all. Various international law mechanisms might be used in the development of an Internet Governance regime. According to the Statute of the International Court of Justice, international legal resources are divided into: treaties, customs, and general principles. On top of that is "soft law," an increasingly important resource of international law.

Treaty Law. Currently, the only convention that deals directly with Internet-related issues is the Council of Europe Cybercrime Convention, but other instruments are applicable. One example is the corpus of human rights conventions. Freedom of expression is protected by Article 19 of the Covenant on Political Rights. Other Internet-related rights, such as privacy and the right to information are regulated by global and regional human rights instruments. In the field of dispute resolution, one of the main instruments is the New York Convention on Arbitrations.

The prevailing approach to Internet Governance (national vs. international, soft vs. hard law) will ultimately influence the type and the form of the IG convention, if any. Some argue that the Internet will require a comprehensive legal instrument, such as the Convention of the Law of the Sea. This analogy is not appropriate, since the Law of the Sea negoti-

ation involved the codification of existing customary law and the integration of four existing conventions.

With the Internet, no customary law exists. It is being constantly fashioned. Many trial-and-error approaches and experiments have been attempted. Instead of a comprehensive Internet treaty, it is more likely that several separate instruments will be adopted.

Customary law. The development of customary law usually requires a longer time-span, for the crystalisation of some legally-binding practices. This was possible in the past. However, technological development after the Second World War required the rapid development of international regulatory frameworks, given the profound economic and political consequences that these changes generate in a very short time-span. The Internet is a good illustration of this tendency. It is not very likely that customary law will play a dominant role within any Internet Governance regime.

"Soft law." Soft Law is usually related to various political documents, such as declarations, guidelines, and model laws. The linguistic criterion for identifying a "soft" law is the frequent use of the word "should," in contrast to the use of the word "shall," which is usually associated with a more legally-binding approach codified in "hard" law (treaties).

Many instances of soft law arrangements have been observed by participatory states. Some of them had considerable importance, such as the Helsinki Act from 1975, which established the framework for East-West relations. Soft law is used by states for various reasons, such as mutual confidence-building, stimulating development in progress, and introducing new legal and governmental mechanisms. Soft law can be a potentially applicable legal technique for Internet Governance.

JURISDICTION

INTRODUCTION

Jurisdiction is the Internet Governance issue requiring the most urgent attention. The number of Internet-related disputes has been steadily increasing. Confusion over jurisdiction can potentially have two immediate consequences:

- the state's inability to exercise its legal power as a responsible entity in regulating social relations within its territory;
- the inability of individuals and legal entities to exercise their right to justice (denial of justice).

Other potential consequences of ambiguous jurisdiction might be:

- legal insecurity on the Internet;
- slower development of e-commerce;
- compartmentalisation of the Internet into legal safe zones.

What is the relationship between jurisdiction and the Internet?

The relationship between jurisdiction and the Internet has a built-in ambiguity, since jurisdiction is based 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 exchanges, difficult (although not impossible) to monitor via traditional government mechanisms. The question of jurisdiction on the Internet exposes one of the key dilemmas associated with Internet Governance: how is it possible to "anchor" the Internet within existing legal and political geography?

Jurisdiction – Basic Techniques

There are three main aspects to jurisdiction:

- Which court or state authority has the proper authority? (procedural jurisdiction);
- Which rules should be applied? (substantive jurisdiction);
- How should court decisions be implemented? (enforcement jurisdiction).

The following main criteria are used for establishing jurisdiction in particular cases:

- Territorial Link – the right of the state to rule over persons and property within its territory;
- Personal Link – the right of the state to rule over its citizens wherever they might be located;
- Effects Link – the right of the state to rule on the economic and legal effects on a particular territory, stemming from activities conducted elsewhere.

Another important principle introduced by modern international law is the principle of universal jurisdiction for cases of genocide, piracy, and human trafficking that involve breaches of core international legal norms (*ius cogens*).

THE CURRENT SITUATION

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 can be accessed from anywhere, any Internet user can potentially be exposed to any national jurisdiction. When placing content on the Web, 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 towards multiple jurisdictions or a so-called spillover effect.

The two most illustrative and frequently quoted cases that exemplify the problem of jurisdiction are the 1996 CompuServe Case in Germany and the 2001 Yahoo! Case in France.

In the CompuServe Case, a German court requested CompuServe to ban access to pornographic materials. In order to observe German law, CompuServe had to remove such materials from its central web server in the US. As a result, it disabled access even for those citizens living in countries (e.g., the US) where access to pornographic materials was not prohibited by law. CompuServe had to accept the most restrictive legislation in this field. This case prompted the fear that the whole Internet would have to adjust to the most restrictive legislation (the least common denominator principle).

A few recent cases, including the Yahoo! Case prosecuted in French courts, reiterated the high relevance of the problem of multiple jurisdictions. The Yahoo! Case was prompted by a breach of French laws on Nazi materials. These laws prohibited anyone in France from accessing a Yahoo! website displaying Nazi memorabilia, even though the website was hosted in the US, where the display of such materials was, and still is, legal.

The real law approach argues that nothing new can be found in cases such as CompuServe, since many examples of the spillover effect occur in the non-Internet world. One well-known example is the the EU Commission's establishment of strict conditions for the otherwise US approved merger of Boeing and McDonnell Douglas. Although neither

company had production facilities in Europe, they still had to observe EU competition law, in order to sell aeroplanes in the EU.

While the "real law" reasoning is sound in principle, it does have serious practical flaws, which would limit the applicability of existing law to the Internet. The main problem is the sheer size of potential Internet-related cases, with almost every website/service being exposed to potential legal action somewhere in the world. Thus, the quantitative aspect (the number of cases) may challenge the legal principle and prompt new solutions.

POTENTIAL SOLUTIONS

Potential solutions for the multi-jurisdiction problem in regard to the Internet might be found in:

- modernisation of international private law;
- harmonisation of national laws, which would make the question of jurisdiction less relevant;
- use of arbitration;
- use of technical solutions for identifying the origin of users (primarily, geo-location software).

The Modernisation of International Private Law

In traditional legal procedures, national courts decide whether they can judge a particular case and which rules should apply. Decisions involving both procedural and substantive jurisdiction are based on international private law ("conflict of laws" in Anglo-Saxon legal systems). Those rules specify the criteria for establishing jurisdiction, such as the link between the 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). The Internet makes the application of these criteria more complex than in traditional cases, but not impossible.

