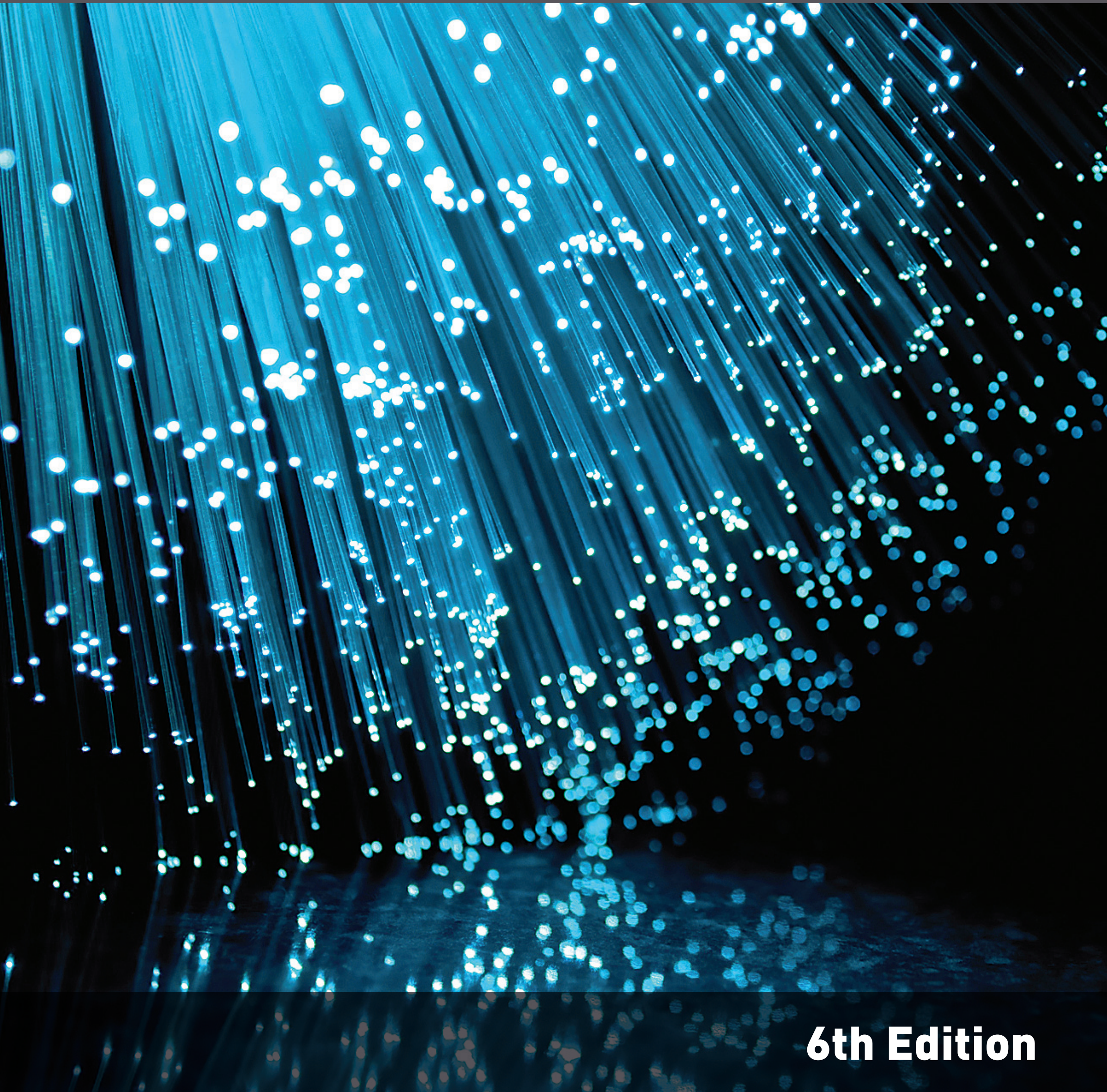
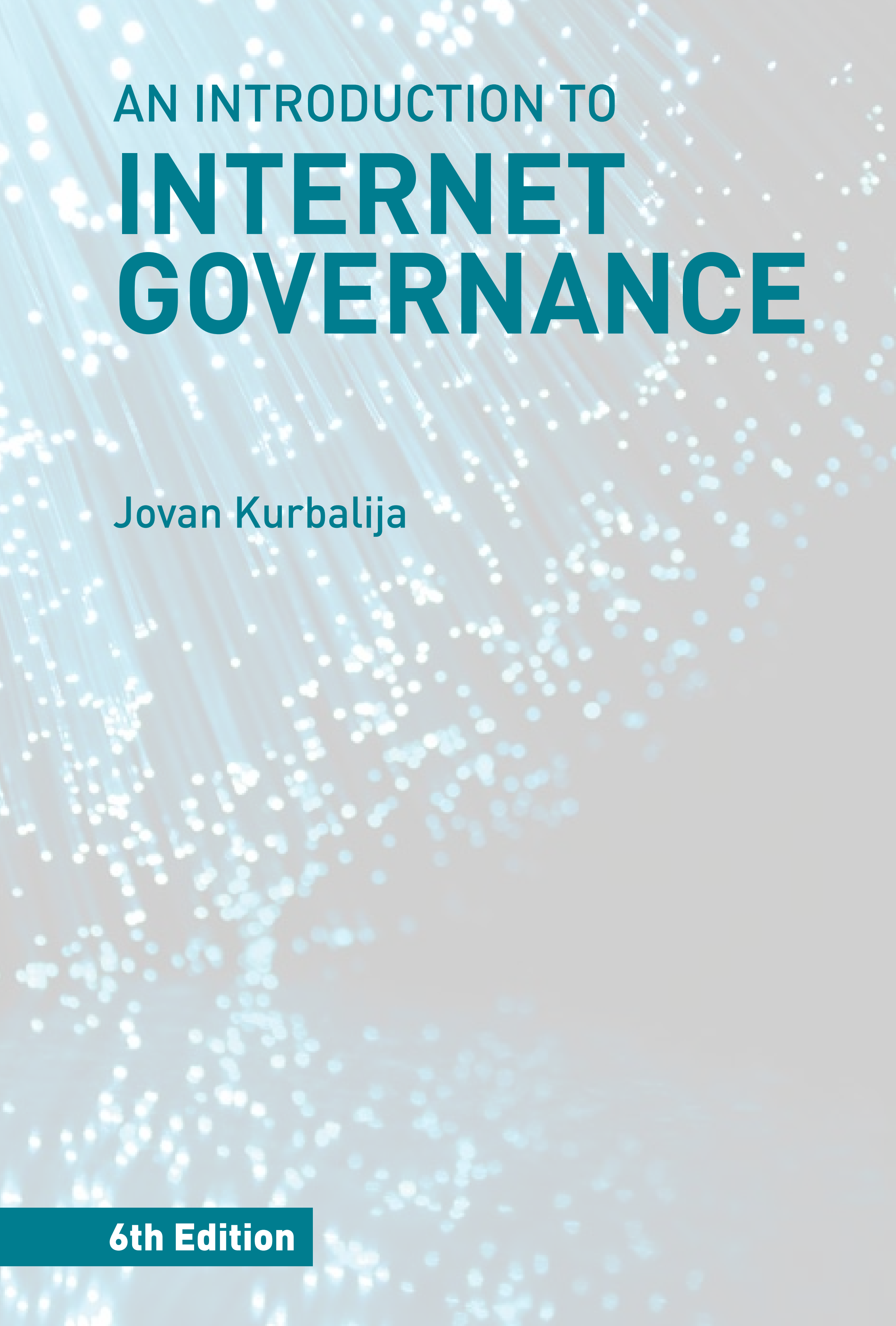
AN INTRODUCTION TO INTERNET GOVERNANCE

Jovan Kurbalija



6th Edition

The history of this book is long, in Internet time. The original text and the overall approach, including the five-basket methodology, were developed in 1997 for a training course on information and communications technology (ICT) policy for government officials from Commonwealth countries. In 2004, Diplo published a print version of its Internet governance materials, in a booklet entitled *Internet Governance – Issues, Actors and Divides*. This booklet formed part of the Information Society Library, a Diplo initiative driven by Stefano Baldi, Eduardo Gelbstein, and Jovan Kurbalija. Special thanks are due to Eduardo Gelbstein, who made substantive contributions to the sections dealing with cybersecurity, spam, and privacy, and to Vladimir Radunovic, Ginger Paque, and Stephanie Borg-Psaila who updated the course materials. Comments and suggestions from other colleagues are acknowledged in the text. Stefano Baldi, Eduardo Gelbstein, and Vladimir Radunovic all contributed significantly to developing the concepts behind the illustrations in the book. In 2008, a special, revised version of the book, entitled simply *An Introduction to Internet Governance*, was published in cooperation with NIXI India on the occasion of the Internet Governance Forum (IGF) 2008 held in Hyderabad, India. In 2009, a revised third edition was published in the cooperation with the Ministry of Communication and Information Technology of Egypt Internet Governance. The fourth edition (2010) was produced in partnership with the Secretariat of the Africa-Caribbean-Pacific Group of Countries and the European Union. The fifth edition (2012) was published in cooperation with the Azerbaijan Diplomatic Academy (ADA).



AN INTRODUCTION TO INTERNET GOVERNANCE

Jovan Kurbalija

6th Edition

Published by DiploFoundation (2014)

Malta: Anutruf, Ground Floor,
Hriereb Street,
Msida, MSD 1675, Malta

Switzerland: DiploFoundation
7bis, Avenue de la Paix
CH-1211 Geneva, Switzerland

E-mail: diplo@diplomacy.edu

Website: http://www.diplomacy.edu

Cover: the Argument by Design – www.tabd.co.uk

Editing: Mary Murphy

Illustrations: Zoran Marcetic – Marča & Vladimir Veljašević

Layout & Prepress: the Argument by Design

Printing: Aleksandar Nedeljkov

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

ISBN: 978-99932-53-28-0

DiPLO
www.diplomacy.edu

Contents

Section 5: The development basket . . . 141

Section 6: The sociocultural basket . . . 155

Section 7: Internet governance actors . . . 177

Section 8: Annex . . . 197

Foreword

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

Today, just ten years later, the same people who asked me to install their printers are coming back to me with questions about how to keep ownership of their data on Facebook or how to ensure their children can navigate the Internet safely. Increasingly, they are concerned about a possible cyberwar and the online risks for water supply, power plants, and other critical infrastructure in their cities and countries. How far we all have come!

Internet governance is moving increasingly into the public eye. The more modern society depends on the Internet, the more relevant Internet governance will be. Far from being the remit of some select few, Internet governance concerns all of us to a lesser or greater extent, whether we are one of the 2.9 billion using the Internet or a non-user who depends on the facilities it services.

Internet governance is obviously more relevant for those who are deeply integrated in the e-world, whether through e-business or networking on Facebook. Yet it has a broad reach. Government officials, military personnel, lawyers, diplomats, and others who are involved in either providing public goods or preserving public stability are also concerned. Internet governance, and in particular the protection of privacy and other human rights, is a focal point for civil society activists and non-governmental organisations. For academia and innovators worldwide, Internet governance must ensure that the Internet remains open for development and innovation. Creative inventors of tomorrow's Google, Skype, Facebook, and Twitter are out there, somewhere, browsing the Net. Their creativity and innovativeness should not be stifled; rather they should be encouraged to develop new, more creative ways to use the Internet.

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

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

Jovan Kurbalija
Director of DiploFoundation
Head of the Geneva Internet Platform
September 2014

Chapitre 1

Introduction

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

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

Introduction

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

What does Internet governance mean?

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

> *Internet governance is the development and application by Governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.*[2]

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

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

Back in 2003, *The Economist* magazine started writing Internet with a lowercase 'i'. This change in editorial policy was inspired by the fact that the Internet had become an everyday item, no longer unique and special enough to warrant an initial capital. The word 'Internet' followed the linguistic destiny of (t)elegraph, (t)elephone, (r)adio, and (t)elevison, and other such inventions.

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

Internet

The term 'Internet' does not cover all of the existing aspects of global digital developments. Two other terms – information society and information and communication technology (ICT) – are usually put forward as more comprehensive. They include areas that are outside the Internet domain, such as mobile telephony. The argument for the use of the term 'Internet', however, is enhanced by the rapid transition of global communication towards the use of Internet protocol (IP) as the main communications technical standard. The already ubiquitous Internet continues to expand at a rapid rate, not only in terms of the number of users but also in terms of the services that it offers, notably voice-over Internet protocol (VoIP), which may displace conventional telephony.

Governance

In the Internet governance debate, especially in the early phase of WSIS 2003, controversy arose over the term 'governance' and its various interpretations. According to one interpretation, governance is synonymous with government. Many national delegations had this initial understanding, leading to the interpretation that Internet governance should be the business of governments and consequently addressed at intergovernmental level with the limited participation of other, mainly non-state actors.[4] This interpretation clashed with a broader meaning of the term 'governance', which includes the governance of affairs of any institution, including non-governmental ones.

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

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

The evolution of Internet governance

Early Internet governance (1970s–1994)

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

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

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

The DNS war (1994–1998)

This decentralised approach to Internet governance soon began to change as governments and the business sector realised the importance of the global network. In 1994, the US National Science Foundation, which managed the key infrastructure of the Internet, decided to subcontract the management of the domain name system (DNS) to a private US company called Network Solutions Inc. (NSI). This was not well received by the Internet community and led to the so-called DNS war.

This war brought new players into the picture: international organisations and nation states. It ended in 1998 with the establishment of a new organisation, the Internet Corporation for Assigned Names and Numbers (ICANN), which has become the focus of most Internet governance debates today.

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

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

After prolonged negotiations and last-minute arrangements, the first WSIS summit in Geneva (December 2003) agreed to establish the Working Group on Internet Governance (WGIG). WGIG prepared a report which was used as the basis for negotiations at the second WSIS summit held in Tunis (November 2005). The WSIS Tunis Agenda for the Information Society elaborated on the question of Internet governance, including adopting a definition, listing Internet governance issues, and establishing the Internet Governance Forum (IGF), a multistakeholder body convoked by the UN Secretary General.

Developments in 2006

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

The second event of 2006 was the Internet Governance Forum (IGF) in Athens. It was the first such forum and, in many respects, it was an experiment in multilateral diplomacy.

The IGF was truly a multistakeholder event with participation of states, business, and civil society. It also had an interesting organisational structure for its main events and workshops. Journalists moderated the discussions and the IGF therefore differed from the usual UN-style meeting format. However, some critics claimed that the IGF was only a 'talk show' without any tangible results in the form of a final document or plan of action.

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

Developments in 2007

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

Developments in 2008

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

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

See **Section 2** for further discussion on network neutrality

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

Developments in 2009

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

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

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

Developments in 2010

The main development in 2010 was the impact of fast-growing social media on the Internet governance debate, including the protection of privacy of users of social media platforms such as Facebook. In 2010, the main development in Internet geo-politics was US Secretary of State Hillary Clinton's speech on freedom of expression on the Internet, in particular in relation to China.[9] Google and Chinese authorities conflicted over the restricted access to Google-search in China. The conflict led to the closing of Google's search operations in China.

There were two important developments in the ICANN world. First was the introduction of non-ASCII domain names for Arabic and Chinese. By solving the problem of domain names in other languages, ICANN reduced the risk of the disintegration of the Internet DNS. Second was ICANN's approval of the .xxx domain (adult materials). With this decision ICANN formally crossed the Rubicon by officially adopting a decision of high relevance for public policy on the Internet. Previously, ICANN had tried to stay, at least formally, within the realm of making only technical decisions.

The IGF review process started in 2010 with the UN Commission on Science and Development adopting the resolution on the continuation of the Forum, which suggested continuation for the next five years, with only minor changes in its organisation and structure. In July 2010, the UN Economic and Social Council (ECOSOC) endorsed this resolution. The UN General Assembly decided in the autumn of 2010 to continue the IGF for the next five years (2011–2015).

Developments in 2011

In 2011, the main general development was the rise of Internet governance higher on the global politics agenda. The relevance of Internet governance moved closer to other diplomatic issues such as climate change, migration, and food security. Another consequence of the growing political relevance of the Internet is the gradual shift of national coverage of Internet governance issues from technology (IT, telecoms) to political ministries (diplomacy, prime ministerial cabinets). In addition, the main global media (e.g. *The Economist, IHT,* Al Jazeera, the BBC) were now following Internet governance developments more closely than ever before.

Internet governance was affected by the Arab Spring. Although there are very different views on the impact of the Internet on the Arab Spring phenomenon (ranging from minimal to key), one outcome is certain: social media is now perceived as a decisive tool in modern political life. In various ways, the

Internet – and its governance – popped up on political radars worldwide this year.

On 27 January, Egyptian authorities cut access to the Internet in a vain hope to stop political protests. This was the first example of a complete countrywide Internet blackout ordered by the government. Previously, even in the case of military conflicts (former Yugoslavia, Iraq), Internet communication had never been completely severed.

Hillary Clinton's initiative on freedom of expression on the Internet, initiated by her speech in February 2010, was accelerated in 2011. There were two major conferences on this subject: the Vienna Conference on Human Rights and the Internet, and The Hague Conference on Internet and Freedom.

In 2011, ICANN continued its soul searching with the following main developments:

- Implementation of management reform.
- Final policy preparations for the introduction of new generic top-level domains (gTLDs).
- The resignation of its CEO and the search for a replacement.

2011 was also marked by the avalanche of Internet governance principles which were proposed by the Organisation for Economic Co-operation and Development (OECD), the Council of Europe, the EU, Brazil, and other players. The numerous convergences of these principles could be the starting position of a future preamble of a global Internet declaration or similar document that could serve as the framework for Internet governance development.

Developments in 2012

Two major events marked the 2012 agenda with important consequences for the years to come: the ICANN leadership change and the revision of the ITU's International Telecommunication Regulations (ITRs).

ICANN went through significant developments in 2012 with the introduction of new generic Top Level Domains (gTLDs). Despite some problems with the registration process (software glitches, controversies over the policy process), over 1900 applications for new gTLDs were received and evaluated. Moreover, the new CEO, Fadi Chehadé brought a fresh approach to the steering of the ICANN multistakeholder policy processes. In his speech to civil society at ICANN 45, he outlined some promising improvements, including development of responsible multistakeholderism, frank recognition of problems, active listening, empathetic guidance, search for compromise, etc.

The World Conference on International Telecommunications (WCIT) converged in Dubai in December 2012 to amend the ITRs for the first time since 1988; it stirred debate on the impact of a new regulation on the future of Internet. At the end of an exhausting two-week conference, the negotiations ended in a stalemate: the participants failed to reach a consensus on the amended text, leaving the debate open for upcoming meetings. The main contentious point was a non-binding resolution on fostering the role of the ITU in Internet governance, which polarised participating states into two blocks: western countries favoured the current multistakeholder model while supporters of the resolution, including states like China, Russia, and Arab countries, leaned towards an intergovernmental model.

Other notable developments registered in the intellectual property rights area, where Internet users mobilisation and protests managed to block national (Stop Online Piracy Act (SOPA) in the USA) and international (Anti-Counterfeiting Trade Agreement (ACTA)) regulations that would have affected users' legitimate rights through their implementation

Developments in 2013

The main development in global digital politics was the Snowden revelations on the various surveillance programmes run by the US National Security Agency (NSA) and other agencies. The Snowden revelations made the global public interested in how the Internet is governed. The main focus was on the question of data protection and rights of privacy.

The question of protection of privacy was addressed by many leaders during the UN General Assembly. The UNGA resolution initiated a new policy process on online privacy. The issue will be further discussed in 2014 at the UN Human Rights Council.

In October 2013, Brazilian president Dilma Rousseff and ICANN's president Fadi Chehadi initiated the NETmundial process. Internet governance came into focus at numerous academic conferences and research activities of think-tanks worldwide.

Prefixes: e- / virtual / cyber / digital

The prefixes e- / virtual / cyber / digital / net are used to describe various ICT/Internet developments. They are used interchangeably. Each prefix describes the Internet phenomenon.

Yet, we tend to use e- for commerce, cyber for crime and security, digital for development divides, and virtual for currencies, such as Bitcoin. Usage patterns have started to emerge. While in our everyday language, the choice of prefixes e- / virtual / cyber / digital / net is casual, in Internet politics the use of prefixes has started to attract more meaning and relevance.

Let's have a quick look at the etymology of these terms and the way they are used in Internet politics.

The etymology of 'cyber' goes back to the Ancient Greek meaning of 'governing'. Cyber came to our time via Norbert Weiner's book *Cybernetics*, dealing with information-driven governance. In 1984, William Gibson coined the word cyberspace in the science-fiction novel *Neuromancer*. The growth in the use of the prefix 'cyber' followed the growth of the Internet. In the late 1990s almost anything related to the Internet was 'cyber': cybercommunity, cyberlaw, cybersex, cybercrime, cyberculture, cyber... If you named anything on the Internet and you had 'cyber'. In the early 2000s, cyber gradually disappeared from wider use, only remaining alive in security terminology.

Cyber was used to name the 2001 Council of Europe Cybercrime Convention. It is still the only international treaty in the field of Internet security. Today there is the USA's Cyberspace Strategy, the ITU's Global Cybersecurity Agenda; NATO's Cyber defense policy, Estonia's Cyber Defence Center of Excellence ...).

Cyberpunk author and *Wired* columnist Bruce Sterling had this to say:

> I think I know why the military calls it 'cyber' — it's because the metaphor of defending a 'battlespace' made of 'cyberspace' makes it easier for certain contractors to get Pentagon grants. If you call 'cyberspace' by the alternate paradigm of 'networks, wires, tubes and cables' then the NSA has already owned that for fifty years and the armed services can't get a word in.[10]

'E' is the abbreviation for 'electronic'. It got its first and most important use through e-commerce, as a description of the early commercialisation of the Internet. In the EU's Lisbon Agenda (2000), e- was the most frequently used prefix. E- was also the main prefix in the WSIS declarations (Geneva 2003; Tunis 2005). The WSIS follow-up implementation is centred on action lines including e-government,e-business, e-learning, e-health, e-employment, e-agriculture, and e-science. Nonetheless, e- is not as present as it used to be. Even the EU has abandoned e- recently, trying, most likely, to distance itself from the failure of the its Lisbon Agenda.

Continued over →

Prefixes: e- / virtual / cyber / digital ... continued

Today, the EU has a Digital Agenda for Europe.[11] *Digital* refers to '1' and '0' – two digits which are the basis of whole Internet world. Ultimately, all software and programmes start with them. In the past, *digital* was used mainly in development circles to represent the digital divide. During the last few years, *digital* has started conquering Internet linguistic space. It is likely to remain the main Internet prefix. J-C Juncker, President-elect of the European Commission used the 'digital' prefix 10 times in his speech at the European Parliament, presenting his policy plan for the next five years. In addition to the EU, Great Britain now has has *digital* diplomacy.

Virtual relates to the intangible nature of the Internet. *Virtual* introduces the ambiguity of being both intangible and, potentially, non-existent. *Virtual* reality could be both an intangible reality, (something that cannot be touched) and a reality that does not exist (a false reality). Academics and Internet pioneers used *virtual* to highlight the novelty of the Internet, and the emergence of 'a brave new world'. *Virtual*, because of its ambigious meaning, rarely appears in policy language and international documents. Today, there is truce in the war for prefix dominance.
Each prefix carves its own domain, without a catch-all domination which, for example, *cyber* had in the late 1990s. Today, *cyber* preserves its dominance in security matters. E- is still the preferred prefix for business. *Digital* has evolved from development issue use to wider use by the government sector. *Virtual* has been virtually abandoned.

The Internet Governance Cognitive Toolkit

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

The Internet Governance Cognitive Toolkit is a set of tools for developing and understanding policy argumentation. The core of the toolkit is a reference framework which includes perceptions of cause-and-effect relationships, modes of reasoning, values, terminology, and jargon. This reference framework is highly relevant in political life. It shapes how particular issues are framed and what actions are taken.

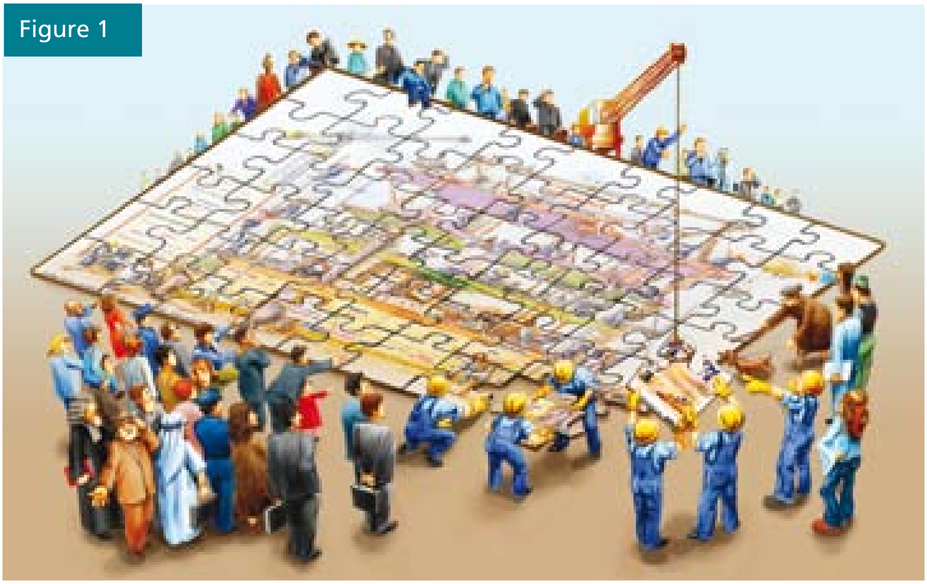
In many cases, the common reference framework is influenced by the specific professional culture (the patterns of knowledge and behaviour shared by members of the same profession). The existence of such a framework usually helps in facilitating better communication and understanding. It can also be used to protect professional turf and prevent outside influence. To quote American linguist, Jeffrey Mirel: 'All professional language is turf language.'[12]

The Internet governance regime is complex as it involves many issues, actors, mechanisms, procedures, and instruments. Figure 1, inspired by Dutch artist MC Escher, demonstrates some of the paradoxical perspectives associated with Internet governance.

The toolkit reflects the nature of Internet governance, as a so-called wicked policy area, characterised by the difficulty encountered in assigning causation for policy development to one specific reason. In many cases, every problem is a symptom of another problem, sometimes creating vicious circles. Certain cognitive approaches, such as linear, mono-causal, and either/or thinking, have a very limited utility in the field of Internet governance. Internet governance is too complex to be strapped inside a corset of coherence, non-contradiction, and consistency. Flexibility, and being open and prepared for the unexpected, might be the better part of Internet.[13]

Like the Internet governance process, the toolkit is also in flux. Approaches, patterns, and analogies emerge and disappear depending on their current relevance in the policy process. They support specific policy narratives in the Internet governance debate.

Figure 1



Approaches and patterns

A number of approaches and patterns have gradually emerged, representing points where differences in negotiation positions as well as in professional and national cultures can be identified. Identifying common approaches and patterns may reduce the complexity of negotiations and help to create a common reference framework.

Narrow vs broad approach

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

Technical and policy coherence

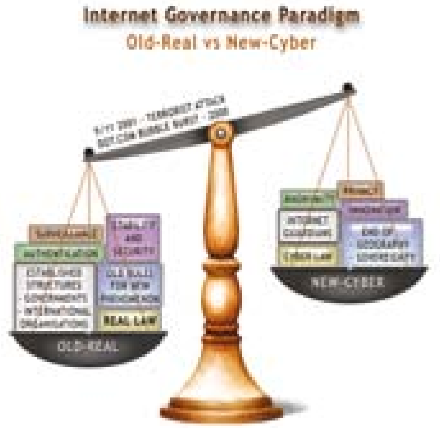
A significant challenge facing the Internet governance process has been the integration of technical and policy aspects, as it is difficult to draw a clear distinction between the two. Technical solutions are not neutral. Ultimately, each technical solution/option promotes certain interests, empowers certain groups, and, to a certain extent, impacts social, political, and economic life. In the case of the Internet, for a long time both the technical and the policy aspects were governed by just one social group – the early Internet community.

With the growth of the Internet and the emergence of new Internet governance actors – mainly the business sector and governments – it was difficult for the Internet community to maintain an integrated coverage of technical and policy issues under one roof. Subsequent reforms, including the creation of ICANN, have tried to re-establish coherence between technical and policy aspects. This issue remains open, and as expected, has shown to be one of the controversial topics in the debate on the future of Internet governance.

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

There are two approaches to almost every Internet governance issue (Figure 2). The 'old-real' approach argues that the Internet has not introduced anything new to the field of governance. It is just another new device, from the governance perspective, no different from its predecessors: the telegraph, the telephone, and the radio.

Figure 2


Internet Governance Paradigm
Old-Real vs New-Cyber
9/11 2001 - TERRORIST ATTACK
DOT.COM BUBBLE BURST - 2000
SURVEILLANCE
AUTHENTICATION
STABILITY AND SECURITY
ESTABLISHED STRUCTURES - GOVERNMENTS - INTERNATIONAL ORGANISATIONS
OLD RULES FOR NEW PHENOMENON
REAL LAW
OLD-REAL
ANONYMITY
PRIVACY
INNOVATION
INTERNET GUARDIANS
END OF GEOGRAPHY SOVEREIGNTY
CYBER LAW
NEW-CYBER

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

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

Decentralised vs centralised structure of Internet governance

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

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

Protection of public interests on the Internet

One of the main strengths of the Internet is its public nature, which has enabled its rapid growth and also fosters creativity and inclusiveness. How to protect the public nature of the Internet will remain one of the core issues of the Internet governance debate. This problem is especially complicated given that a substantial part of the core Internet infrastructure – from transcontinental backbones to local area networks – is privately owned. Whether or not private owners can be requested to manage this property in the public interest and which parts of the Internet can be considered a global public good are some of the difficult questions that need to be addressed. The question of the public nature of the Internet has been re-opened through the debate on network neutrality.

See **Section 2** for further discussion on network neutrality

Geography and the Internet

One of the early assumptions regarding the Internet was that it overcame national borders and eroded the principle of sovereignty. With Internet communication easily transcending national borders and user anonymity embedded in the very design of the Internet, it seemed to many, to quote the famous Declaration of Independence of Cyberspace,[5] that governments had 'no moral right to rule us [users]' nor 'any methods of enforcement we have true reason to fear'. Technological developments of the recent past, however, including more sophisticated geo-location software, increasingly challenge the view of the end of geography in the Internet era.

Today, it is still difficult to identify exactly who is behind the screen but it is fairly straightforward to identify their geographical location. The more the Internet is anchored in geography, the less unique its governance is. For example, with the possibility of geographically locating Internet users and transactions, the complex question of jurisdiction on the Internet can be solved through existing laws.

Policy uncertainty

Internet technology develops very quickly. New services are introduced almost on daily basis. This creates additional difficulties in organising the Internet governance debate. For example, in November 2005, when the current Internet governance arrangement was negotiated at WSIS in Tunisia,[14] Twitter did not exist. Today, Twitter has triggered some of the core Internet governance issues, such as protection of privacy, freedom of expression, and protection of intellectual property.

Another example of fast technology changes is the relevance of spam. Back in 2005, it was one of the key governance issues. Today, thanks to highly sophisticated technological filters, spam is a less prominent IG issue.

Policy balancing acts

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

- Freedom of expression *vs* protection of public order: the well-known debate between Article 19 (freedom of expression) and Article 27 (protection of public order) of the Universal Declaration on Human Rights has been extended to the Internet. It is very often discussed in the context of content control and censorship on the Internet.
- Cybersecurity *vs* privacy: like security in real life, cybersecurity may endanger some human rights such as the right to privacy. The balance between cybersecurity and privacy is in constant flux, depending on the overall global political situation. After 09/11 with the securitisation of the global agenda, the balance shifted towards cybersecurity.

See **Section 2** for further discussion on cybersecurity

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

See **Section 3** for further discussion on intellectual property

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

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:

- those invented for the Internet (e.g. ICANN);
- those that require considerable adjustment in order to address Internet-related issues (e.g. trademark protection, e-taxation); and
- 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 and yet remain flexible enough to adopt changes leading towards increased functionality and higher legitimacy. General consensus recognises that the stability and functionality of the Internet should be one of the guiding principles of Internet governance.

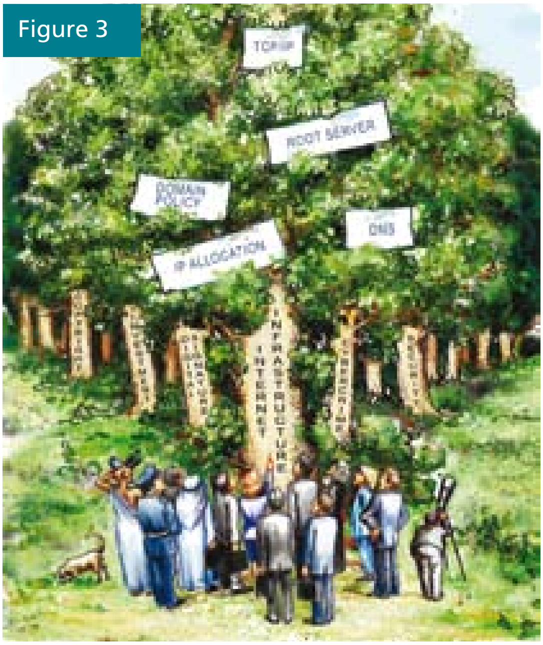
The stability of the Internet should be preserved through the early Internet approach of 'running code', which involves the gradual introduction of well-tested changes in the technical infrastructure. However, some actors are concerned that the use of the slogan 'if it ain't broke, don't fix it' will provide blanket immunity from any changes in the current Internet governance, including changes not necessarily related to technical infrastructure. One solution is to use this principle as a criterion for the evaluation of specific Internet-governance-related decisions (e.g. the introduction of new protocols and changes in decision-making mechanisms).

Promotion of a holistic approach and prioritisation

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

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.

Figure 3



Among developing countries there are considerable differences in priorities, level of development, and IT-readiness (e g. between ICT-advanced countries, such as India, China, and Brazil, and some least-developed countries in sub-Saharan Africa).