The traditional approach is used rarely for settling Internet-related disputes due to its complexity, slowness, and high cost. It also does not fit into the Internet *modus operandi*, which is fast, simple, and pragmatic. The main mechanisms of international private law were developed at a time when cross-border interaction was less frequent and intensive. Proportionally, fewer cases involved individuals and entities from different jurisdictions. With the advent of the Internet, cross-border interaction is commonplace. Communications, exchanges, and disputes between in-

stitutions and individuals from different countries are much more frequent and intense than hitherto.

A potential solution might be the modernisation of international private law, in order to have a fast and low cost process for the assignment of national jurisdictions in Internet cases. Possible improvements might include simplified procedures for identifying appropriate jurisdictions, the option of online deliberation, and flexible arrangements for legal counselling.

At the regional level, the European Union has adopted the Brussels Convention, which simplifies the process of reaching decisions on jurisdiction and favours the protection of customers in the case of e-commerce.

At the global level, the main venue for the development of international private law is the Hague Conference. Current negotiations have been dominated by the United States. In 1992, the US initiated negotiations on jurisdiction with the main objective of strengthening the protection of intellectual property through the global enforcement of US court decisions. Since 1992, the growth of the Internet and e-commerce has changed the negotiation landscape. It is becoming increasingly risky for US Internet companies to operate in an environment of multiple jurisdictions. Both the CompuServe (Germany) and the Yahoo! (France) cases have shown how content hosted in the US can trigger court cases in other countries.

Internet "Flags of Convenience"

Another potential consequence of a lack of harmonisation will be the migration of "data" and web materials to countries with lower levels of content control. Using the analogy of the Law of the Sea, some countries might become "flags of convenience" or the "offshore" centres of the Internet world.

If the initial proposal of the Hague Convention were to be adopted, it would pose a considerable challenge to the US legal system. US courts would have to enforce foreign court judgements, which would involve content on US-hosted websites and would ultimately challenge the freedom of speech enshrined in the First Amendment to the US Constitution. This possibility caused a change in the US position and reduced ambitions for reforming the international private law system. The lack of progress in the modernisation of international private law at the global level could strengthen other options.

The Harmonisation of National Laws

The harmonisation of national laws should result in the establishment of one set of equivalent rules at the global level. With identical rules in

place, the question of jurisdiction should become less relevant. Harmonisation can 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 Internet security. However, in some fields, including content policy, it is not very likely that a global consensus on the basic rules will be reached.

Another option for solving the jurisdiction problem is arbitration, which is discussed below.

ARBITRATION

Arbitration is an alternative dispute resolution mechanism that can be used instead of, usually, slow and complex juridical procedures. 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 are available, specifying such issues as place of arbitration, procedures, and choice of law.

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.

Online arbitrations are also used for solving not only Internet but also regular commercial disputes. Online arbitration is conducted completely over the Internet, including the presentation of evidence and rulings.

Arbitration has particular advantages when it comes to one of the most difficult tasks in Internet court cases, enforcement of decisions (awards). The enforcement of arbitration awards is regulated by the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, signed by the majority of countries. According to this convention, national courts are obliged to enforce arbitration awards. It is simpler to enforce arbitration awards than foreign court judgements.

Arbitration has been used extensively in order to fill the gap engendered by the inability of current international private law to deal with Internet cases. A particular example of the use of arbitration in Internet cases is the Universal Domain Name Dispute Resolution Policy (UDRP). The UDRP was developed by WIPO and implemented by ICANN as the key dispute resolution procedure. UDRP is stipulated in advance as a dispute resolution mechanism in all contracts involving the registration of gTLDs (.com, .edu, .org, .net). The 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 as 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 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 would be a more delicate proposition when it came to content and socio-cultural aspects, where a national legal system reflects specific cultural content.

Fourth, existing Internet-related jurisprudence indicates that arbitrations, such as those based on UDRP, have been more receptive to the interests of the business sector than to those of individuals. Here is an example dealing with two similar cases. First, an ordinary French court ruled against the French company "Danone," and for the disgruntled employee who had registered the domain "jeboycottedanone.com" (I boycott Danone). Yet, in a second case, WIPO arbitration (UDRP) accepted Vivendi Universal's request to remove the website "vivendiuniversalsucks.com." In both cases, domain names were used as a means of protest and criticism. An ordinary court in France accepted this type of protest, while WIPO arbitration did not.

INTELLECTUAL PROPERTY RIGHTS

Knowledge and ideas are the key resources in the global economy. Their protection, through Intellectual Property Rights (IPRs), is becoming one of the most important Internet issues, with considerable legal and political consequences. IPR issues cover various Internet Governance aspects. Since knowledge and ideas are an important part of cultural heritage and social interaction, they retain a special value for many societies. IPRs are also at the core of the development debate. Various aspects of IPRs make them complex and challenging to manage. Internet-related IPRs include trademarks, copyrights, and patents.

TRADEMARKS

The relevance of trademarks to the Internet is related to 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 business companies and selling them later for a higher price. With the growing importance of the Internet, this became a major problem, because companies were open to being misrepresented on the Internet. Legal remedies through regular court systems were not very practical since such cases took too long to resolve.

This situation compelled the business sector to place the question of 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 ICANN, the US government requested ICANN to 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).

The use of UDRP as a dispute resolution mechanism was a compulsory stipulation in all domain registration contracts for top level domains, such as .com, .org, and .net. Trademark holders increasingly encourage the extension of UDPR to country domains.

Trademarks are also tackled in the following parts of the booklet:

- The Domain Names System (p. 41);
- Universal Dispute Resolution Procedure – UDRP (p. 79).

COPYRIGHT

The traditional concept of copyright has been challenged by Internet developments 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. Materials can be copied and distributed worldwide by means of the Internet without significant cost.

These developments endanger the delicate balance between the interests of the authors of protected materials and the public interests of increasing creativity, public knowledge, and general well-being. Preventing the unlimited copying of materials and, at the same time, safeguarding Internet access to those materials is one of the conundrums of Internet Governance. 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.

Copyright protects only the expression of an idea as materialised in various forms, such as book, CD, computer file, etc. The idea itself is not protected by copyright.

One of the watershed developments in the field of copyrights, triggering an active response by copyright holders, was music-sharing through peer-to-peer networks. It is estimated that Napster, the prime example, brought about losses of $4.3 billion to the music recording industry. The reaction of the music recording industry brought to light the many pitfalls, erroneous analogies, and insufficiencies of the current legal system. It is also an illustration of the current status of copyright protection on the Internet and of the numerous remaining open issues.

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 WIPO Copyright Treaty (1996). This treaty also provides 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 StreamFast, two companies that produce P2P file-sharing software. Following DMCA-provisions, the US Record Association requested these companies to desist with the development of file-sharing technology that contributes to the infringement of copyrights. By stressing analogy, the court indicated that Grokster and StreamFast, like the developers of VCRs and photocopy machines, did not envisage the use of their software for copyright infringement under reasonable circumstances.