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

The principle of technological neutrality

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

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

See **Section 2** for further discussion on network neutrality

Make tacit technological solutions explicit policy principles

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

Avoid the risk of running society through programmers' code

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

Analogies

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

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

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

Second, with the increasing convergence of different telecommunication and media services, the traditional differences between the various services are blurring. For example, with the introduction of VoIP, it is increasingly difficult to make a clear distinction between the Internet and telephony. In spite of these limiting factors, analogies are still powerful; they are still the main cognitive tool for solving legal cases and developing an Internet governance regime.

Internet – telephony

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

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

Used by: This analogy is used by those who oppose the regulation of Internet content (mainly in the USA). If the Internet were analogous to the telephone, the content of Internet communication cannot be legally controlled, unlike – for example – broadcasting. It is also used by those who argue that the Internet should be governed like other communication systems (e.g. telephony, post), by national authorities with a coordinating role of international organisations, such as the ITU. According to this analogy, the Internet DNS should be organised and managed like the telephony numbering system.[15]

A new twist in the complex analogy was created by VoIP (e.g. Skype) which performs the function of the telephone while using Internet protocols. This dichotomy triggered a policy controversy at the 2012 World Conference on International Telecommunications (WCIT) in Dubai. The current view that VoIP is the Internet service is challenged by those who argue that it should be regulated like telephone service on both national and international level, including a more prominent role for the ITU.

Internet – mail/post

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

The postal system and ICANN

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

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 the recipient than the e-mail system, where the active intermediary function is performed by ISPs or an e-mail service provider like Yahoo! or Hotmail.

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

The families of US soldiers who died in Iraq have also attempted to make use of the analogy between mail (letters) and e-mail in order to gain access to their loved ones' private e-mail and blogs, arguing that they should be allowed to inherit e-mail and blogs as they would letters and diaries. ISPs have found it difficult to deal with this highly emotional problem. Instead of going along with the analogy between letters and e-mail, most ISPs have denied access based on the privacy agreement they had signed with their users.

Internet – television

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

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

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

Internet – library

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

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

- Traditional libraries aim to serve individuals living in a particular place (city, country, etc.), whereas the Internet is global.
- Books, articles, and journals are published using procedures to ensure quality (editors). The Internet does not always have editors.
- Libraries are organised according to specific classification schemes, allowing users to locate the books in their collections. There is no such classification scheme for information on the Internet.
- Apart from keyword descriptions, the contents of a library (text in books and articles) are not accessible until the user borrows a particular book or journal. The content of the Internet is immediately accessible via search engines.

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

Internet – VCR, photocopier

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

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

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

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

Internet – highway

Similarities: What the highway is for transportation in the real world, the Internet is for communication in a virtual space.

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

Highways and the Internet

Hamadoun Touré, the ITU Secretary General, used an analogy between highways and the Internet by relating highways to telecommunications and the Internet traffic to trucks or cars: 'I was giving a simple example, comparing Internet and telecommunications to trucks or cars and highways. It is not because you own the highways that you are going to own all the trucks or cars running on them, and certainly not the goods that they are transporting, or vice versa. It's a simple analogy. But in order to run your traffic smoothly, you need to know, when you are building your roads, the weight, the height and the speed of the trucks, so that you build the bridges accordingly. Otherwise, the system will not flow. For me, that's the relationship between the Internet and the telecommunication world. They are condemned to work together.'[16]

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

> *It's a liberal law that has nothing to do with censorship but clearly sets the conditions for what a provider can and cannot do. The Internet is a means of transporting and distributing knowledge… just as with highways, there need to be guidelines for both kinds of traffic.*[17]

Internet – high seas

Similarities: Initially, this analogy was driven by the fact that like the high seas, the Internet seems to be beyond any national jurisdiction.

Differences: Nowadays, it is clear that most of the Internet lies within some national jurisdiction. The technical infrastructure through which Internet traffic is channelled is owned by private and state companies, typically telecommunication operators. The closest analogy to the Internet in the maritime field would be a shipping company's transport containers.

When it comes to legal instruments, the Convention on the Law of the Sea regulates activities beyond national jurisdiction, such as on the high seas. There is nothing analogous in the field of Internet telecommunication.

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

Classification of Internet governance issues

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

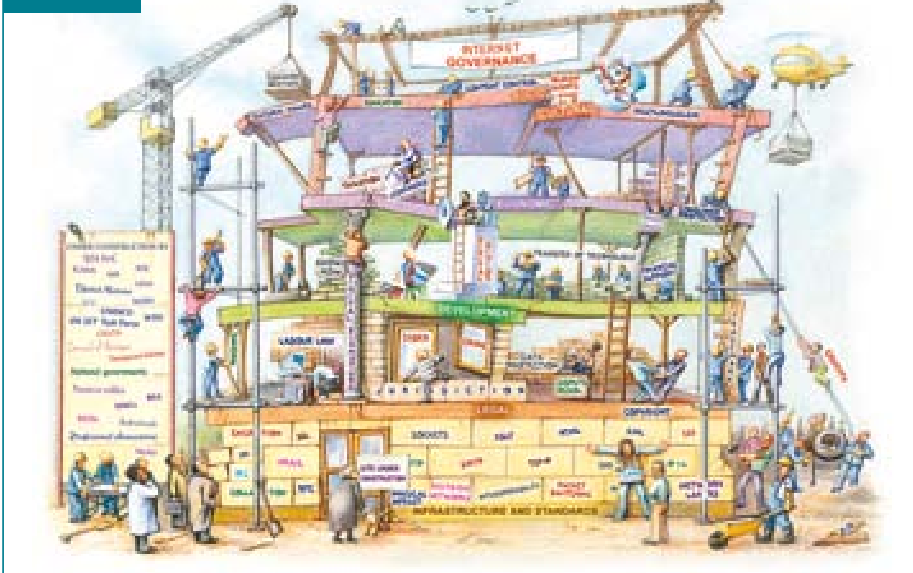
The practical need for classification was clearly demonstrated during the WSIS process. In the first phase, during the lead-up to the Geneva summit (2003), many players, including nation states, had difficulty grasping the complexity of Internet governance. A conceptual mapping, provided by various academic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

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

The agenda for the first IGF held in Athens (2006) was built around the following thematic areas: access, security, diversity, and openness. At the second IGF in Rio de Janeiro (2007), a fifth thematic area was added to the agenda: managing critical Internet resources. These five thematic areas have influenced the agendas of all subsequent IGF meetings.

Although the classification changes, Internet governance addresses more or less the same set of 40–50 specific issues, with the relevance of particular issues changing. For example, while spam featured prominently in the WGIG classification in 2004, its policy relevance diminished at the IGF meetings,

Figure 4



where it became one of the less prominent themes within the Security thematic area. Diplo's classification of Internet governance groups the main 40–50 issues into the following five baskets:

- Infrastructure and standardisation
- Legal
- Economic
- Development
- Sociocultural

This classification (Figure 4) reflects both the aforementioned (WGIG, IGF) policy approaches as well as academic research in this field. The classification was developed in 1997 with constant adjustment based on feedback from students (an alumni of 1542 students as of 2013), research results, and insights from the policy process.[18]

Endnotes

[1] The UN General Assembly Resolution 56/183 (21 December 2001) endorsed the holding of the World Summit on the Information Society (WSIS) in two phases. The first phase took place in Geneva from 10 to 12 December 2003 and the second phase took place in Tunis, from 16 to 18 November 2005. The objective of the first phase was to develop and foster a clear statement of political will and to take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake. More than 19 000 participants from 174 countries attended the summit and related events. Source: **http://www.itu.int/wsis/basic/about.html** [accessed 21 January 2014].

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

[3] Shannon V (2006) What's in an 'i'? *International Herald Tribune,* 3 December 2006. Available at: **http://www.nytimes.com/2006/12/03/technology/03iht-btitu.3755510.html** [accessed 21 January 2014].

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

[5] Barlow JP (1996) A declaration of the independence of cyberspace. Available at: **https://projects.eff.org/~barlow/Declaration-Final.html** [accessed 21 January 2014].

[6] For the evolution of the use of the word 'Internet' in the preparation for the WSIS Summit: DiploFoundation (2003) The Emerging Language of ICT Diplomacy – Key Words. Available at **http://archive1.diplomacy.edu/IS/Language/html/words.htm** [accessed 3 August 2014].

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

[8] For more on network neutrality, see our explanatory video at **https://www.youtube.com/watch?v=R-uMbZFfJVU** [accessed 12 February 2014].

[9] Clinton H (2010) Remarks on Internet freedom. Available at **http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm** [accessed 21 January 2014].

[10] Newitz A (2013) The bizarre evolution of the word 'cyber'. Available at **http://io9.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487** [accessed 3 August 2014].

[11] European Commission (no date) Digital Agenda for Europe. Available at **http://ec.europa.eu/digital-agenda/** [accessed 3 August 2014].

[12] Cited in Helfand D (2001) Edpseak is in a class by itself. *Los Angeles Times*, 16 August. Available at **http://articles.latimes.com/2001/aug/16/news/mn-34814** [accessed 13 February 2014].

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

[14] The WSIS process started with the first preparatory meeting held in July 2002 in Geneva. The first summit was held in Geneva (December, 2003) and the second summit in Tunisia (November, 2005).

[15] Volker Kitz provides an argument for the analogy between administration of telephony systems and Internet names and numbers. Kitz V (2004) ICANN may be the only game in town, but Marina del Rey isn't the only town on Earth: Some thoughts on the so-called uniqueness of the Internet. Available at **http://studentorgs.law.smu.edu/Science-and-Technology-Law-Review/Articles/Fall-2005/Kitz.aspx** [accessed 21 January 2014].

[16] Excerpts from the Secretary General's speech delivered at the ICANN meeting in Cairo (6 November 2008). Available at **https://cai.icann.org/files/meetings/cairo2008/toure-speech-06nov08.txt** [accessed 21 January 2014].

[17] Quoted in Mock K, Armony L (1998) Hate on the Internet. Available at **http://archive.is/M70XS** [accessed 13 February 2014].

[18] The term 'basket' was introduced into diplomatic practice during the Organization for Security and Co-operation in Europe (OSCE) negotiations.

Section 2

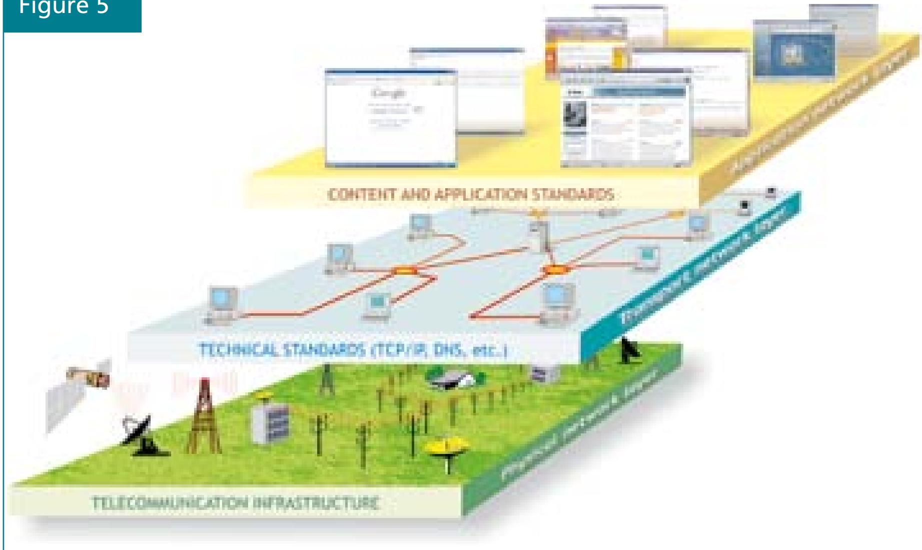
The infrastructure and standardisation basket

The infrastructure and standardisation basket

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

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

Figure 5


CONTENT AND APPLICATION STANDARDS
TECHNICAL STANDARDS (TCP/IP, DNS, etc.)
TELECOMMUNICATION INFRASTRUCTURE

1. The telecommunications infrastructure, through which all Internet traffic flows.
2. The Internet technical standards and services, the infrastructure that makes the Internet work (e.g. TCP/IP: Transmission Control Protocol/Internet Protocol; DNS: domain name system; SSL: secure sockets layer).
3. The content and applications standards (e.g. HTML: HyperText Markup Language; XML: eXtensible Markup Language)

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

The telecommunication infrastructure[2]

The current situation

Internet data can travel over a diverse range of communication media: telephone wires, fibre-optic cables, satellites, microwaves, and wireless links. Even the standard electric grid can be used to relay Internet traffic utilising power line technology.[3]

The way in which telecommunication is regulated impacts Internet governance directly. The telecommunications infrastructure is regulated at both national and international level by a variety of public and private organisations. The key international organisations involved in the regulation of telecommunications include the International Telecommunication Union (ITU), which developed rules for coordination among national telecommunication systems, the allocation of the radio spectrum, and the management of satellite positioning; and the World Trade Organization (WTO), which played a key role in the liberalisation of telecommunication markets worldwide.[4]

The ITU International Telecommunication Regulations (ITRs)

The 1988 ITU International Telecommunication Regulations (ITRs) facilitated the international liberalisation of pricing and services and allowed a more innovative use of basic services in the Internet field, such as international leased lines, in the Internet field. They provided one of the infrastructural bases for the rapid growth of the Internet in the 1990s. The ITRs were amended in December 2012 during WCIT-12 in Dubai; 89 states – mostly developing countries – have signed the amended ITRs, while 55 states, including the USA and many European states, have not.[5]

The roles of the ITU and the WTO are quite different. The ITU sets detailed voluntary technical standards and telecommunication-specific international regulations, and provides assistance to developing countries.[6] The WTO provides a framework for general market rules.[7]

Following liberalisation, the ITU's near monopoly as the principal standards-setting institution for telecommunications was eroded by other professional bodies and organisations. At the same time, large telecommunication companies – such as AT&T, Cable and Wireless, France Telecom, Sprint, and WorldCom – were given the opportunity to globally extend their market coverage. Since most Internet traffic is carried over the telecommunication infrastructures of such companies, they have an important influence on Internet developments.

The issues

The local loop – last mile

The 'local loop' (or 'last mile') is the name given to the connection between ISPs and their individual customers. Problems with local loops are an obstacle to the more widespread use of the Internet in many, mainly developing countries. Wireless communication is one possible, low-cost solution to the local loop problem.[8] Apart from increasingly available technological options, the solution to the problem of the local loop also depends on the liberalisation of this segment of the telecommunication market.

The liberalisation of telecommunication markets

A considerable number of countries have liberalised their telecommunication markets with the aim of boosting development of new communication services by allowing access to existing (state-owned) infrastructure. However, many developing countries are faced with a hard choice: to liberalise and make the telecommunication market bigger and more efficient, or to preserve an important budgetary income from the existing telecommunication monopolies. This question was discussed at the World Conference on International Telecommunications 2012 (WCIT-12) with some developing countries raising the question of redistribution of income from Internet communication services.[9]

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.[10] The very function of setting or implementing standards in such a fast developing market affords these institutions considerable influence.

Who owns the electromagnetic spectrum?

The current regime of spectrum management is based on the assumption that it is a scarce resource that should be managed by government institutions, regional initiatives (such as the EU's Radio Spectrum Committee (RSC) and the Radio Spectrum Policy Group (RSPG)), and the ITU. Development of new technologies that use the spectrum more efficiently than before has resulted in it being conceived as a less scarce resource in practice. Ultimately, the volume and limits of the use of the spectrum will depend on technological developments. This approach argues that current government regulation should be replaced with an 'open spectrum', i.e., open access for all.

There are two potential problems with this view. One is practical and related to the huge investments that telecommunications companies, especially in Europe, made in acquiring the rights to operate third-generation mobile-phone networks.[11] The other issue is that if the spectrum becomes a free-for-all, this does not necessarily mean that it will be used by many as a public good. Rather, it will be utilised by actors that have technical capacities to utilise 'free' spectrum.

The development of new communication services using radio spectrum, most notably wireless broadband and mobile communications, has increased the demand for radio frequencies, urging governments around the world to find solutions to accommodate an optimal spectrum use. Replacing conservative analogue broadcasting with digital television allows the freeing up of an important part of the radio spectrum that can be thus allocated to other services – the so-called digital dividend. The EU has developed a comprehensive regulatory programme for radio spectrum management,[12] while the USA has taken a market-led approach by submitting the frequencies to auction processes.

Transmission Control Protocol/Internet Protocol (TCP/IP)

The current situation

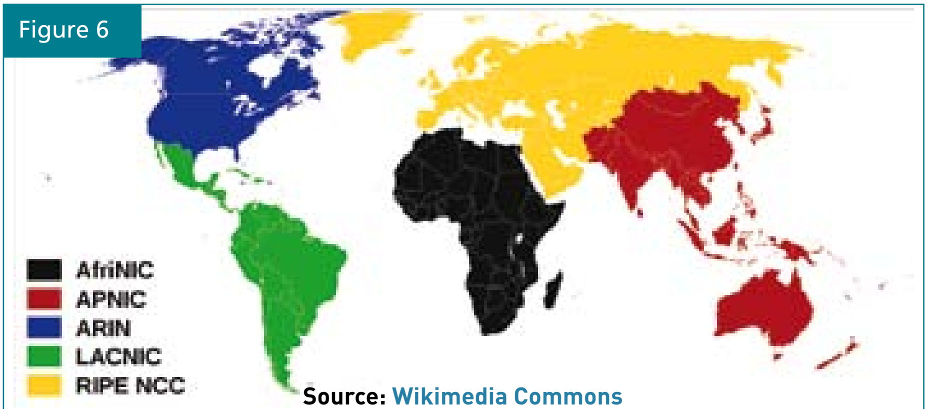
TCP/IP is the main Internet technical standard. It is based on three principles: packet-switching, end-to-end networking, and robustness. Internet governance related to TCP/IP has two important aspects:

- The introduction of new standards
- The distribution of IP numbers

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

IP numbers are unique numeric addresses that all computers connected to the Internet must have. 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 the Internet Corporation for Assigned Names and Numbers – ICANN), which distributes blocks of IP numbers to the five regional Internet registries (RIRs).[13] RIRs distribute IP numbers to the local Internet registries (LIRs) and national Internet registries (RIRs), which in turn distribute IP numbers to smaller ISPs, companies, and individuals further down the ladder.

Figure 6



Source: Wikimedia Commons

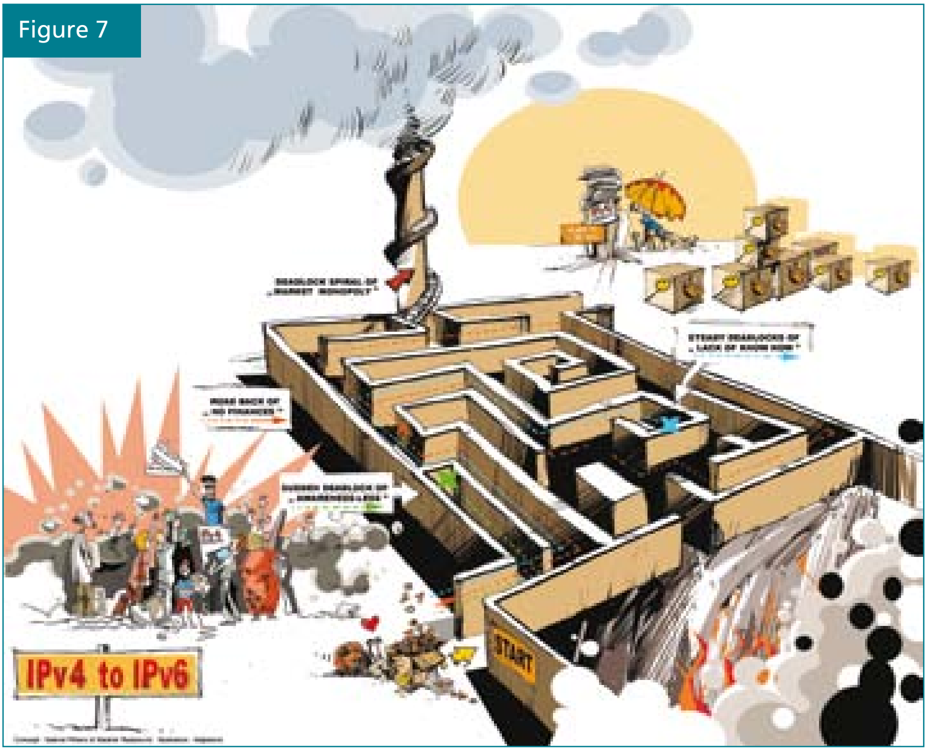
The issues

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

The pool of IP numbers under IPv4 (Internet Protocol, version 4) contains some four billion numbers which had been fully allocated by IANA between the five RIRs in February 2011. The depletion of IPv4 numbers was accelerated with the introduction in recent years of Internet-enabled devices (such as mobile phones, personal organisers, game consoles, and home appliances) and the rise of worldwide Internet connectivity. The concern that IP numbers might run out and eventually inhibit the further development of the Internet has led the technical community to take three major actions.

- Rationalise the use of the existing pool of IP numbers through the introduction of Network Address Translation (NAT).
- Address the wasteful address allocation algorithms used by the RIRs by introducing Classless Inter-Domain Routing (CIDR).
- Introduce a new version of the TCP/IP protocol – IPv6 – which provides a much bigger pool of IP numbers (over 340,000,000,000,000,000,000).

Figure 7


DEADLOCK SPIRAL OF „MARKET MONOPOLY"
STEADY DEADLOCKS OF „LACK OF KNOW HOW"
ROAD BACK OF „NO FINANCES"
SUDDEN DEADLOCK OF
START
IPv4 to IPv6

The response of the Internet technical community to the problem of a potential shortage of IP numbers is an example of prompt and proactive management. While both NAT and CIDR provided a quick fix for the problem, a proper long-term solution is the transition to IPv6. Although IPv6 was introduced back in 1996, its deployment has been very slow, due to lack of awareness about the need for transition as well as limited funds for investment in new equipment in developing countries.

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

Given the complexity of the transition to IPv6, developing countries may benefit from the delayed start and the possibility of introducing IPv6-based networks from the beginning. In this process, developing countries will need technical assistance.[14]

Apart from the problem of transition, the policy framework for IPv6 distribution will require a proper distribution of IP numbers, demanding the introduction of open and competitive mechanisms to address the needs of end-users in the most optimal way. Even with the introduction of IPv6 an 'artificial' scarcity of IP numbers could still arise, if those responsible for allocating them at local level, such as ISPs, choose to abuse their power and link such allocation to, for example, the purchase of other services, thus affecting the availability and price of IP numbers.

Changes in TCP/IP and cybersecurity

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

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, the TCP/IP. A new protocol (IPv6) provides some security improvements, but still falls short of a comprehensive solution. Such protection would require considerable modifications to TCP/IP.[15]

Technology, standards, and politics

Standardisation could be politics by other means. Technical standards could have far-reaching economic and social consequences, promoting specific interests and altering the balance of power between competing businesses and/or national interests. Standards are essential for the Internet. Through standards and software design, Internet developers can shape how human rights are used and protected (e.g. freedom of information, privacy, and data protection).

Efforts to create formal standards bring private technical decisions made by system builders 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.

Changes in TCP/IP and the problem of limited bandwidth

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

The Domain Name System (DNS)

The current situation

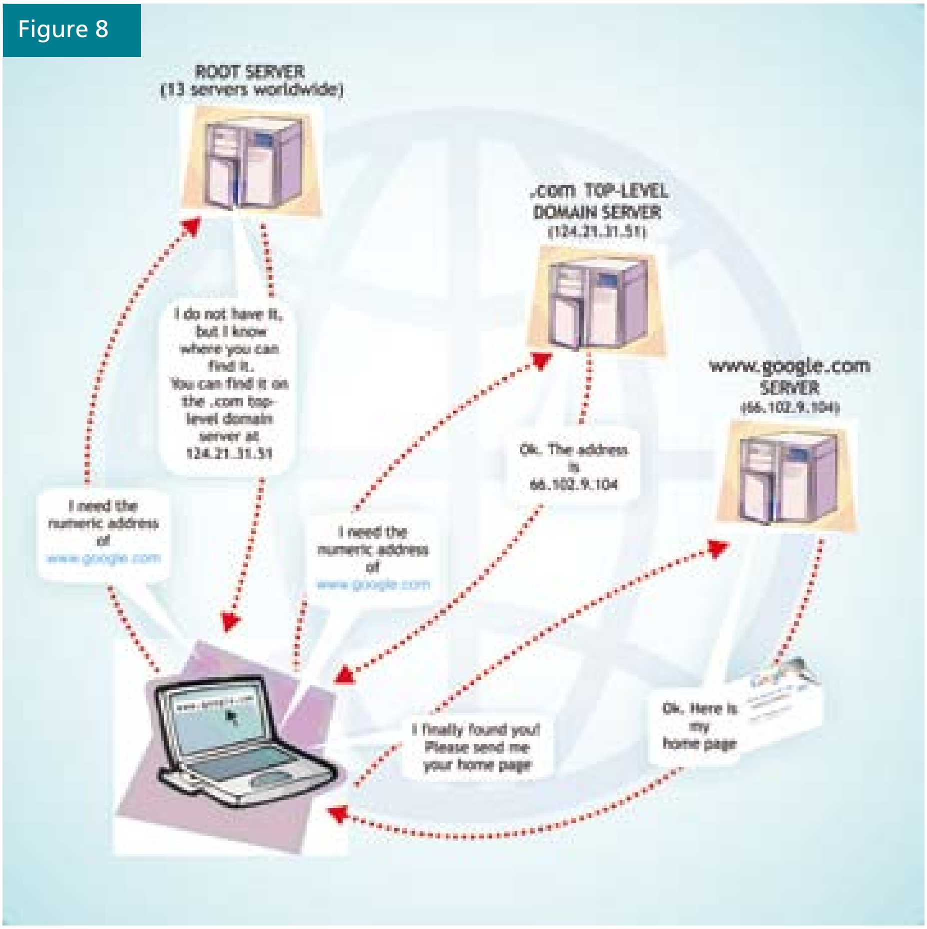
The DNS handles Internet addresses (such as www.google.com) and converts them to IP numbers (a simplified scheme of this process is presented in Figure 8). The DNS consists of root servers, top-level domain (TLD) servers, and a large number of DNS servers located around the world.[16]

The DNS includes three types of top-level domains: generic (gTLD), country code (ccTLD), and sponsored (sTLD). gTLDs include domains that could be obtained by anyone (.com, .info, .net, and .org). Since 2014 many other gTLDs have been added like .pub, .رازاب (bazaar), .rentals, .ngo, or .游戏 (game). sTLDs are limited to a specific group. For example, the sTLD '.aero' is open for registration only for air-transport industry. ccTLDs are designating specific countries or territories (.uk, .cn, .in).

For each gTLD there is one registry that maintains an address list. For example, the .com gTLD is managed by VeriSign. The salesman function is performed by registrars. ICANN provides overall coordination of the DNS system by concluding agreements and accrediting registries and registrars. An important part of DNS management is the protection of trademarks and dispute resolution. The first-come-first-served principle of domain name allocation used in the early days of the Internet triggered the phenomenon known as cybersquatting, the practice of registering domain names that could be resold later. The Uniform Dispute Resolution Policy (UDRP) developed by ICANN and the World Intellectual Property Organization (WIPO)

See **Section 3** for further discussion on intellectual property

Figure 8


ROOT SERVER
(13 servers worldwide)
.com TOP-LEVEL
DOMAIN SERVER
(124.21.31.51)
www.google.com
SERVER
(66.102.9.104)
I do not have it, but I know where you can find it. You can find it on the .com top-level domain server at 124.21.31.51
Ok. The address is 66.102.9.104
I need the numeric address of www.google.com
I need the numeric address of www.google.com
I finally found you! Please send me your home page
Ok. Here is my home page

provides mechanisms that have significantly reduced cybersquatting. Intellectual property is discussed in more detail in the Legal basket.

Another important element in the survey of the current organisation of DNS governance is the management of ccTLDs. Currently, some country codes are still managed by a variety of institutions or individuals that received accreditation in the early days of the Internet, when some governments were not all that interested in such matters.

The issues

The creation of new generic domain names

Technically, the creation of new TLDs is almost unlimited. However, the introduction of new gTLDs has been a very slow and debated process.[17] After six years of consultations and development of a new policy, ICANN began implementation of a new gTLD programme in 2012. Under the new programme, any organisation in the world could apply to run a new gTLD registry, including in non-Latin language scripts. The main opposition to the creation of new gTLDs originated from the trademark lobby, concerned about the protection of their trademarks in the context of the increasing number of domains and the increase of cybersquatting. Although the debate on the introduction of new gTLDs continues, the programme is up and running.

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

Intellectual property was not the only concern in this process. The most illustrative situation was the proposal to introduce the .xxx domain for adult materials.[18] Initiated first in 2000 and resubmitted in 2004, the proposal was rejected by the ICANN Board in March 2007. The main criticism of this decision was that ICANN made it under pressure from the US government, which strongly opposed its introduction.[19] Such a move by the US government resulted in a wide range of reactions. Among them were sceptical voices stating that .xxx wouldn't be attractive to the Internet sex business because of the risk of being heavily filtered. The issue was revisited in June 2010 following a new submission; the ICANN Board positively reviewed the application for the .xxx domain, which was finally approved as an sTLD in 2011. This decision also re-opened the discussion about ICANN's role in public policy issues.

Other controversies may continue to arise in relation to gTLDs for cultural and linguistic communities. In 2003, ICANN introduced a new .cat domain for the Catalan language – the first domain introduced for a language.[20] This decision was not opposed by the Spanish government, but there could be cases where language and cultural communities requesting the same may have aspirations towards nationhood and this aspect might cause potential controversy and conflict with existing states.

Protection of geographical indicators appeared to be another hot potato: ICANN stopped the delegation process for .amazon to Amazon (the online retailer) after a strong revolt from Latin American countries in its Governmental Advisory Committee (GAC). Delegation of .wine/.vin has been strongly contested by Switzerland and France, as well as several other countries. When ICANN assigned .Africa to the consortium led by the African Union Commission, this decision was contested by a private company.[21]

The management of country domains[22]

The management of ccTLDs involves three important issues. The first concerns the often politically controversial decision as to exactly which country codes should be registered when dealing with countries and entities with unclear or contested international status (e.g. newly independent countries, resistance movements). One controversial issue was the allocation of a Palestinian Authority domain name. In justifying its decision to assign the .ps TLD, IANA reiterated the principle of allocating domain names in accordance with the ISO 3166 standard for country codes, as was proposed by Jon Postel, one of the founding fathers of the Internet.[23]

The second issue concerns who should manage ccTLDs. Many countries have been trying to gain control over their country domains, which are considered to be national resources. National governments have chosen a wide variety of policy approaches.[24] Transition (re-delegation) to a new institution managing the ccTLD (delegee) within each country is approved by ICANN only if there is no opposition from any of the interested stakeholders within the country. Given the importance of this issue and the wide variety of approaches, there were two important initiatives at international level to introduce a certain level of harmonisation. The first, the GAC Principles,[25] was adopted by ICANN's GAC, which proposed policy and specified procedures for the re-delegation of ccTLD administration. The second was Best Practices, proposed by the World Wide Alliance of Top-Level Domains (June 2001).

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

Internationalised domain names

The Internet was originally a predominantly English-language medium. Through rapid growth, it has become a global communication facility with an increasing number of non-English-speaking users. For a long time, the lack of multilingual features in the Internet infrastructure was one of the main limits of its future development.

In May 2010, after a long testing period and political uncertainties, ICANN started approving TLDs in a wide variety of scripts, including Chinese, Arabic, and Cyrillic. The introduction of internationalised domain names

(IDNs) is considered to be one of the main successes of the Internet governance regime.

Root servers

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

The current situation

The function and robustness of the DNS can be illustrated by analysing the concern that the Internet would collapse if the root servers were ever disabled. First, there are 13 root servers distributed around the world, the maximal number technically possible: 10 in the USA and one each in Sweden, the Netherlands, and Japan; of the 10 in the USA, several are operated by US government agencies. If one server crashes, the remaining 12 would continue to function. Even if all 13 root servers went down simultaneously, the resolution of domain names into IP addresses (the main function of root servers) would continue on another domain name servers, distributed hierarchically throughout the Internet.[26]

Therefore, hundreds 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.

The system of root servers is considerably strengthened by the Anycast scheme,[27] which replicates root servers throughout the world. This provides many advantages, including an increased robustness in the DNS and the faster resolving 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:[28] academic/public institutions (6), commercial companies (4), and government institutions (3). Institutions managing root servers receive a root zone file proposed by IANA (ICANN) and approved by the US government (Department of Commerce). Once the content is approved by the Department of Commerce, it is entered into the master root server operated by VeriSign under contract to the Department.[29]

The file in the master root server is then automatically replicated on 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

Internationalisation of the control of root servers

Many countries have expressed concern about the current arrangement in which the ultimate decision-making concerning the content of root servers remains the responsibility of one country (the USA). There were various proposals in the Internet governance process, including adopting a Root Convention, which would put the international community in charge of policy supervision of the root servers or, at least, grant nation states rights over their own national domain names.

New possibilities for solutions are open with the announcement of the US government (NTIA) to relinquish the supervision over IANA and pass to new mechanisms/body. The transition process, that is expected to complete by 30 September 2015, should be guided by the following principles:[30]

- Support and enhance the multistakeholder model.
- Maintain the security, stability, and resiliency of the Internet DNS.
- Meet the needs and expectation of the global customers and partners of the IANA services.
- Maintain the openness of the Internet.

Alternative root servers – feasibility and risks

Creating an alternative root server is technically straightforward. The main question is how many followers an alternative server would have, or, more precisely, how many computers on the Internet would point to it, when it came to resolving domain names. Without users, any alternative DNS becomes useless. A few attempts to create an alternative DNS have been made: Open NIC, New.net, and Name.space. Most of them were unsuccessful, accounting for only a few percent of Internet users.

Conceptual discussion: single vs alternative root server system

For a long time, the principle of the single root server was considered to be one of the main Internet mantras, which were not supposed to be touched or even discussed. Various arguments have been put forward in order to prevent any discussions about alternatives to the single root server. One argument is that the current (single root server) system prevents the risk of the DNS being used by some governments for censorship.[31] However, the censorship argument against changes in DNS policy is losing ground on a functional basis. Governments do not need control over the DNS system or the root zone file in order to introduce censorship. They already rely on more effective tools, based on the filtering of Web traffic.