Software Against Copyright Infringement

Tools that are used by offenders can be used by defenders too. Traditionally, state authorities and businesses enacted 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 TRIPS and WIPO's 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 academ-

ic 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 protected by foreign entertainment and media companies.

WIPO and TRIPS

Two main international regimes exist for copyright protection. 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. 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 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.

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.

For Internet Governance, the main development was the flexible granting of patent protection to business processes on the Internet, such as the "1-Click" procedure used by Amazon.com. The main criticism of this decision is that Amazon protected only the idea (the use of one click), not a particular business process.

The successful registration of the "1-Click" patent triggered a wave of registrations, including some ridiculous proposals, such as a patent on Internet downloading. Another controversial case is British Telecom's request for licence fees for the patent of hypertext links, which it registered in the 1980s. If British Telecom wins this case, Internet users will have to pay a fee for each hypertext link created or used. Otherwise, it will go down in history together with such cases as the attempt to patent the wheel.

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.

CYBERCRIME

Technology is developed to be **used**, but it is very often also mis**used** or even ab**used**. In general, cybercrime deals with the abuse of information and communications technology. While the "crime" part of the term has been clearly defined (e.g. theft, child pornography), opinions about the meaning of "cyber" abound.

A dichotomy between "real" and "cyber" law exists in the discussion of cybercrime. The real law approach stresses that cybercrime is merely offline crime, committed with computers. The crime is the same, only the tools are different. The cyber law approach stresses that 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.

The convention regulates computer-related fraud, infringements of copyright, child pornography, and network security. The recently adopted protocol to the convention adds the distribution of racist or xenophobic content as another crime regulated by the convention.

The convention specifies various procedural mechanisms for the anticrime activities of states, such as sharing data related to cybercrime, including Internet traffic logs. Internet service providers are assigned special responsibilities in this cybercrime regime, including the obligation to preserve users' Internet logs and to facilitate lawful interception in support of the gathering of evidence. It remains to be seen whether the convention will be ratified by the US Congress; such ratification would be an important step towards global coverage.

Besides the Council of Europe, the G-8 adopted an Action Plan that specifies coordinated action on the following Internet-related crimes: paedophilia and sexual exploitation, drug-trafficking, money-laundering, electronic fraud, as well as industrial and state espionage.

In 2003, the OECD produced guidelines to assist governments in combating Internet-related fraud. The European Union initiated the process for adopting the Framework Decision on Cybercrime, strengthening practical measures and cooperation in the field of cybercrime.

THE ISSUES

Definition of Cybercrime

The definition of cybercrime is one of the core issues with a practical legal impact. Many serious differences occur in the interpretation of cy-

bercrime and this could have a direct impact on the effectiveness of the international cybercrime regime.

For example, if the focus of the definitions of cybercrime is on the method – such as the unauthorised access to secure computer systems – there is a potential risk of confusing cybercrime with hacktivism (digital civil disobedience).

Cybercrime vs. 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.

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 found in the network logs that provide information about who accessed particular Internet resources, and when they did so. The Convention on Cybercrime has some provisions dealing with this issue.

DIGITAL SIGNATURES

Broadly speaking, digital signatures are linked to the authentication of individuals on the Internet and this impacts 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 concluding 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 forced by pressure to establish an e-commerce enabling environment, many governments started adopting legislation on digital signatures. The main challenge has been that governments are not regulating an existing problem, such as cybercrime or copyright, but creating a new 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. The first is a "minimalist" approach, specifying that electronic signatures cannot be denied on the grounds that 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 "maximalistic," 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 that can certify future users of digital signatures. This approach prevails in the laws of European countries such as Germany and Italy.

The third approach, adopted in the EU Digital Signatures Directive, combines the two above-mentioned approaches. It has a minimalistic provision for the recognition of signatures supplied via an electronic medium. The maximalistic approach is also recognised through granting that "advanced electronic signatures" will have stronger legal effect in the legal system (e.g. easier to prove these signatures in court cases).

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 remains. Only eight countries have implemented the directive's requirements that digital signatures should be treated in the same way as regular ones.

At the global level, in 2001 UNCITRAL adopted the Model Law on Electronic Signatures. The model law 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.

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

Need for Detailed Standards for Implementation

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

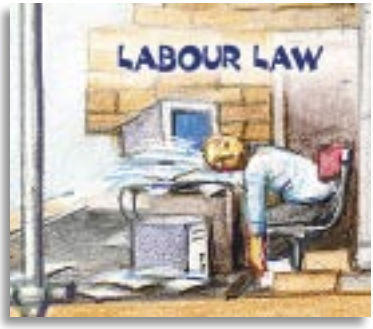
Risk of Incompatibility

The variety of approaches and standards in the field of digital signatures could lead towards the incompatibility of 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.

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 issues such 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 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.

PRIVACY AND DATA PROTECTION

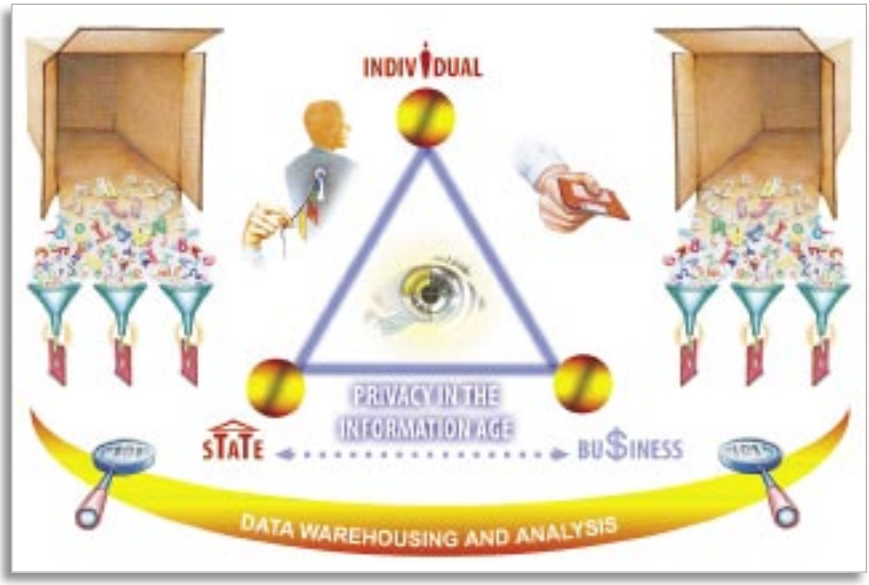
Privacy and data protection are closely interrelated Internet Governance issues. Data protection is a legal mechanism that ensures privacy.

What is privacy? The definition of privacy depends on individual perspectives. Some individuals do not mind disclosing some private information, while others guard their privacy more closely. Privacy is also determined by national cultures. Although the issue of privacy is important in western societies, it may have lower importance in other cultures.

Nevertheless, keeping in mind these caveats, privacy needs to be defined before it can be used as a legal concept. Definitions range widely. One traditional definition describes privacy as "the right to be left alone." Modern definitions of privacy focus on privacy of communication (no surveillance of communication) and information privacy (no handling of information about individuals). Traditionally, privacy was related, mainly, to the relationship between citizens (individuals) and the state. However, nowadays, the privacy framework has been extended and now also includes the business sector, as reflected in the drawing on the next page.

Privacy Protection: Individuals and States

Information has always been an essential commodity for state authorities' oversight of their territory and population. This can be gleaned from the oldest written records, most of which deal with state functions. Information technologies have enormously enhanced the state's capabilities to gather and analyse information. This includes both information managed by government departments (tax, social security, health, property, criminal records) as well as companies licensed by governments to provide essential services (electricity, water, telecommunications).



All of this information is collected with the implicit but involuntary agreement of the citizenry, as it is not possible for an individual to opt-out of these schemes, short of emigrating to another country, where he would be confronted with the same problem anyway.

Technologies, such as data warehousing, are used to aggregate and relate data from many individual systems (for example taxation, housing records, car ownership) in order to conduct sophisticated analyses, searching for patterns, inconsistencies, unusual patterns, and other discoveries. They could have a dramatic impact on society and, in most cases, still remain within the scope of the Universal Declaration of Human Rights.

Terrorism, espionage, and other activities against a state have given rise to the increased surveillance of suspect individuals (be they nationals of the state or not). Civil liberties campaigners warn of the gradual erosion of personal privacy through the introduction of ever more stringent national security measures.

A few years ago, the proposal to equip personal computers with a processor chip that would give them a unique identity (the "Clipper" chip), which coincidentally (or not) could also have been used to provide a back-door for government surveillance, caused considerable public furo-

re. The Clipper chip battle was won by the libertarians, but the pendulum is swinging back towards strengthened national security.

After 9/11 the US "Patriot Act," and comparable legislation in other countries, introduced a framework for the stricter control of electronic communications, including a provision for Lawful Interception. The concept of Lawful Interception in support of the gathering of evidence is also included in the Council of Europe's Convention on Cybercrime of 2001 (Articles 20 and 21).

More powerful surveillance tools will emerge as technology evolves, which could further strengthen the role of the state while further reducing the privacy of individuals.

Privacy Protection: Individuals and Businesses

In this privacy triangle, the second, and increasingly important, relationship is the one between individuals and the business sector. In an information economy, information about customers, including their preferences and purchase profiles, becomes an important market commodity. Selling data about customers is a very lucrative business on the Internet.

A different kind of "surveillance" exists between individuals and businesses, and particularly so in the case of electronic commerce.

Here, millions of individuals willingly disclose considerable amounts of personal information to business organisations: credit card numbers, address details, and other information that, if used inappropriately could lead to serious consequences, such as fraud or identity theft.

The success and sustainability of electronic commerce, both business-to-customer and business-to-business, depend on the establishment of extensive trust both in the businesses' privacy policies and in the security measures businesses set up to protect their clients' confidential information from theft and misuse.

Business organisations also exploit data warehousing technologies to gain an insight into the habits and preferences of their clients. Supermarkets use loyalty card schemes to track the buying habits of their customers, what day of the week/time of day they prefer to shop, how much they spend, which products they buy (as the data warehouse is also linked to point of sale equipment).

The results of these analyses are subsequently used to target personalised marketing initiatives at individual households. If there is no data

protection legislation in place, information about individuals gathered by businesses may be sold and used in other contexts.

Privacy Protection: State and Business

This third side of the triangle is the least publicised and possibly the most relevant. Both sides, state and business, collect considerable amounts of data about individuals. It has been reported that some of this data was exchanged within the context of anti-terrorist activities. However, in some situations, such as in the case of the European Directive on Data Protection, the state supervises and protects data about individuals held by business companies.

Privacy Protection: Individuals-Individuals

The last aspect of privacy protection, not represented within the triangle scheme, is the potential risk to privacy from individuals. Today, technology has empowered individuals with powerful surveillance tools. Even a simple mobile phone with camera can become a surveillance tool. Nowadays, more sophisticated miniature cameras and microphones can be bought at affordable prices. Technology has "democratised surveillance," to quote *The Economist*. Many instances of the invasion of privacy have been documented, from simple voyeurism to the more sophisticated use of cameras for recording card numbers in banks and electronic espionage.

The main problem is that most legislation is focussed on the privacy risks stemming from the state. Faced with the 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. Similar privacy laws, preventing individual surveillance, were also adopted in Germany and a few other countries.

The International Regulation of Privacy and Data Protection

The main international document on privacy and data protection is the OECD's "Guidelines on Protection of Privacy and Transborder Flows of Personal Data" from 1980. These guidelines and the subsequent work of the OECD have inspired many international and regional regulations in this field. The principles proposed in the OECD Guidelines have been widely accepted. The main differences lie in the way in which those principles are implemented.

One approach, used in the US, is based on self-regulation. Privacy policies are set by business companies. It is up to companies and individuals to decide about privacy policies themselves. The main criticism of this approach is that individuals are put in a comparatively weaker position.

According to the second approach, promoted by the European Union, the protection of privacy should be ensured by public authorities. This approach to privacy, promoted in the 1995 European Directive on Data Protection (95/46/EC), covers the protection of individuals with regards to the processing of personal data and on the free movement of such data. Besides the European Directive, which is the main mechanism, the European approach to privacy and data protection is also shaped by other regional instruments, such as the Council of Europe's Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

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

The conflicting views on e-privacy protection between the EU and the US confirmed that increasing interdependence created by electronic commerce can challenge some basic principles embedded in their respective social and cultural histories. Globalisation will cause this issue to reappear with the participation of other societies. The "Safe Harbour Agreement" should be seen as a valuable precedent and a useful tool for formulating similar arrangements between the EU and other countries, including Canada and Australia.

SECTION 4

The Economic Basket

THE ECONOMIC BASKET

The importance of the economic aspect of Internet Governance is illustrated by the title of the document that initiated the reform of Internet Governance and established ICANN: "Framework for Global Electronic Commerce" (1997). The Framework 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 regime.

Various policy and regulatory mechanisms of high importance for e-commerce are classified in other baskets.