A more solid argument is that any alternative root servers could lead towards the fragmentation and even, maybe, the ultimate disintegration of the Internet, including one possible scenario of violent disintegration. The fragmentation of the Internet could endanger one of the core functions of the Internet – a unified global communication system. How realistic is this danger? Vittorio Bertola provides a very comprehensive analysis of this challenge.[32]

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

The potential of removing other countries' domain names from the Internet has often been mentioned in discussions of the USA's key role in the management of root servers. The potential power of removing a country from the Internet (by deleting the country's domain name) can hardly be qualified as a power, since it has no effective use. The key element of power is forcing the other side to act in the way the holder of power wants. The use of US power could create unintended consequences, including countries and regions establishing their own Internets. In such a scenario, the Internet might disintegrate and US interests could be endangered (the predominance of US values on the Internet, English as the Internet *lingua franca,* the predominance of US-based companies in the field of e-commerce and Internet services). This power over root servers has not been used even in the case of military conflicts between the USA and other countries (e.g. Yugoslavia, Iraq, Libya).

Internet access: Internet service providers (ISPs)

Since ISPs connect end-users to the Internet, they provide the most direct and straightforward enforcement of legal rules on the Internet. This is why many states have started concentrating their law enforcement efforts on ISPs.

The issues

Telecommunication monopolies and ISPs

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

ISPs responsibility for copyright

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

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

The approach of placing limited liability on ISPs has been generally supported by jurisprudence. Some of the most important cases where ISPs were freed of responsibility for hosting materials in breach of copyright law are the Scientology Case (the Netherlands),[33] RIAA vs Verizon (United States),[34] SOCAN vs CAIP (Canada),[35] and more recently Scarlet vs SABAM (Belgium).[36]

Nevertheless, recent years have witnessed an increased pressure on ISPs to handle copyright matters, since their position of gatekeepers between end-users and Internet content places them in the best position to control access. This argument was speculated in promoting legal provisions such as Hadopi Law in France forcing ISPs to intervene in case of suspicions of copyright infringements.

See **Section 3** for further discussion on copyright

The role of ISPs in content policy

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

The role of ISPs in anti-spam policy

ISPs are commonly seen as the primary institutions involved with anti-spam initiatives. Usually, ISPs have their own initiatives for reducing spam, either through technical filtering or the introduction of anti-spam policy. The ITU's report on spam states that ISPs should be liable for spam and proposes an anti-spam code of conduct, which should include two main provisions:

- An ISP must prohibit its users from spamming.
- An ISP must not peer with ISPs that do not accept a similar code of conduct.[37]

The problem of spam exposes ISPs to new difficulties. For instance, Verizon's anti-spam filtering led to a court case as it also blocked legitimate messages causing inconvenience for users who did not receive their legitimate e-mail.[38]

Internet access: 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 providers (IBPs). Tier 1 carriers are the major IBPs. They usually have peering[39] arrangements with other Tier 1 IBPs. The main difference between Tier 1 and Tier 2 IBPs is that Tier 1 IBPs exchange traffic through peering, while Tier 2 IBPs have to pay transit fees to Tier 1 providers.[40] Tier 1 is usually run by large companies, such as AT&T, Verizon, Level 3 Communications, Sprint, and NTT Communications.

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 (i.e., principal data routes between large, strategically interconnected networks and core routers in the Internet), commonly having optical cables or satellite links, have become critical to the operation of the Internet. Their pivotal position within the Internet network grants their owners the market power to impose prices and conditions for providing their services.[41] Ultimately, the functioning of the Internet could depend on the decisions taken by the owners of central backbones.

Can reliability be guaranteed?

Is it possible for the global Internet community to request assurances and guarantees for the reliable functioning of the critical Internet infrastructure from major Internet companies and telecommunication operators? The trend in discussion is on imposing certain public requirements on private Internet infrastructure operators.

IBPs and critical infrastructure

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

- Are the main Internet cables properly protected?
- What are the respective roles of national governments, international organisations, and private companies in the protection of Internet cables?
- How can we manage the risks associated with potential disruption of the main Internet cables?

Telecommunications liberalisation and the role of ISPs and IBPs

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

Network neutrality

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

The importance of network neutrality to the success of the Internet is key. The debate has attracted a wide range of actors: everyone from the President of the United States to human rights grassroots activists. The way in which network neutrality is treated can influence the future development of the Internet.

The current situation

Paradoxically, network traffic management has always been in place. Since the early days of dial-up modem connection to the Internet, there has been a gap between available bandwidth and the users' bandwidth needs. In order to address this challenge and provide quality service, Internet operators (telecom companies and ISPs) – also commonly referred to as carriers – have used various traffic management techniques to prioritise certain traffic. For example, Internet traffic carrying voice conversation over VoIP services (e.g. Skype) should have priority over traffic carrying a simple email: while we can hear delays in Skype voice chat, we won't notice minor delays in an email exchange. The need for traffic management is especially important today with the extended demands for high bandwidth: a growing number of users regularly use Internet voice and video calls (Skype, Google Hangout, teleconferencing), play online games, or watch TV shows and movies in high definition (HD) quality (e.g. services like Hulu or Netflix). Traffic management is important for wireless communication due to, on one hand, expansion of use of mobile devices and, on the other hand, the technical limits of the wireless spectrum. [42] Cisco predicts that, by 2020, some 50 billion devices will be connected to the Internet within the expanding concept of the Internet of Things.[43]

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

The issues

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

Economic issues

During the past few decades, many significant network operators – including both telecoms and ISPs – have changed their business models: besides providing Internet access to households and businesses, they have introduced their own VoIP (telephony via Internet) or IPTV (television via Internet) services, video on demand (akin to renting movies), music or video download portals, etc. They are now competing not only with their counterparts for providing cheaper, faster, and better quality connections, but also with the over-the-top (OTT) service providers – content and service providers like Google, Facebook, Netflix, and Skype.

Traffic management may be an important tool when competing in service and content provision by prioritising packages according to business-driven preferences. For instance, an operator may decide to slow down or fully ban the flow of data packages from a competing company (such as Skype or Google Voice) to end-users through its network, while giving priority to data packages of its own in-house service (such as the IP telephony or Internet television it offers to its customers).[44]

At the same time, operators argue that the expansion of bandwidth demand begs for increased investments in basic infrastructure. Seeing OTT service providers as the ones contributing the most to the expanded demand and benefiting the most from the improved infrastructure, they are suggesting multi-tiered network policy models that would request the OTT service providers to pay for the outreach to operators' customers (Internet end-users) if they wish a guaranteed quality of service. In such cases, traffic management would again be used for economic rather than technical reasons. In order to search for a way to the increased income, the telecoms designed a new type of offers. Zero rating tariffs offered to customers by mobile telecom providers allow unlimited (free) use of specific applications like Facebook or Wikipedia; while this is certainly financially beneficial for customers, it prioritises certain services over the other. Besides, telecoms refer to 'specialised services' – such as HD video streaming offers that require high bandwidths, or future e-health solutions – that may need to be offered in future and would require high quality and therefore special treatments.

Proposals on a multi-tier Internet have been at the heart of discussions on net neutrality for years. The business tier has also been proposed in the form of 'additional online services', by Verizon and Google in their Legislative Framework Proposal for an Open Internet[45] in 2010. Proponents argue this would bring more choice of services for users and encourage investment in the infrastructure; opponents fear the best effort network will suffer and eventually disappear, since both economic and business tiers would effectively use same 'pipes' (i.e., wireless spectrum and cables).

In the meantime, the market has brought changes in the way the Internet works: in order to reduce transit costs and time, content providers have come closer to users by setting up Content Delivery Networks (CDNs) – caching servers placed close to regional IXP hubs or within big regional telecoms. This has improved network performance and costs – yet only for OTT companies that can afford to build or rent CDNs and pay the telecoms companies for placement.[46]

Multi-tier Internet

The Internet traffic is currently delivered with 'best effort': it implies no guarantees of a QoS, effective speed, or delivery time of data packages. Instead, users share the available bandwidth and obtain variable bit rates (speed) depending on the traffic load at the time.[47] Traffic management therefore plays an important role in the effective quality of service for end-users.

The multi-tier Internet concept refers to introducing a 'the business tier' to the Internet, i.e., special services with a guaranteed QoS beyond best effort. Proponents explain that the business tier would run in parallel with the 'economic tier' (the Internet as we know it now) which would remain based on best effort; besides, they say the OTT service providers could still decide to run their services through the best effort network without cost, if they wished to do so.

Human rights issues

Consequences of the violation of network neutrality principles are not only economic. The Internet has become way more important than just for the economy – it has become one of the key pillars of modern society linked to basic human rights, including access to information, freedom of expression, health, and education. Entirely profit-led models (even if clearly leading to more innovation and investment) may increase the divide between the haves and the have nots: while the rich would be using unlimited online services with full quality, the poor might ultimately end up with useless, best-effort services or only prioritised services – a choice of which would be made by the telecom providers based on their economic interests. Endangering Internet openness could thereby impact fundamental rights.

Besides, the ability to manage network traffic based on origin or destination, on service or content, could give authorities the opportunity to filter Internet traffic with objectionable or sensitive content in relation to the country's political, ideological, religious, cultural, or other values. This opens possibilities for political censorship through Internet traffic management.

Users or customers?

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

Who are the main players and what are their arguments?

The position of the main players is in a state of constant flux. For example, the Google-Verizon 2010 proposal for a mid-way approach to network neutrality shook the positioning of the main players.[48] Google has been considered one of the main proponents of network neutrality; others include consumer advocates, online companies, some technology companies, many major Internet application companies including Yahoo!, Vonage, Ebay, Amazon, EarthLink, and software companies like Microsoft.

Opponents of network neutrality include the main telecom companies, ISPs, producers of networking equipment and hardware, and producers of video and multimedia materials. Their arguments against any related regulation are market-centred, starting from the need to offer what consumers want. Contrary to the common tendencies of the telecom operators against any regulation on net neutrality, the ETNO proposal to WCIT-12 requested international regulation – one that should prevent further national regulations protecting net neutrality! Their US counterparts – like Verizon – however, oppose the ETNO initiative.[49]

There are four main arguments in the network neutrality debate (Table 1).

Table 1

Argument	Proponents of network neutrality	Opponents of network neutrality
Past/future argument	New Internet companies developed thanks to the Internet's open architecture, and end-users are benefiting from innovation and diversity of services thanks to net neutrality. Network neutrality will preserve the Internet architecture that has enabled the fast and innovative development of the Internet so far.	Traffic management is inevitable, and neutrality has never existed. Besides, there are already non-neutral leased services like VPNs (virtual private networks). Without network neutrality restrictions Internet companies can develop new services in which customers will be interested, with guaranteed QoS.
Economic argument	Without network neutrality, the Internet will look like cable TV: a handful of big companies will control access and distribution of content, deciding what users get to see and how much it costs them to see it. New entrants and small businesses will not have a chance to develop, especially those in developing countries. OTT service providers already pay loads to telecoms for their Internet connections, and invest in infrastructure like caching servers.	Without net neutrality restrictions in commercial agreements with content and service providers, telecoms operators will raise funds which would make them more interested in investing in better infrastructure. Better infrastructure will encourage new services and innovations, more tailored to customers' needs, bringing more revenue to all. OTT service provides will also find value in possible innovative services with QoS, enabled by the operators if not restricted by net neutrality provisions.
Ethical argument	The Internet is the result of developments by many volunteers over decades. They invested time and creativity in developing everything on the Internet from technical protocols to content. The Internet is more than a business – it has become a global heritage of mankind. It is not justifiable to have such a huge investment of time and creativity harvested by only a few companies who will lock the Internet in constrained business models by breaching network neutrality, and turn creativity of many into profit of a few.	Network neutrality is ethically questionable because operators have to invest in maintaining and expanding the Internet's infrastructure to support new services, while most benefits are reaped by Internet 'content' companies such as Google, Facebook, and Amazon.
Regulation argument	Network neutrality must be imposed by government to preserve the public interest. Any form of self-regulation will leave it open for operators to breach the principle of network neutrality. The open market is not a sufficient mechanism since major global telecoms are at the core of the Internet infrastructure. Even if there is a possibility to choose, this is not always realised since users need technical and legal literacy and awareness of the consequences of the various choices available.	The Internet has developed because of very light or no regulation. Heavy government regulation could stifle creativity and the future development of the Internet. The open market is based on choice, and users can always change their Internet provider if not satisfied with the offer. The users' choice and the market will kill bad offers and sustain good ones.

The basic principles

In recent years, policy debates and regulations on network neutrality have crystallised a few key principles for network neutrality:[50]

- Transparency: Operators must provide complete and accurate information on their network management practices, capacity, and the quality of their service to customers, in a form understandable by an average user.
- Access: Users should be able to have unrestricted] access to any [legal] content, service or application [with minimum quality of service guaranteed for the meaningful use, as prescribed by the regulator] or to connect any hardware that does not harm the network.
- (Non)discrimination: Operators should make no discrimination [or reasonable discrimination] of traffic based on:
    - o Origin of sender or receiver.
    - o Type of content, type of application and service [with fair competition – no discrimination against undesired competitors or OTT service providers' services].
    - o Where 'reasonable' could be any practice for public benefit (assuring quality of service, security and resilience of network, innovations and further investments, lowering costs, etc.) but not for business advantage only.

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

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

Policy approaches

With the network neutrality debate, another question has come to the fore: what is the role of the legislators and regulators in broadband policy and operator practices? One of the major challenges regulators face is whether to act preemptively (ex-ante), in order to prevent possible breaches of the network neutrality principle, or to respond based on precedents (ex-post) once (and if) the breach occurs. A challenge that legislators and policymakers face is whether the problem should be dealt with, with 'hard law' – encoding the principles into legislation – or if 'soft law' (guidelines and policies) would be sufficient.[51]

Developed countries

In response to the Comcast case, the US Federal Communications Commission (FCC) adopted the guidelines on network neutrality as an update to its 2005 policy paper,[52] which reflected the need for access to and choice of content and devices, and addressed the issues of discrimination and transparency. In the meantime, the FCC's decisions in support of net neutrality were overruled in early 2014 by the US appeals court on the basis of the FCC's limited mandate. It forced the FCC to consider allowing telecom providers some form of 'pay for preference' regimes or reclassify broadband as a public utility, thereby obtaining a mandate to enforce net neutrality. The EU regulatory framework on electronic communications targets protecting freedom of expression, users' choice, and access rights, along with the transparency principle; yet it also stresses the need for investment, fair competition with no discrimination, and opportunities for new business models including innovative business.[53] In 2014, the European Parliament adopted the Regulation on the Single Telecoms Market, with strong net neutrality provisions (including a rigorous definition and solid framework for 'specialised services').[54] Brazil,[55] Chile,[56] Slovenia, and the Netherlands protect net neutrality by national legislation.

Developing countries

Due to limited infrastructure and bandwidth, regulators of developing countries put more focus on fair usage policy – affordable prices and fair access for all. Some raise concerns over cross-border non-discrimination, saying that the traffic from all countries should be treated the same way with no preferences based on termination costs. Also, certain countries have more sensitivity to internal cultural, political, or ethical aspects, thereby understanding '(in)appropriate use' and management differently than others. Concerns have been raised that the innovative models of the developed world might hamper developing markets: by prioritising the services of big Internet companies, emerging business and competition would be additionally downsized, threatening innovation, local content and services, and media diversity. Few major formal policies or regulatory practices on network neutrality, however, have yet come from the developing world. Other positions may include copying the emerging US model and allowing national telecoms to charge global OTTs for priority, thereby adding to the income of incumbent telecoms; or, on the contrary, enforcing net neutrality on a national level in order to attract the OTTs to operate from outside the USA.

International organisations and NGOs

Many international organisations and user groups have also developed policy positions with regard to network neutrality. The Council of Europe (CoE), within its 2010 Declaration of the Committee of Ministers on network neutrality, emphasises the fundamental rights to freedom of expression and information;[57] the Internet Society (ISOC) promotes its user-centric approach which dominantly tackles the issues of access, choice, and transparency through the Open Inter-networking debate rather than the one on network neutrality.[58] The Trans Atlantic Consumer Dialogue (TACD), a forum of US and EU consumer organisations additionally emphasises requests for carrier non-discriminatory behaviour, calling on the USA and the EU to entitle regulators to act as safeguards of users' rights.[59] Network neutrality and a multi-tiered Internet were heavily discussed within the WCIT-12 process. The final NETmundial document in 2014 did not include net neutrality among the agreed principles, but has invited further discussions on the topic, especially by the IGF, during IGF 2014.

Many NGOs are especially concerned about the future of non-commercial and non-competing online content and services, requesting these to be broadcast through any carrier network equal to commercial ones. They also emphasise the rights of marginalised groups – especially people with disabilities – to use content, services, and applications (including those that demand high-bandwidth) for their needs without any limits whatsoever.