The Infrastructure and Standardisation Basket:

- The introduction of *broadband access* and *quality of service* is a precondition for the faster growth of e-commerce in the multimedia field (e.g., in the distribution of movies and songs).
- *Internet security* should increase reliability and robustness of the e-commerce environment. It should also help in building consumers' trust in e-commerce.
- *Encryption* is crucial for the protection of communications, especially in financial transactions.

The Legal Basket

- *Jurisdiction* is important for the legal reliability of e-commerce, in particular to consumer protection.
- The importance of *intellectual property rights* for e-commerce is linked to the increased volume of e-commerce transactions of intangible products.
- *Digital signature* facilitates easier transactions online and solves the problem of authentication.
- With more information about individuals gathered in e-commerce, *data protection* provides essential protection of the privacy of individuals.

E-COMMERCE

The choice of a definition for e-commerce has many practical and legal implications. Depending on the classification of a particular transaction as e-commerce specific rules are applied, such as those regulating the 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. WTO defines e-commerce more precisely as: "the production, distribution, marketing, sale, or delivery of goods and services by electronic means."

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. In 2001, the volume of B2B transactions in the US totalled US$995 billion, which represents 93.3% 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 relate to e-commerce.

WTO AND E-COMMERCE

The key policy player in modern global trade, the World Trade Organisation (WTO), regulates many relevant e-commerce issues, including tele-

communication liberalisation, intellectual property rights, and some aspects of ICT developments. The WTO addresses e-commerce directly through the following 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.

Although e-commerce has been on the WTO diplomatic backburner, various initiatives have arisen and a number of key issues have been identified. Two 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 TRIPs 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 telecommunications 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 covered 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 ebXML by the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFAT). In fact, ebXML could soon become the main standard for the exchange of electronic trade documents, replacing thee current one – Electronic Data Interchange (EDI).

The OECD's activities touch on various aspects related to e-commerce, including customer protection and digital signatures. The OECD emphasises the promotion of and research regarding e-commerce through its recommendations and guidelines. Other international organisations, such as the United Nations Conference on Trade and Development (UNCTAD) and the UN ICT Task Force also conduct various e-commerce capacity-building and research activities.

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 latest and most prominent initiative is APEC's Paperless Trading Individual Action Plan, aiming to create complete 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 information about payment cards, misleading advertising, and the delivery of defective products. A new idiosyncrasy of e-commerce is the internationalisation of consumer protection, which is not an important issue in regular commerce. In the past, consumers rarely needed international protection. 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 being exposed 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 a few 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. For example, 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.

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

The Internet Governance dilemma of whether cyber-issues should be treated differently from real ones has been clearly mirrored in the question of taxation. 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. 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. Many states in the US have argued along the same lines, requesting the taxation of Internet transactions.

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 fact that the EU has more e-commerce consumers than sellers.

CUSTOMS

Customs are directly affected by e-commerce. The transaction of digital goods over international borders cannot be controlled in the same way as the transaction of material goods. It is difficult, if not impossible, to identify Internet packages containing products on which customs duties should be paid. This opens up many issues related to the applicability of the existing concept of customs controls as well as the introduction of some new procedures.

At the policy level, the main initiative is the WTO's Moratorium on imposing customs duties on e-commerce transmissions (1998). The last explicit extension of the moratorium was carried out in Doha in 2001. Due to the failure of the Cancun WTO Negotiations (2003), this issue was not officially discussed. It left broad room for different interpretations about whether a global customs moratorium was still in force or not. Practically speaking, it does not make a big difference, since it is almost impossible to impose customs on goods and services delivered via the Internet due to the technical difficulties in inspecting goods and services.

E-PAYMENTS: E-BANKING AND E-MONEY

Electronic payment can be defined as the conclusion of financial transactions within an online environment through the use of various online payment instruments. The existence of an electronic payment system is a pre-condition for the successful development of e-commerce. The field of electronic payments requires a distinction between e-banking and e-money.

E-banking involves the use of a PC and 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 essen-

tially the same. E-banking provides advantages to customers and reduces the costs of transactions. In terms of governance, it does not pose any specific problems beyond those already covered, such as 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 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.
- Its transactions involve a complex system, including the issuer of the e-money value, the network operators, and the clearer of e-money transactions.

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

The first is an evolutionary development that 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 that would move e-money out of the control of central banks. Already, the Bank for International Settlement (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. As one prominent banker said: "the successors to Bill Gates would have put the successors to Alan Greenspan out of business." Such a development would have considerable implication for the future of the state and international relations or, as the same speaker noted, "Societies have managed without central banks in the past. They may well do so in the future." Other possibilities for the use of e-money remain speculative.

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 banks will be seriously challenged by more cost-effective e-banking.

2. 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 almost impossible to conduct without credit cards. This is a significant obstacle for those 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.

3. 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.

   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.

4. 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 an additional amount for accessing articles or other services on the Internet. A micro-payment scheme based on e-money may provide the necessary solution. W3C, the main Internet standardisation body, is involved in creating standards for micro-payment systems.

5. Due to the nature of the Internet, it is likely that e-money will become global--providing reason to *address this issue at the international level.* One potential player in the field of e-banking is the Ba-

sel Committee E-Banking Group. This group has already started addressing authorisation, prudential standards, transparency, privacy, money laundering, and cross-border supervision, key issues for the introduction of e-money.

6. Various forms of electronic payments have been developed, primarily within the advanced economies. Electronic payments require a stable, secure, and functional legal ambience. However, *most developing countries still have cash-based economies.* If the use of cards is allowed at all, it is predicated on the use of signatures. This huge discrepancy also affects the development of e-commerce and increases the digital divide between the rich North and the poor South. Unlike measures such as the purchase of equipment, the introduction of electronic payments requires many gradually introduced institutional and technical arrangements. One element essential to both e-commerce and e-payments and which cannot be acquired quickly is consumer trust.

7. The latest request from the New York State Attorney General to Paypal and Citibank not to execute payments to Internet casinos *directly links electronic payment and law enforcement.* What the law-enforcement authorities could not achieve through legal mechanisms, they could through the control of electronic payments.

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 on the distribution of power and development has given rise to many questions:

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

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

Almost every Internet Governance issue has a developmental aspect. The following issues are relevant to development:

- the existence of a telecommunications infrastructure, 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 a recent article in *The Economist* ("Falling through the Net?", 21 September 2000). 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, 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."

Is the Digital Divide Increasing?

ICT 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 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 ac-

cess 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 telecommunications access to all citizens has been the basis of US telecommunications 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 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. Various forms of 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 UNDP or the World Bank, as well as regional development initiatives and banks. With increased liberalisation of the telecommunications market, a tendency for developing telecommunications 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.

The importance of the financial aspect was clearly recognised during the Geneva phase of WSIS. One idea proposed at WSIS was the establishment of an UN-administered Digital Solidarity Fund to help technologically disadvantaged countries build telecommunication infrastructures. The fund would rely on voluntary contributions. One proposal suggest-

ed a donation system, such as $1 per purchase of a personal computer, software package, or piece of network equipment. However, the proposal to establish a Digital Solidarity Fund did not garner broad support. The developed countries favour direct investment instead of the establishment of a centralised development fund. In order to explore the possibilities for more flexible and appropriate financing schemes, it was agreed to establish the Working Group on Financing ICT4D which will report to the WSIS 2005 in Tunisia.

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 the 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 the 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 the brain drain, is the increase in the outsourcing of ICT tasks to developing countries. The most successful examples have been the development of India's software industry centres, such as Bangalore.

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.

UNESCO's initiatives are particularly relevant to the social aspect of the digital divide. UNESCO adopted a convention on the protection of cultural diversity and instigated a few projects aimed at promoting linguistic and cultural diversity on the Internet.

TELECOMMUNICATIONS POLICY AND REGULATION

Telecommunications 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 a telecommunications 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 telecommunications 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.

SECTION 6

The Socio-Cultural Basket

THE SOCIO-CULTURAL BASKET

Networks connecting computers existed long before the Internet. What makes the Internet different is its facilitation of various forms of human communication and creativity. The major breakthroughs are linked to the ways in which the Internet was used for new modes of communication (e-mail, Web, multimedia). In this context, some authors argue that the Internet is more a social than a technological phenomenon. It supplements traditional communication as well as provides new forms of communication of its own (e.g. cyber-communities). Such occurrences have led to the development of a socio-cultural aspect to the Internet. The socio-cultural basket includes some of the most controversial issues in the whole field of Internet Governance, such as content policy and multilingualism. These issues, in particular, reflect today's most prevalent national, religious, and cultural differences.

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), to name a few.

Discussion about content usually focusses on three groups of content. The *first group* consists of content where a global consensus for its control is in place. Included here are child pornography and various issues, such as justification of genocide and incitement or organisation of terrorist acts, prohibited by international law (*ius cogens*). While a consensus about the need to remove this content from the Net has been established, different interpretations remain. For example, what exactly constitutes terrorism-support acts?

The *second group* consists of content that might be sensitive for particular countries, regions, or ethnic groups due to their particular religious and cultural values. Globalised and more intensive communication chal-

lenges local cultural and religious values. Most Internet court cases are related to this group of content. In the Yahoo! Case, a French court requested Yahoo.com (USA) to prohibit French citizens from accessing parts of a website selling Nazi materials and memorabilia. Germany has very developed jurisprudence, with many court cases against owners of websites hosting Nazi materials. Most content control in Middle Eastern and Asian countries is officially justified as the protection of specific cultural values. This usually includes blocking access to pornographic and gambling websites.

The third group consists of politically and ideologically sensitive content. In essence, this involves Internet censorship. Transparency International has reported a number of such practices in China, Burma, and Saudi Arabia.

HOW IS CONTENT POLICY CONDUCTED?

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

Public (Governmental) Filtering of Content

The common element for governmental filtering is an "Internet Index" of websites blocked for access by citizens. If a website is in the "Internet Index," access will not be granted. Technically speaking, the filtering typically utilises router-based IP blocking, proxy servers, and DNS redirection. Filtering of content is carried out in many countries. In addition to countries usually associated with such practices (China, Saudi Arabia, and Singapore) other countries increasingly practice it. For example, Australia has a filtering system for specific national pages. The state of North-Rhine-Westphalia requested ISPs to filter access to mainly, but not solely, neo-Nazi sites.

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 suggested the implementation of *rating and filtering systems* controlled by end users. Technically speaking, filtering mechanisms are built into the Internet browsers. The accessibility of particular content is indicated via a label that corresponds to a par-

ticular website. The use of this type of filtering was especially favoured as a system for accessing only "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 geographical/national origin of users. The Yahoo! Case was important in this respect since the group of experts involved, including Vint Cerf, indicated that in 90% of cases Yahoo! would be able to determine whether sections of one of its websites hosting Nazi memorabilia were being accessed from France. This technological assessment helped the court to come to a final decision. Geo-location software companies claim that they can identify the home country without mistake and the city in about 85% of the cases, especially if it is a large city. Geo-location software can help various Internet content providers filter access according to nationality and avoid court cases in foreign courts.

Content Control through Search Engines

There is significant difference between availability and accessibility of materials on the Internet. The fact that a particular webpage or content is available on the Internet does not mean that it will be accessed by many users. For example, if a particular website cannot be found on Google its relevance is seriously diminished. The bridge between the end user and web-content is usually a search engine. It has been widely reported that one of the first examples of content control through search engines was carried out by the Chinese authorities towards the Google search engine. If users entered prohibited words into Google Search, they would lose their IP connectivity for a few minutes. The Chinese information department stated: "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."

In order to adjust to local laws, Google decided to restrict some materials on its national websites. For example, on German and French versions of Google, it is not possible to search for and find websites with Nazi materials. This indicates a certain level of self-censorship on the part of Google in order to avoid possible court cases.

Need for an Appropriate Legal Framework

The legal vacuum in the field of content policy, which characterised early Internet use, provided governments with high levels of discretion in content control. Since content policy is a sensitive issue for every society, there is a need to adopt legal instruments. 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 are linked to European countries with strong legislation in the field of hate speech, including anti-racism and anti-Semitism. European regional institutions have been trying to impose those rules on cyberspace. The key legal instrument addressing the issue of content is the Council of Europe Additional Protocol on the Cybercrime Convention. The protocol specifies various types of hate speech that should be prohibited on the Internet, including racist and xenophobic materials, justification of genocide, and crimes against humanity.

The Organisation of Security and Co-operation in Europe (OSCE) is particularly active in this field. In June 2003, the OSCE Meeting on Freedom of Media and the Internet adopted the Amsterdam Recommendations on Freedom of the Media and the Internet. The recommendations promote freedom of expression and attempt to reduce censorship on the Internet. In June 2004, the OSCE organised the Conference on the Relationship between Racist, Xenophobic, and Anti-Semitic Propaganda on the Internet and Hate Crimes (Paris, 16-17 June 2004). The focus of this event was on the potential misuses of the Internet and freedom of expression. These OSCE events provided a wide range of academic and policy views addressing these two aspects of content control.

The EU has carried out several initiatives in the context of 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 safer use of the Internet.