Open issues

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

- Where should the balance be between public good effects of the Internet and user (and human) rights on the one hand, and the rights of the providers to innovate within the networks they own on the other?
- Would an unregulated market with open competition, as advocated by the carriers, provide unlimited (or sufficient) choice for users? And would the users be able to make meaningful decisions?[60] Or should the regulators inevitably be empowered as safeguards, and if so, with what authority?
- How would different legal and regulatory approaches impact the broadband market and further investment and innovation?

- What are the implications of network (non)neutrality for the developing world?
- What are the implications of a tiered Internet for competition, innovation, investment, and human rights?
- Should zero rating tariffs or the development of CDNs be considered a 'tiered Internet'?
- Will the dominant OTT – both content and service providers – find a tiered Internet and possible new services a lucrative business model as well? In such case, will they be able to adapt it to include the users of developing countries, or will those be left out?
- Can telecom operators innovate their business models to grow their revenues without violating network neutrality (following successful examples of iTunes, Google, and other OTT service providers, and the potential for partnerships between OTT service providers and operators[61])?
- Will the need for traffic management for technical (quality) reasons be outdated in future, due to advancements in carrier technology?
- How will the growing dependence on clouds and the Internet of Things influence the debate on network neutrality, and vice versa?
- Should the debate be extended from traffic management on a carrier level to content and application management on content and application provider level, such as Google, Apple, or Facebook?
- Will consumer protection continue to be intrinsically linked to network neutrality?
- If network neutrality is 'defeated', what principles will support consumer protection in the future?

Web standards

By the late 1980s, the battle of 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 (the European Organization for Nuclear Research) in Geneva, consisting of a new standard for sharing information over the Internet, called HTML

(HyperText Markup Language, really just a simplification of an existing ISO standard called SGML– Standard Generalized Markup Language). Content displayed on the Internet first had to be organised according to HTML standards. HTML, as the basis of the World Wide Web, paved the way for the Internet's exponential growth.

Since its first version, HTML has been constantly upgraded with new features. The growing relevance of the Internet has put the question of the standardisation of HTML into focus. This was particularly relevant during the Browser Wars between Netscape and Microsoft, when each company tried to strengthen its market position by influencing HTML standards. While basic HTML only handled text and photos, newer 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 Markup 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 Markup Language (WML). Application standardisation is carried out mainly within the framework of the W3C, headed by Tim Berners-Lee. It is interesting to note that in spite of its high relevance to the Internet, so far, the W3C has not attracted much attention in the debate on Internet governance.

Cloud computing

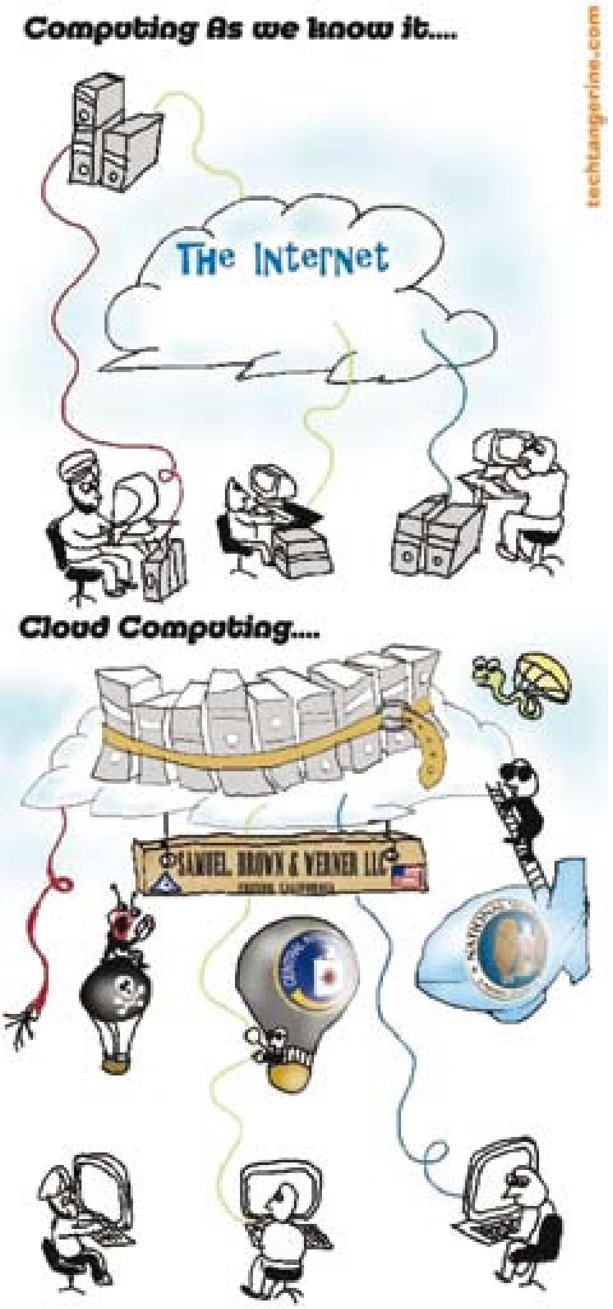
Cloud computing could be described as the shift of data from hard disks on our computers to servers in the clouds (i.e., huge server farms). The first wave of cloud computing started with the use of online mail servers (Gmail, Yahoo!), social media applications (Facebook, Twitter) and online applications (Wikis, blogs, Google docs). Apart from everyday applications, cloud computing is extensively used for business software. More and more of our digital assets are moving from our hard disks to the cloud. The main players in cloud computing are Google, Microsoft, Apple, Amazon, and Facebook, who either already have or plan to develop big server farms.

In the early days of computers, there were powerful mainframe computers and 'dumb' workstations. The power was in the centre. After that, for a long time, with PCs and Windows applications, computer power moved to the periphery. Will cloud computing close the circle? Are we going to have a few big central computers/server farms and billions of dumb units in the form of notebooks, monitors, and mobile phones? The answer to this and other questions will need time. Currently, we can identify a few Internet governance issues which are very likely to emerge in parallel with the development of cloud computing.

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

Internet governance of cloud computing is likely to emerge through the interplay of various actors and bodies. For example, the EU is concerned with privacy and data protection. The Safe Harbour agreement which was supposed to solve the problem of different privacy regimes in the USA and the EU does not work well. With more digital data crossing the Atlantic Ocean, the EU and the USA will have to address the question of protection of privacy according to EU regulation by US companies, the main operators in cloud computing. This issue came into sharper focus after the Snowden revelations of mass surveillance. When it comes to standards, it is very likely that the main companies will agree among themselves. Google has already started

Figure 9



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

Convergence: Internet telecommunication multimedia

Historically, telecommunication, broadcasting, and other related areas were separate industry segments; they used different technologies and were governed by different regulations. The broad and prevailing use of the Internet has aided in the convergence of technological platforms for telecommunication, broadcasting, and information delivery. Today, we can make telephone calls, watch TV, and share music on our computers via the Internet. Only a few years ago it was handled by different technological systems.

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

The issues

The economic implications of convergence

At the economic level, convergence has started to reshape traditional markets by putting companies that previously operated in separate domains, into direct competition. Companies use different strategies. The most frequent approach is merger and acquisition.

The need for a legal framework

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

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

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

The risk of convergence: the merger of cable operators and ISPs

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

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

The main difference between ADSL and cable is that cable is not regulated by so-called common carrier rules which apply to the telephony system and 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 (LANs), 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.'[62]

This convergence problem may be addressed by deciding if the cable Internet is an 'information service' or a 'telecommunication service'. If it is the latter, it will have to be regulated through common carrier rules.

Cybersecurity

The current situation

The Internet was originally designed for use by a closed circle mainly of academics. Communication was open. Security was not a concern.

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

Cybersecurity issues can be classified according to three criteria:

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

The cybersecurity framework includes policy principles, instruments, and institutions dealing with cybersecurity. It is an umbrella concept covering several areas:

- Critical information infrastructure protection (CIIP) is ever more important because the global critical infrastructure now depends on the Internet. Many vital parts of global society – including energy, water, and finance – are heavily dependent on the Internet and other computer networks as an information infrastructure. This includes not only the equipment and links, but also the protocols, data centres, and the critical Internet resources (CIR). The vulnerability of the Internet is the vulnerability of modern society.
- Cybercrime is crime committed via the Internet and computer systems. It includes old, i.e., traditional, crimes now conducted through cyberspace (like various frauds), crimes that have evolved due to technology (e.g. credit card frauds and child abuse), new crimes that have emerged with the Internet (e.g. denial-of-service attacks and pay-per-click frauds), and cybercrime tools which are used to facilitate other crimes (e.g. botnets). Combating child pornography is the most developed area of international cooperation; this cooperation is missing, however, in dismantling global

cybercrime black markets which offer outsourced criminal services and easy-to-use digital weapons (e.g. viruses and botnets) to almost anyone.

- Cyberconflicts, often labelled as cyberwar, have high media visibility and still low policy and legal reflections. Cyberconflicts can be dissected in three main areas: conduct of cyberconflicts (i.e., can the existing law, mainly The Hague Conventions, be applied to cyberspace; if not, what type of new legal instruments should be developed?); weapons and disarmament (i.e., how to introduce cyberweapons into the disarmament process); and humanitarian law (i.e., how to apply the Geneva Conventions to cyberconflicts).

Cybersecurity, as a policy space, is in its formative phase, with the ensuing conceptual and terminological confusion. Other terms are also in general discussion without the necessary policy precision: cyber-riots, cyberterrorism, cybersabotage, etc. Cyberterrorism, particularly, came into sharper focus after 9/11, when an increasing number of cyberterrorist attacks were reported. Cyberterrorists use similar tools to cybercriminals, but for a different end. While cybercriminals are motivated mainly by financial gain, cyberterrorists aim to cause major public disruption and chaos.

Cybersecurity policy initiatives

Many national, regional, and global initiatives focus on cybersecurity. At national level, a growing volume of legislation and jurisprudence deals with cybersecurity, with a focus on combating cybercrime, and more and more the protection of critical information infrastructure from sabotage and attacks as a result of terrorism or conflicts. It is difficult to find a developed country without some initiative focusing on cybersecurity.

At international level, the ITU is the most active organisation; it has produced a large number of security frameworks, architectures, and standards, including X.509, which provides the basis for the public key infrastructure (PKI), used, for example, in the secure version of HTTP(S) (HyperText Transfer Protocol (Secure)). The ITU moved beyond strictly technical aspects and launched the Global Cybersecurity Agenda.[63] This initiative encompasses legal measures, policy cooperation, and capacity building. Furthermore, at WCIT-12, new articles on security and robustness of networks and on unsolicited bulk electronic communications (usually referred to as spam) were added to the ITRs.[64]

The Commonwealth Cybercrime Initiative (CCI) was given its mandate from Heads of government of the Commonwealth in 2011 to improve legislation and the capacity of member states to tackle cyber crime.[65] Dozens of partners involved with CCI assist interested countries with providing scoping missions, capacity building programmes, and model law outlines in the fields of cybercrime and cybersecurity in general.

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

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

A major international legal instrument related to cybersecurity is the Council of Europe's Convention on Cybercrime,[66] which entered into force on 1 July 2004. Some countries have established bilateral arrangements. The USA has bilateral agreements on legal cooperation in criminal matters with more than 20 other countries (Mutual Legal Assistance in Criminal Matters Treaties (MLATs)). These agreements also apply in cybercrime cases.

Cyberconflict remains an area with the least advances in terms of policy developments. At the same time, an increasing number of states appear to be developing their own cybertools for warfare and intelligence, as was presented by the UN report of 2010.[67] In 2013, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), prepared the Tallinn Manual elaborating on the implementation of the existing international humanitarian law on entering and conducting a war (*jus ad bellum* and *jus in bello*) in cyberspace.[68]

One attempt by academics and non-state actors to draft an international agreement is that of the Stanford Draft Convention on Protection from Cyber Crime and Terrorism.[69] This draft recommends the establishment of an international body, named the Agency for Information Infrastructure Protection (AIIP).

The issues

Influence of Internet architecture on cybersecurity

The very nature of the Internet organisation affects its security. Should we continue with the current approach of building security on a pre-existing non-secure foundation or modify the basis of the Internet's infrastructure? How would such a change affect other features of the Internet, especially its openness and its transparency? Most of the past development of Internet standards aimed at improving performance or introducing new applications. Security was not a priority. It is unclear whether the IETF will be able to change e-mail standards to provide proper authentication and, ultimately, reduce the misuse of the Internet (e.g. spam, cybercrime). Given the controversy surrounding any changes to basic Internet standards, it is likely that security-related improvements in the basic Internet protocol will be gradual and slow. Yet decisive steps are starting to be implemented in this direction; the Domain Name System Security Extensions (DNSSEC)[70] is a good illustrative example. Following almost 12 years of research, trials, and debates within the technical community, DNSSEC first started to be deployed for some ccTLDs and from 2010 it was also implemented at the root server level. However, further challenges reside in the large-scale adoption of this new security standard down the ladder by the domain name registrars, ISPs, and website owners.[71]

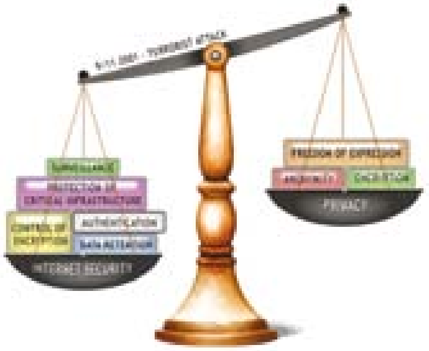
Figure 10

Important improvements to security, however, can be achieved through the proper configuration of the main Internet nodes such as the DNS servers around the world. Many incidents, such as the 2013 private cyberwar between two companies – CyberBunker and Spamhaus – that resulted in temporary congestion of large portions of the global Internet, are possible because of several dozens of millions of misconfigured DNS servers around the world known as open resolvers.[72] Besides, introducing security-by-design into all new technologies – software, hardware, and protocols – would bring additional security layers.

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

Cybersecurity is often mentioned as one of the preconditions for the rapid growth of e-commerce. Without a secure and reliable Internet, customers will be reluctant to provide confidential information online, such as credit card numbers. The same applies to online banking and the use of electronic money. Increasing numbers of successful attacks on companies' servers for acquiring customers' personal data and credit card numbers are evident, such as the collection of over 1.2 billion user-name-and-password combinations and half a billion e-mail addresses stolen in 2014 by one Russian gang.[73] These undermine user trust in online services. If general cybersecurity only slowly improves (and with an accompanying lack of standards), it is likely that the business sector will push for faster developments in cybersecurity. This may lead to further challenges for the principle of net neutrality and the development of 'a new Internet', which would facilitate, among other things, more secure Internet communication.

Figure 11



Surveillance and espionage

The 2013 revelations by the NSA employee Edward Snowden have again confirmed that states – the USA included – exploit the vulnerabilities of the Internet for their own interests. The NSA's PRISM project based its surveillance capabilities on the ability to access the cables, routers, and cloud servers of major Internet companies (US-based telecoms, service, and content providers). In response, other countries – especially EU and BRICS – have started considering mitigation tactics, including laying their own intercontinental submarine cable connections to avoid passing through US nodes,[74] requiring Internet companies to store personal data of their citizens on data centres within their jurisdictions, and encouraging the development of local services and content.

In 2013, the US-based security company Mandiant released a report about a cyber-espionage campaign against US companies conducted by China.[75] After the USA charged five Chinese 'military hackers', China in turn accused the USA of cyber-espionage, which resulted with the suspension of the activities of the China-US Cyber Working Group.[76]

The increasing militarisation of cyberspace through the use of exploits and hacking tools by states leads to increasing political tension. Such tension may accelerate the need for global efforts to prevent the proliferation of cyber-arms.

Cybersecurity and human rights

The link between cybersecurity and human rights is highly relevant for the future of the Internet. So far, these two fields are being addressed separately in their respective silos. However, recent experiences (SOPA, ACTA, PRISM/NSA) show that the protection of human rights (privacy, freedom of expression, access) is not only a value-based priority, it is also a very practical tool for ensuring that the Internet remains open and secure. Human rights are a matter of cyber realpolitik.

Individual Internet users are the pillars of cybersecurity. Yet they are often the 'weakest link' when it comes to protection from cyber-attacks. Our personal computers are used to stage cyber-attacks (as part of botnets) and spread viruses and malware. Unprotected access to our computers and mobile devices offers a backdoor for access to the datasets of our companies or institutions, and compromises many more computers.

Concerns of the end users, however, are usually not about possible greater damage (often due to ignorance) as a result of their compromised computer, but rather about the protection of their own data, and thus integrity and privacy and rights in general. Post-PRISM discussions emphasise making personal computers more 'surveillance-safe', including how to employ encryption, regular patches and updates, IPSec and VPN protocols[77] – awareness measures that would, in fact, also prevent unprotected access and contribute to better general cybersecurity.

Global cybersecurity – built around the important role of individual Internet users – has human rights as one of its cornerstones. The recognition of this link has already started emerging in policy documents. The EU's cybersecurity strategy, for instance, considers preserving an open, free, and secure cyberspace – including support for the promotion and protection of fundamental rights – as one of its five strategy pillars.[78]

The main challenge will be to overcome the post-9/11 dominant view of win/lose: more security implies fewer human rights and vice versa. Yet there are many win/win areas in empowering and protecting individuals as pillars of the cybersecurity system (access to information, privacy protection), which should be given priority.