THE ISSUES

Content Control vs. Freedom of Expression

When it comes to content control, the other side of the coin is very often restriction of freedom of expression. This is especially important in the US, where the First Amendment guarantees broad freedom of expression, even the right to publish Nazi and similar materials. Achieving a proper balance between content control and freedom of expression is a considerable challenge. Most of the recent Internet Governance debate, including court cases and Congress legislation, has been related to finding this balance.

The US Congress has inclined towards stricter content control, while the Supreme Court seeks to protect the First Amendment of the US Constitution (the Freedom of Expression). The most notable example was the US Congress's Communications Decency Act (1996), which was declared unconstitutional by the Supreme Court with the judgement that it breached the First Amendment.

Freedom of expression largely shapes the US position in the international debate on Internet Governance. For example, while the US has signed on to 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. It is the line beyond which the US will not step in international negotiations.

"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 share and

spread of 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 rules themselves.

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. Just as easily, however, technically speaking, any control mechanism 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. 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 should be controlled and how. Some groups of individual users, such as parents, are keen to introduce a more efficient content policy to protect children. Various rating initiatives are aimed at helping parents to filter child-friendly content. Content control is also performed by private companies and universities to restrict access to some materials. In some cases, content is controlled through software packages; for example, the Scientology movement has distributed a software package, Scienositter, to members, limiting access to websites critical of Scientology.

One innovative initiative is the Internet Watch Foundation in the UK, which aims at combating child abuse on the Internet. The foundation is a multistakeholder initiative established by the government, Internet service providers, and user representatives.

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. During the first WSIS phase, many civil society groups proposed the introduction of the right to communicate that goes beyond existing Internet-related rights.

Existing human rights that have not been covered in other parts of this booklet are briefly surveyed here.

The Freedom of Expression and Right to Seek, Receive, and Impart Information

This is one of the fundamental human rights, usually appearing in the focus of discussions on content control and censorship. In the UN Human Rights Declaration, the freedom of expression 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 discussion and implementation of Article 19 must be put in the context of establishing a proper balance between two needs. This ambiguous regime opens many possibilities for different interpretations of norms and ultimately different implementations.

Right to Privacy

The right to privacy is discussed in the Legal Basket (p. 69).

Intellectual Property Rights

Intellectual property rights entitle anyone to enjoy the protection of the moral and material interests resulting from scientific, literary, or artistic production. This right is counter-balanced by the right of everyone to participate freely in cultural life and to share scientific advances. Establishing a balance between those two claims is one of the main challenges for Internet Governance.

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. The 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. 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 Unicode. The Unicode Consortium is a non-profit institution that develops standards to facilitate the use of character sets for different languages. Recently, ICANN and IETF took an important step in promoting international 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 organisations such as UNESCO. UNESCO has instigated many initiatives focussing 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.

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

One of the key features of the Internet is that through worldwide interaction of users new knowledge and information is produced. Considerable knowledge has been generated through exchanges on mailing lists, discussion groups, and blogs. In many cases, no international legal mechanisms protect such knowledge. Left in the legal vacuum, it is made available for commodification and commercialisation by individuals. This common pool of knowledge, an important basis of creativity, is at risk of being depleted. The more the Internet is commercialised, the less spontaneous exchanges may become. This could lead towards reduced creative interaction. The concept of global public goods could provide solutions that would also protect common Internet knowledge for future generations.

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

Protecting the Internet as a Global Public Good

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. At the global level, the United Nations Development Programme (UNDP) has introduced the concept of global public goods. In international law, a potential solution is the concept of *res communis omnim* (space as a common heritage for humankind to be regulated and garnered by all nations).

It will be important to consider which of these concepts might be applied to the Internet and with what consequences. Many agree that the model for the future development of the Internet will depend on the establishment of a proper balance between private and public interests.

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.

E-learning has also brought more intensive cross-border education, with students participating in online courses delivered from other countries. This has introduced an international governance dimension to the educational sector.

Traditionally, education has been governed by national institutions. The accreditation of educational institutions, the recognition of qualifica-

tions, 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.

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 US/UK educational sector to gain global market coverage in education, and has received considerable opposition from many countries.

The main argument against such a standpoint is that universities provide public goods and that they play an important social and cultural function in every country, beyond the simple transference of knowledge and information. According to this view, the free global market in education might endanger universities in small and developing countries and lead to educational dominance by educational institutions from the US and UK, considerably reducing cultural diversity and depriving many societies of the university role as catalyst for the development of national culture. Another criticism of free trade in education is its potential incompatibility with the implementation of the right to education.

The forthcoming debate, likely to develop within the context of WTO and other international organisations, will focus on the dilemma of education as a commodity or a public good. If education is considered a commodity, 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. The outcome of this debate will have a considerable impact on the development of online learning.

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.

Discussions about transnational learning in general and online learning in particular have begun at the international level. One of the first comprehensive attempts to provide quality assurance in transnational educational programmes is that of UNESCO and the Council of Europe in their "Code of Good Practice in the Provision of Transnational Education."

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.

A general tendency towards student mobility in higher education makes possible study at a number of universities. The EU, in particular, has made advances in this field, through various initiatives such as Socrates. Student mobility requires the transfer of credits between universities in different countries. The necessary regulatory frameworks have started to be developed at regional levels. The EU has started to develop a regulatory framework with the European Credit Transfer System (ECTS). The Asia-Pacific region is following the European lead by introducing its own regional model for the exchange of students and a related credit system (UCTS).

The Standardisation of Online Learning

The early phase of online learning development was characterised by rapid development and high diversity of materials, in the sense of platforms, content, and didactics. However, there is a need to develop com-

mon standards in order to facilitate the easier exchange of online courses and introduce a certain standard of quality.

The first standard, AICC (Aviation Industry CBT Committee), was developed by the aviation industry association with the primary objective of providing interoperability in online learning packages. The next major development was the introduction of IMS (Instructional Management System), which introduced a number of standards for online learning, including meta-data specifications that could be shared by online learning courses (a description of the content, course title, authors, cost, learning taxonomy, etc.). IMS is based on eXtended Markup Language (XML). In addition, the Learning Technology Standards Committee (LTSC) of the Institute of Electrical and Electronic Engineers (IEEE) has carried out some standardisation.

The US Department of Defence (DoD) initiated the latest development in 1997. Faced with the limitations of all existing standards, the DoD established the Advanced Distributed Learning (ADL) initiative, resulting in a new standard named Shareable Content Object Reference Model (SCORM). SCORM is the most elaborate and most widely adopted standard for online courses. One of the reasons for SCORM's success is that it has become the required standard for courses delivered to the DoD (a market of US$700 million per year) and other US government departments. SCORM is also gaining wider international visibility and usage.