Encryption

Today, encryption refers to the scrambling of electronic documents and communication into an unreadable format which can be read only through the use of encryption software. Traditionally, governments were the only players who had the power and the know-how to develop and deploy powerful encryption in their military and diplomatic communications. With packages such as Pretty Good Privacy, encryption has become affordable for any Internet users, including criminals and terrorists. It has triggered many governance issues related to finding the right balance between the need to respect privacy of communication of Internet users and the need for governments to monitor some types of communication of relevance for the national security (potential criminal and terrorist activity remains an issue).

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

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

International regimes for encryption tools

Encryption has been tackled in two contexts: the Wassenaar Arrangement and the OECD. The Wassenaar Arrangement is an international regime adopted by 41 countries to restrict the export of conventional weapons and 'dual use' technologies to countries at war or considered to be 'pariah states'.[79] The arrangement established a secretariat in Vienna. US lobbying, with the Wassenaar Group, aimed at extending the Clipper Approach[80] internationally, by controlling encryption software through a key escrow. This was resisted by many countries, especially Japan and the Scandinavian countries.

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

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

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

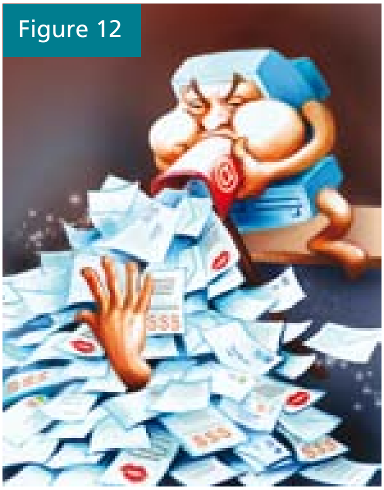
Spam

The current situation

Spam is usually defined as unsolicited e-mail, which is sent to a wide number of Internet users. Spam is mainly used for commercial promotion. Its other uses include social activism, political campaigning, and the distribution of pornographic materials. Spam is classified in the infrastructure basket because it affects the normal functioning of the Internet by impeding one of the Internet's core applications, e-mail. It is one of the Internet governance issues that affect almost everyone who connects to the Internet. According to statistics from 2014, 66% of e-mail traffic is spam.[81]Besides the fact that it is annoying, spam also causes considerable economic loss, both in terms of bandwidth used and lost time spent checking/deleting it.

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

Figure 12



On the legal side, many states have reacted by introducing new anti-spam laws. In the USA, the Can-Spam Law involves a delicate balance between allowing e-mail-based promotion and preventing spam.[82] Although the law prescribes severe penalties 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).

In July 2003, the EU introduced its own anti-spam law as part of its directive on privacy and electronic communications. The EU law encourages self-regulation and private sector initiatives that would lead towards a reduction in spam.[83]

Spam and 'policy fashion'

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

Since 2005, the volume of spam has tripled, according to conservative estimates (2005: 30 billion messages per day; 2008: 100 billion messages per day; 2010: 200 billion messages per day). The policy relevance of spam does not follow this trend. Spam now has a very low visibility in global policy processes.

In November 2006, the European Commission adopted its Communication on Fighting Spam, Spyware and Malicious Software. The Communication identifies a number of actions to promote the implementation and enforcement of the existing legislation outlined above, as the lack of enforcement is seen as the main problem.

The international response

Both of the anti-spam laws adopted in the USA and the EU have one weakness: a lack of provision for preventing cross-border spam. The Canadian Industry Minister, Lucienne Robillard, stated that the problem cannot be solved on a 'country by country' basis.[84] A similar conclusion was reached in a 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.'[85] A global solution is required, implemented through an international treaty or some similar mechanism.

An MoU signed by Australia, Korea, and the UK is one of the first examples of international cooperation in the anti-spam campaign.

The OECD established a task force on spam and prepared an anti-spam toolkit. The ITU was also proactive by organising the Thematic Meeting on Countering Spam (2004) to consider various possibilities of establishing a global Memorandum of Understanding on Combating Spam.[86] At regional level, the EU established the Network of Anti-Spam Enforcement Agencies, and APEC prepared a set of consumer guidelines.

Another possible anti-spam approach was undertaken by the leading Internet companies that host e-mail accounts: America Online, British Telecom, Comcast, EarthLink, Microsoft, and Yahoo! They established in 2003 the

Anti-Spam Technical Alliance (ASTA) with the main task of coordinating technical and policy-related anti-spam activities.

The issues

Different definitions of spam

Different understandings of spam affect the anti-spam campaign. In the USA, a general concern about the protection of the freedom of speech and the First Amendment 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 USA, this difference in definitions seriously limits any possibility of introducing an effective international anti-spam mechanism.

Spam and e-mail authentication

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

The need for global action

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

Endnotes

[1] The terms Internet and www are sometimes used interchangeably; however, there is a difference. The Internet is a network of networks connected by TCP/IP. Sometimes, the term Internet is used to encompass everything, including infrastructure, applications (e-mail, ftp, Web) and content. The www is just one of many Internet applications, a system of interlinked documents connected with the help of the HyperText Transfer Protocol (HTTP).

[2] Following a policy of technological neutrality, the European Union has been using the term 'electronic communications' instead of 'telecommunications'. This covers, for example, Internet traffic over the electronic grid, which is not part of the telecommunications infrastructure.

[3] Internet transfer via an electric grid is called Power Line Communication (PLC). The use of the power grid would make the Internet more accessible to many users. For a technical and organisational review of this facility, please consult: Palet J (2003) *Addressing the Digital Divide with IPv6-enabled Broadband Power Line Communication,* Internet Society, ISOC Member Briefing No. 13. Available at **http://www.isoc.org/briefings/013** [accessed 13 February 2014].

[4] The liberalisation of telecommunication markets of WTO members was formalised in 1998 in the so-called Basic Telecommunication Agreement (BTA). Following the adoption of BTA, more than 100 countries began the liberalisation process, characterised by the privatisation of national telecommunication monopolies, the introduction of competition, and the establishment of national regulators. The agreement is formally called *The Fourth Protocol to the General Agreement on Trade in Services* (adopted on 30 April 1996 and entering into force on 5 February 1998). Available at **http://www.wto.org/english/tratop_e/serv_e/4prote_e.htm** [accessed 13 February 2014].

[5] ITU (no date) Signatories of the Final Acts – WCIT-12. Available at **http://www.itu.int/osg/wcit-12/highlights/signatories.html** [accessed 11 August 2014].

[6] One of the controversies surrounding WSIS was the ITU's intention to become more involved in the Internet governance process, especially within a domain handled by ICANN. For more information about ITU's Internet policy, please consult **http://www.itu.int/osg/csd/intgov/** [accessed 13 February 2014].

[7] For more information about the WTO's role in the field of telecommunications, consult **http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm** [accessed 13 February 2014].

[8] Latvia and Moldova are good examples of how it is possible to make a quantum leap forward in the quick development of a telecommunications infrastructure through the introduction of wireless communication; check **http://www.isoc.org/isoc/conferences/inet/99/proceedings/4d/4d_2.htm** [accessed 13 February 2014].

[9] Nothias J-C (2012) The hypocrisy threatening the future of the Internet. *The Global Journal.* Available at **http://theglobaljournal.net/article/view/904/** [accessed 10 August 2014].

[10] Initially the Wi-Fi Alliance was called the Wireless Ethernet Compatibility Alliance (WECA). It received its current name in 2002. It was established by some of the leading developers of telecom equipment including: 3Com, Cisco, Intersil, Agere, and Nokia.

[11] It is estimated that this investment totals approximately €109 billion, according to *The Economist* (2003) Beyond the Bubble Survey: Telecoms. Available at **http://www.economist.com/node/2098913** [accessed 13 February 2014].

[12] For more information about the EU radio spectrum policy see **http://ec.europa.eu/digital-agenda/en/what-radio-spectrum-policy** [accessed 13 February 2014].

[13] The current RIRs are: ARIN (the American Registry for Internet Numbers), APNIC (the Asia Pacific Network Information Centre), LACNIC (the Latin American and Caribbean IP Address Regional Registry), RIPE NCC (Reseaux IP Européens Network Coordination Centre – covering Europe and the Middle East) and AFRINIC (the African Network Information Centre). A detailed explanation of the RIR system is available at **http://www.ripe.net/internet-coordination/internet-governance/internet-technical-community/the-rir-system** [accessed 13 February 2014].

[14] For a detailed discussion on IPv6, please consult the research project: *IP Allocation and IPv6* by Jean Philémon Kissangou, Marsha Guthrie, and Mwende Njiraini, part of the 2005 Internet Governance Capacity Building Programme. Available at **http://archive1.diplomacy.edu/poolbin.asp?IDPool=130** [accessed 13 February 2014].

[15] For a comprehensive and highly technical survey of TCP/IP Security, please consult: Chambers C, Dolske J and Iyer J., *TCP/IP Security*, Department of Computer and Information Science, Ohio State University. Available at **http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html** [accessed13 February 2014].

[16] One of the few referential documents on the domain name system (DNS) is RFC 1591 (March 1994), which specifies the governance structure of DNS. Available at **http://www.ietf.org/rfc/rfc1591.txt** [accessed 13 February 2014].

[17] An overview of the gTLDs with a link to the list of all the TLDs is available at **http://www.icann.org/en/resources/registries/about** [accessed 13 February 2014].

[18] The text of proposal is available at **http://archive.icann.org/en/tlds/stld-apps-19mar04/xxx.htm**; the retrospective of the .XXX application, within the minutes of the meeting of 30 March 2007 when it was rejected by the ICANN Board, is available at **http://www.icann.org/en/groups/board/documents/resolutions-30mar07-en.htm#_blank** [accessed 13 February 2014].

[19] The US government did not use an ICANN procedure. It used its *de facto* authority via a letter sent by the US Department of Commerce to the Chairman of ICANN.

[20] The application form for the registration of the .cat domain: **http://archive.icann.org/en/tlds/stld-apps-19mar04/cat.htm** [accessed 13 February 2014].

[21] Summary report ICANN 50. Geneva Internet Platform. Available at **http://www.giplatform.org/resources/gip-summary-report-icann-50** [accessed 9 August 2014].

[22] The ITU's website contains a comprehensive bibliography of materials related to Country Domain Management; most materials were delivered at the ITU Workshop on Country Domain Management held in Kuala Lumpur. Available at **http://www.itu.int/ITU-T/worksem/cctld/kualalumpur0704/contributions/index.html** [accessed 13 February 2014].

[23] The IANA Report on the county code top-level domain for Palestine is available at **http://www.iana.org/reports/ps-report-22mar00.htm** [accessed 13 February 2014].

[24] 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 nongovernmental to governmental control is often cited as an example of an unsuccessful transition. The government reduced the quality of services and introduced higher fees, which have made the registration of Cambodian domains much more difficult. For more information, please consult: Alfonso C (2004) BR: CCTLD An asset of the commons, in MacLean D (ed) *Internet Governance: A Grand Collaboration.* New York: UN ICT Task Force, pp. 291-299; Klien N (2004) Internet Governance: Perspectives from Cambodia in MacLean D (ed) *Internet Governance: A Grand Collaboration.* New York: UN ICT Task Force, pp. 227-237. Excerpts available at **http://books.google.ro/books?id=pEFAypES4t0C&printsec=frontcover&hl=ro#v=onepage&q&f=false** [accessed 13 February 2014].

[25] ICANN (2005) Principles for the Delegation and Administration of Country Code Top-Level Domains. Available at **http://archive.icann.org/en/committees/gac/gac-cctldprinciples-23feb00.htm** [accessed 13 February 2014].

[26] The list of root zone servers, their nodes and positions, and managing organisations is available at **http://www.root-servers.org/** [accessed 13 February 2014].

[27] ISC Inc. (2003) Hierarchical Anycast for Global Distribution. Available at **http://ftp.isc.org/isc/pubs/tn/isc-tn-2003-1.html** [accessed 13 February 2014].

[28] IANA root servers. Available at **http://www.iana.org/domains/root/servers** [accessed 9 August 2014].

[29] The root zone file is publicly available at **http://www.iana.org/domains/root/files** [accessed 9 August 2014].

[30] NTIA (2014) NTIA announces intent to transition key Internet domain names functions. Available at **http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions**[accessed 9 August 2014].

[31] US officials counter that the Internet is too valuable to tinker with or place under an international body like the UN: 'What's at risk is the bureaucratisation of the Internet and innovation', said Michael Gallagher, the Department of Commerce official who administered the government's tie to ICANN. Mr Gallagher and other backers of ICANN also pointed out that the countries loudest in demanding more international input – China, Libya, Syria, Cuba – have non-democratic governments. Allowing these nations to influence how the Internet works could hinder the freedom of speech, they said. (Source: Rhoads C (2006) Endangered Domain: In Threat to Internet's Clout, Some Are Starting Alternatives. *The Wall Street Journal,* 19 January 2006; p. A1).

[32] Bertola V (no date) Oversight and multiple root server systems. Available at **http://wgig.org/docs/book/Vittorio_Bertola.html** [accessed 13 February 2014].

[33] 'The Court of Appeal of The Hague ruled against the Church of Scientology in its copyright infringement suit against a Dutch writer and her ISP, XS4ALL. The writer, formerly a practicing Scientologist, posted to a website parts of confidential church documents, and the church sued under the Dutch Copyright Act of 1912. In 1999, the District Court ruled in favour of the defendants, citing freedom of speech concerns. However, that court also ruled that ISPs should be held liable for posted materials that might violate existing copyrights. The Court of Appeal affirmed the first ruling, but reversed the second, holding that ISPs were not liable for posted materials.' For more information consult Gelman L (2003) Church of Scientology Loses Copyright Infringement Case in Dutch Court. Available at **http://cyberlaw.stanford.edu/packets001638.shtml** [accessed 13 February 2014].

[34] For more information on this case see Electronic Privacy Information Center (2004) RIAA *vs* Verizon. Available at **http://epic.org/privacy/copyright/verizon/** [accessed 13 February 2014].

[35] The Supreme Court of Canada rejected the argument of the Society of Composers, Authors and Music Publishers of Canada that Canadian ISPs should pay royalties because some of their customers download copyrighted works (SOCAN *vs* CAIP). More information available at **http://www.canlii.org/en/ca/scc/doc/2004/2004scc45/2004scc45.html** [accessed 13 February 2014].

[36] 'SABAM (the Belgian collective society – *Société belge des auteurs, compositeurs et éditeurs*) wanted the ISP Scarlet to install a generalised filtering system for all incoming and outgoing electronic communications passing through its services and to block potentially unlawful communications. In First Instance, while refusing the liability of the ISP, the Brussels Court concluded that the SABAM's claim was legitimate and that a filtering system had to be deployed. Scarlet appealed and the case was referred to the Court of Justice of the European Union. In its decision, the Court of Justice ruled that a filtering and blocking system for all its customers for an unlimited period, *in abstracto* and as preventive measure, violates fundamental rights, more particularly the right to privacy, freedom of communication and freedom of information. In addition, it breaches the freedom of ISPs to conduct business.' For more information, see *Scarlet v SABAM: a win for fundamental rights and Internet freedoms* EDRi-gram newsletter No. 9.23, 30 November 2011. Available at **http://edri.org/edrigramnumber9-23scarlet-sabam-win-fundamental-rights** [accessed 15 March 2014].

[37] Williams F (2006) ISPs should be liable for spam, says UN report, *Financial Times*. Available at **http://www.ft.com/intl/cms/s/09b837c0-ae02-11da-8ffb-0000779e2340,Authorised=false.html?_i_location=http%3A%2F%2Fwww.ft.com%2Fcms%2Fs%2F0%2F09b837c0-ae02-11da-8ffb-0000779e2340.html%3Fsiteedition%3Dintl&siteedition=intl&_i_referer=#axzz1l2VhnlN0** [accessed 13 February 2014].

[38] Shannon V (2006) The end user: Junk payout in spam case – Technology – *International Herald Tribune*. Available at **http://www.nytimes.com/2006/04/12/technology/12iht-PTEND13.1523942.html** [accessed 13 February 2014].

[39] In computer networking, peering is a voluntary interconnection of administratively separate Internet networks for the purpose of exchanging traffic between the customers of each network. The pure definition of peering is settlement-free or 'sender keeps all', meaning that neither party pays the other for the exchanged traffic; instead, each derives revenue from its own customers. Peering requires physical interconnection of the networks, an exchange of

routing information through the Border Gateway Protocol (BGP) routing protocol and is often accompanied by peering agreements of varying formality, from 'handshake' to thick contracts. (Source: Wikipedia).

[40] Tier 2 Internet Bandwidth Providers are usually called ICP (Internet connection points) or Internet gateways.

[41] Two related cases were mentioned in Spaink K (2002) *Freedom of the Internet, our new challenge*. Available at **http://www.spaink.net/english/osce_internetfreedom.html** [accessed 13 February 2014]. 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 Flashback's ISP, Air2Net, and the main backbone operator MCI/WorldCom. Under pressure from this campaign, MCI/WorldCom decided to disconnect Flashback in spite of a lack of any legal basis for doing so. Flashback'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. A small Dutch ISP provider, Xtended Internet, was disconnected by its US-based upstream provider under pressure from the Scientology lobby.