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

SECTION 7

Annex

ANNEX I

"THE BLIND MEN AND THE ELEPHANT"

<table>
<tr><td colspan="2">It was six men of Indostan
To learning much inclined,
Who went to see the Elephant
(Though all of them were blind),
That each by observation
Might satisfy his mind.</td></tr>
<tr><td>The First approached the Elephant,
And happening to fall
Against his broad and sturdy side,
At once began to bawl:
"God bless me! but the Elephant
Is very like a wall!"</td><td>The Fourth reached out an eager hand,
And felt about the knee.
"What most this wondrous beast is like
Is mighty plain," quoth he;
"'Tis clear enough the Elephant
Is very like a tree!"</td></tr>
<tr><td>The Second, feeling of the tusk,
Cried, "Ho! what have we here
So very round and smooth and sharp?
To me 'tis mighty clear
This wonder of an Elephant
Is very like a spear!"</td><td>The Fifth, who chanced to touch the ear,
Said: "E'en the blindest man
Can tell what this resembles most;
Deny the fact who can
This marvel of an Elephant
Is very like a fan!"</td></tr>
<tr><td>The Third approached the animal,
And happening to take
The squirming trunk within his hands,
Thus boldly up and spake:
"I see," quoth he, "the Elephant
Is very like a snake!"</td><td>The Sixth no sooner had begun
About the beast to grope,
Than, seizing on the swinging tail
That fell within his scope,
"I see," quoth he, "the Elephant
Is very like a rope!"</td></tr>
<tr><td colspan="2">And so these men of Indostan
Disputed loud and long,
Each in his own opinion
Exceeding stiff and strong,
Though each was partly in the right,
And all were in the wrong!

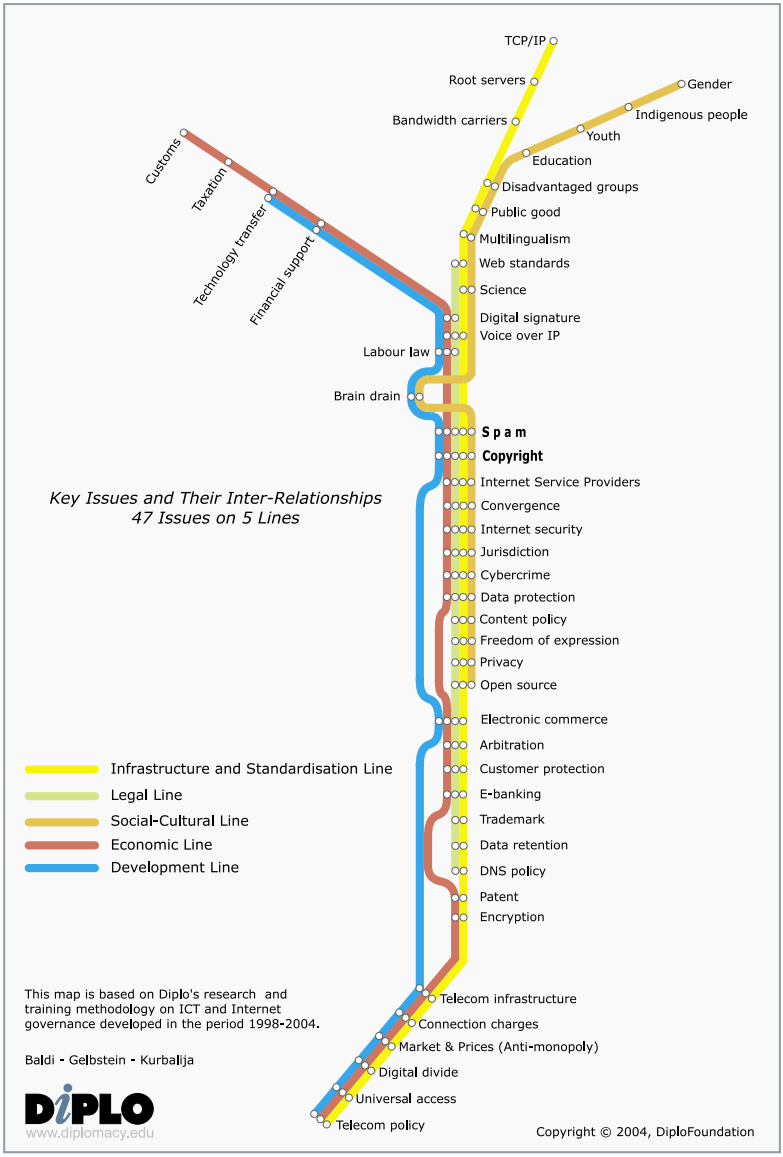
Moral: So oft in theologic wars,
The disputants, I ween,
Rail on in utter ignorance
Of what each other mean,
And prate about an Elephant
Not one of them has seen!</td></tr>
<tr><td colspan="2">US poet John Godfrey Saxe (1816-1887)</td></tr>
</table>

ANNEX II – THE EVOLUTION OF INTERNET GOVERNANCE

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				
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 Rot 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 FUNTIONING 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	
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 remain very strong. Thus the interests of both private business and the "guardians" communities were properly protected. It was not the case with 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			

ANNEX III – A MAP FOR A JOURNEY THROUGH INTERNET GOVERNANCE



ANNEX IV – 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 our 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 AUTHORS

Ed Gelbstein

Eduardo Gelbstein is a Senior Special Fellow of the United Nations Institute for Training and Research (UNITAR) and a contributor to the United Nations Information and Telecommunications (ICT) Task Force and to the preparatory work for the World Summit on the Information Society. He is the former Director of the United Nations International Computing Centre.

In addition to his collaboration with the United Nations, he is a conference speaker and university lecturer reflecting his 40 years experience in the management of information technologies.

He has worked in Argentina, the Netherlands, the UK, Australia and after joining the United Nations in 1993, in Geneva (Switzerland) and New York (USA). He graduated as an electronics engineer from the University of Buenos Aires, Argentina in 1963 and holds a Master's degree from the Netherlands and a PhD from the UK.

gelbstein@diplomacy.edu

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. Since the late 1980s he has been involved in research on ICT and law. In 1992 he was in charge of establishing the first Unit for IT and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of successful work in the field of training, research and publishing, in 2003 the Unit evolved into DiploFoundation.

Jovan Kurbalija directs online learning courses on ICT and diplomacy and lectures in academic and training institutions in Switzerland, the United States, Austria, the United Kingdom, the Netherlands, and Malta.

The main areas of his research are: diplomacy and development of the international regime on the Internet, the use of hypertext in diplomacy, online negotiations, and diplomatic law.

jovank@diplomacy.edu