[42] Signal transmission technologies – both for wireless (like LTE) and optical cables (like DWDM) – promise to solve the 'bandwidth exhaustion' problem with much greater bandwidth specifications (up to terabits per second). The demand-supply run, however, is perpetual.

[43] Cisco (no date) The Internet of Things. Available at **http://www.cisco.com/web/solutions/trends/iot/overview.html** [accessed 10 August 2014].

[44] *The Economist* (2009) America insists on net neutrality: The rights of bits. 24 September. Available at **http://www.economist.com/node/14517422** [accessed 13 February 2014].

[45] Full text of a Verizon and Google Legislative Framework Proposal for an Open Internet is available at **http://www.google.com/googleblogs/pdfs/verizon_google_legislative_framework_proposal_081010.pdf** [accessed 13 February 2014].

[46] McMillan R (2014) What everyone gets wrong in the debate over net neutrality. Available at **http://www.wired.com/2014/06/net_neutrality_missing/** [accessed 10 August 2014].

[47] The bandwidth (bit rate) agreed to in a contract with the ISP is, in fact, only the maximum available rather than a guaranteed effective speed.

[48] Ogg E (2010) *Report: Google, Verizon reach Net neutrality deal*. Available at **http://news.cnet.com/8301-31021_3-20012703-260.html?tag=mncol;mlt_related** [accessed 13 February 2014].

[49] McCullagh D (2012) *European ISPs defend U.N. Internet tax*. Available at **http://news.cnet.com/8301-13578_3-57496581-38/european-isps-defend-u.n-internet-tax/** [accessed 13 February 2014].

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

[51] Radunovic V (2012) Network Neutrality in law – a step forwards or a step backwards? Diplo Blog. Available at **http://www.diplomacy.edu/blog/network-neutrality-law-%E2%80%93-step-forwards-or-step-backwards** [accessed 13 February 2014].

[52] FCC (2005) Policy statement. Available at **http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf** [accessed 13 February 2014].

[53] Kroes N (2010) *Net neutrality in Europe*. Speech given by Vice President of the European Commission Commissioner for the Digital Agenda. Available at **http://europa.eu/rapid/press-release_SPEECH-10-153_en.htm?locale=en** [accessed 13 February 2014].

[54] La Quadrature du Net (2014) Net neutrality: a great step forward for the free Internet. Available at **http://www.laquadrature.net/en/net-neutrality-a-great-step-forward-for-the-free-internet** [accessed 11 August 2014].

[55] English version of the Brazilian *Marco Civil* is available at **http://giplatform.org/resources/text-brazils-new-marco-civil** [accessed 10 August 2014].

[56] TechnoLlama (2012) Chile enforces net neutrality for the first time, sort of. Available at **http://www.technollama.co.uk/chile-enforces-net-neutrality-for-the-first-time-sort-of** [accessed 13 February 2014].

[57] Integral text of the 2010 Declaration of the Committee of Ministers on network neutrality of Council of Europe is available at **https://wcd.coe.int/ViewDoc.jsp?id=1678287** [accessed 13 February 2014].

[58] ISOC considers the concept of network neutrality as rather ill-defined, and instead discusses the continued open inter-networking. Available at **http://www.internetsociety.org/articles/internet-society-publishes-statement-open-inter-networking** [accessed 13 February 2014]. Its 16 May 2010 Public consultation on Net Neutrality states: *Rather than focusing simply on the range of possible Network Neutrality definitions, the Internet Society believes it is more appropriate to concentrate more broadly on the imperative of preserving the open, user-centric Internet model that has been so successful to date.*

[59] TACD (no date) TACD calls for Net Neutrality. Available at **http://tacd.org/?option=com_content&task=view&id=162&Itemid=43** [accessed 13 February 2014].

[60] Radunovic V (2012) Can free choice hurt open Internet markets? Diplo Blog. Available at **http://www.diplomacy.edu/blog/can-free-choice-hurt-open-internet-markets** [accessed 13 February 2014].

[61] Chetan Sharma lists some interesting opportunities for cooperation between OTT and mobile operators, like analysing real-time network conditions, sharing user behaviour info, location and presence (within limits of privacy regulations), or third-party services billing through mobile subscription. Available at **http://synergy.syniverse.com/2012/05/mobile-operators-and-otts-building-a-win-win-partnership/** [accessed 13 February 2014].

[62] ACLU White Paper (2005) No competition: How monopoly control of the broadband Internet threatens free speech. ACLU: New York, NY, USA. Available at **https://www.aclu.org/technology-and-liberty/monopoly-control-broadband-internet-threatens-free-speech** [accessed 13 February 2014].

[63] Global Cybersecurity Agenda (no date). Available at **http://www.itu.int/osg/csd/cybersecurity/gca/** [accessed 13 February 2014].

[64] ITU (2012) WCIT-12 Final Acts. Available at **http://www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf** [accessed 10 August 2014].

[65] CCI (no date) Commonwealth Cybercrime Initiative. Available at **http://www.commonwealthcybercrimeinitiative.org/** [accessed 11 August 2014].

[66] Council of Europe (2001) Convention on Cybercrime. Available at **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm** [accessed 13 February 2014].

[67] UN report A/65/201 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Available at **http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf** [accessed 10 August 2014].

[68] CCDCOE (2013) *The Tallinn Manual.* Available at **http://www.ccdcoe.org/tallinn-manual.html** [accessed 10 August 2014].

[69] Sofaer AD *et al.* (2000) Proposal for an international convention on cybercrime. Available at **http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm** [accessed 13 February 2014].

[70] DNSSEC explained. Available at **http://everything.explained.at/DNSSEC/** [accessed 13 February 2014].

[71] For an overview of current status and challenges in DNSSEC deployment see Marsan C (2012) Will 2012 be the dawn of DNSSEC? 18 January 2012 Networkworld. Available at **http://www.networkworld.com/news/2012/011812-dnssec-outlook-255033.html** [accessed 13 February 2014].

[72] Radunovic V (2013) Waging a (private) cyber war. Available at **http://www.diplomacy.edu/blog/waging-private-cyberwar** [accessed 10 August 2014].

[73] Perlroth N and Gellese D (2014) Russian gang said to amass more than a billion stolen Internet credentials. *New York Times.* Available at **http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0** [accessed 10 August 2014].

[74] Brazil and the EU have pushed forward their dialogue on developing a direct submarine link. Available at **http://rt.com/news/brazil-eu-cable-spying-504/** [accessed 10 August 2014].

[75] Keck Z (2014) China expands cyber spying. Available at **http://thediplomat.com/2014/04/china-expands-cyber-spying/** [accessed 10 August 2014].

[76] Ranger S (2014) We're the real hacking victims, says China. Available at **http://www.zdnet.com/were-the-real-hacking-victims-says-china-7000029666/** [accessed 10 August 2014].

[77] Schneier B (2013) NSA surveillance: A guide to staying secure. Available at **www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance** [accessed 12 August 2014].

[78] EU Commission (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Available at **http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security** [accessed 12 August 2014].

[79] The Wassenaar Arrangement. Available at **http://www.wassenaar.org/** [accessed 13 February 2014].

[80] The Clipper approach was proposed by the US government back in 1993. At its core was the use of a Clipper chip which was supposed to be used in all telephones and other voice communication tools. The Clipper chip had a 'back door' which could be used by governments for lawful surveillance. After strong opposition from human rights activists and the general public, the US government dropped this proposal in 1995. See: Denning D (1995) The case for clipper. *MIT Technology Review.* MIT: Cambridge, MA, USA. Available at **http://encryption_policies.tripod.com/us/denning_0795_clipper.htm** [accessed 13 February 2014].

[81] Spam stops here (2014) Global Spam Threat Report. Available at **http://www.spamstopshere.com/global-report/spam-threats-february-2014.php** [accessed 11 August 2014].

[82] More references to Can-Spam are available at the Bureau of Consumer Protection (2009). *The CAN-SPAM Act: A Compliance Guide for Business.* Available at **http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business** [accessed 13 February 2014].

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

[84] As quoted in Johnsson O (2007) Methods to combat SPAM. Available at **http://home.swipnet.se/Johnson_Consulting/images/spam1.htm** [accessed 13 February 2014].

[85] *BBC NEWS* (2004) European anti-spam laws lack bite. 28 April. Available at **http://news.bbc.co.uk/2/hi/technology/3666585.stm** [accessed 13 February 2014].

[86] For more information about ITU activities related to combating spam see ITU (no date) ITU Activities on Countering Spam. Available at **http://www.itu.int/osg/spu/spam/** [accessed 13 February 2014].

Section 3

The legal basket

The legal basket

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

1. A real-law approach, where the Internet is essentially treated no differently from previous telecommunication technologies, in the long evolution from smoke signals to the telephone. Through faster and more comprehensive communication, the Internet introduces quantitative but not qualitative changes in modern society. Consequently, any existing legal rules can also be applied to the Internet.[1]
2. A cyberlaw approach, based on the presumption that the Internet introduces new types of social relationships in cyberspace. Consequently, there is a need to formulate new cyberlaws in order to regulate cyberspace. One argument for this approach is that the sheer speed and volume of Internet-facilitated cross-border communication hinders the enforcement of existing legal rules.

The real-law approach is gaining predominance. A considerable part of existing legislation can be applied to the Internet. For some issues – such as cybercrime – real laws would have to be adapted in order to be applicable to the cyber world.

Legal instruments

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

Note

A frequent argument for a new regulation for cyberspace is that traditional regulation (e.g. crime, taxation) is not efficient enough. It is important to keep in mind that laws do not make prohibited behaviour impossible, only punishable.

National and community legal instruments

Legislation

Legislative activities have progressively intensified in the field of the Internet. This is especially the case within EU and OECD countries, where the Internet is widely used and has a high degree of impact on economic and social relations. To date, the priority areas for Internet legislation 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 societal change. This is particularly noticeable in this day and age, when technological development reshapes social reality much faster than legislators can follow. Sometimes, rules become obsolete even before they come into force. The risk of legal obsolescence is an important consideration in Internet regulation.

Social norms (customs)

Like legislation, social norms proscribe certain behaviour. Unlike legislation, no state power enforces those norms. They are enforced by the community through peer-to-peer pressure. In the early days of the Internet, its use was ruled by a set of social norms labelled 'netiquette', where peer pressure and exclusion were the main sanctions. During this period in which the Internet was used primarily by relatively small, mainly academic communities, social rules were widely observed. The growth of the Internet has made those rules ineffective. This type of regulation can still be used, however, within restricted groups with strong community ties. For example, the Wikipedia community is governed by social norms regulating the way Wikipedia articles are edited and how conflicts over articles are settled. Through codification into manuals Wikipedia rules have been gradually evolving into self-regulation.

Self-regulation

The US government's 1998 White Paper on Internet Governance[2] that paved the way for the foundation of ICANN, proposed 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 tacit and diffused rules, self-regulation is based on an explicit and well-organised set of rules. Self-regulation rules usually codify a set of rules in form or good conduct.

The trend towards self-regulation is particularly noticeable among ISPs. In many countries, ISPs are under increasing pressure from government authorities to enforce rules related to content policy. ISPs try to answer this pressure through self-regulation by imposing certain standards of behaviour for their customers.

While self-regulation can be a useful regulatory technique, some risks remain in using it for regulating areas of high public interest, such as content policy, freedom of expression, and protection of privacy. Can they make decisions in lieu of legal authorities? Can ISPs judge what acceptable content is?

Jurisprudence

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

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

International legal instruments

The difference between international private law and international public law

The cross-border nature of Internet activities implies the need for the use of international legal tools. In discussions on international law there is a terminological confusion that could have substantive consequences. The term *international law* is mainly used as a synonym for international *public* law, established by nation states, usually through the adoption of treaties and conventions. International public law applies to many areas of the Internet including telecommunications, human rights, and cybercrime to name a few. However, international *private* law is equally, if not more important, for dealing with Internet issues, since most Internet court cases involve issues such as contracts, torts, and commercial responsibilities. The rules of international private law specify the criteria for establishing applicable jurisdiction and law in legal cases with foreign elements (e.g. legal relations involving two or more entities from different countries). For example, who has jurisdiction in the potential legal cases between Internet companies (e.g. Facebook, Twitter) and their users scattered all over the world. The jurisdiction criteria include the link between an individual and national jurisdiction (e.g. nationality, domicile) or the link between a particular transaction and national jurisdiction (e.g. where the contract was concluded, where the exchange of goods took place).

International private law

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

International public law

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

International conventions

The main set of conventions on Internet-related issues was adopted by the ITU, with the ITRs being the most important for preparing a telecommunication policy framework for subsequent Internet developments. The current version of the ITRs (1998) was amended at WCIT-12. Apart from the ITU conventions, the only convention that deals directly with Internet-related issues is the CoE's Cybercrime Convention. However, many other international legal instruments address broader aspects of Internet governance, such as human rights, trade, and intellectual property rights.

International customary law

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

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

Soft law

Soft law has become a frequently used term in the Internet governance debate. Most definitions of soft law focus on what it is not: it is not a legally binding instrument. Typically, soft law instruments contain principles and norms rather than specific rules which are usually found in international documents such as declarations and resolutions. Since it is not legally binding, it cannot be enforced through international courts or other dispute resolution mechanisms.

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

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

Ius cogens

Ius cogens is described by the Vienna Convention on the Law of Treaties[3] in Article 53 as a 'norm, accepted and recognised by the international community of States as a whole, from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character'. Professor Brownlie lists the following examples of *ius cogens* rules:

- The prohibition of the use of force.
- The law of genocide.
- The principle of racial non-discrimination.
- Crimes against humanity.
- The rules prohibiting trade in slaves and piracy.[4]

In Internet governance, *ius cogens* could be used for activities that promote some of these rules (e.g. genocide, racial discrimination, slavery).

Jurisdiction

Jurisdiction is the authority of the court and state organs to decide on legal cases. The relationship between jurisdiction and the Internet has been ambiguous, since jurisdiction rests predominantly on the geographical division of the globe into national territories. Each state has the sovereign right to exercise jurisdiction over its territory. However, the Internet facilitates considerable cross-border exchange, difficult (although not impossible) to monitor via traditional government mechanisms. The question of jurisdiction on the Internet highlights one of the central dilemmas associated with Internet governance: how is it possible to 'anchor' the Internet within existing legal and political geography?[5]

Jurisdiction – basic techniques

Three main considerations are important when deciding on jurisdiction:

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

The following criteria establish jurisdiction in particular cases:

- Territorial Principle – the right of the state to rule over persons and property within its territory.
- Personality Principle – the right of the state to rule over its citizens wherever they might be (nationality principle).

- Effects Principle – the right of the state to rule on economic and legal effects on its territory, stemming from activities conducted abroad.

Another important principle introduced by modern international law is that of universal jurisdiction.[6] 'The concept of universal jurisdiction in its broad sense [is] the power of a state to punish certain crimes, wherever and by whomsoever they have been committed, without any required connection to territory, nationality, or special state interest.'[7] Universal jurisdiction covers such crimes as piracy, war crimes, and genocide.

Conflict of jurisdiction

The conflict of jurisdiction arises when more than one state claims jurisdiction on a particular legal case. It usually happens when a legal case involves an extra-territorial component (e.g. involves individuals from different states, or international transactions). The relevant jurisdiction is established by one of the following elements: territoriality, nationality, or effect of action). When placing content or interacting on the Internet, it is difficult to know which national law, if any, might be violated. In this context, almost every Internet activity has an international aspect that could lead to multiple jurisdictions or a so-called spill-over effect.[8]

One of the early and frequently quoted cases that exemplify the problem of multiple jurisdictions is the 2001 Yahoo! case in France.[9] It was prompted by a breach of French law, which prohibits the exhibition and sale of Nazi objects, even though the website that provided these items – the **Yahoo.com** auction website – was hosted in the USA, where the display of such materials was, and still is, legal. The court case was solved through the use of a technical solution (geo-location software and filtering of access). Yahoo! was forced to identify users who accessed the site from France and block their access to the web pages showcasing Nazi materials.[10]

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

The harmonisation of national laws

The harmonisation of national laws could result in the establishment of one set of equivalent rules at global level. With identical rules in place, the question of jurisdiction would become less relevant. Harmonisation might be achieved in areas where a high level of global consensus already exists, for example, regarding child

See **Section 2** for further discussion on cybersecurity and spam pornography, piracy, slavery, and terrorism. Views are converging on other issues, too, such as cybercrime. However, in some fields, including content policy, it is not very likely that a global consensus on the basic rules will be reached, since cultural differences continue to clash in the online environment more saliently than in the offline world.[11] Another potential consequence of a lack of harmonisation is the migration of Web materials to countries with lower levels of Internet regulation. Using the analogy of the Law of the Sea, some countries might become 'flags of convenience' or the 'offshore' centres of the Internet world.

Arbitration

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

Table 2 presents a short overview of the main differences between traditional court systems and arbitration.

Table 2

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

In comparison to traditional courts, arbitration offers many advantages, including higher flexibility, lower expenses, speed, choice of jurisdiction, and the easier enforcement of foreign arbitration awards. One of the main advantages of arbitration is that it overcomes the potential conflict of jurisdiction. Arbitration has particular advantages in regard to one of the most difficult tasks in Internet-related court cases, enforcement of decisions (awards). The New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards[12] regulates the enforcement of arbitration awards. According to this convention, national courts are obliged to enforce arbitration awards. Paradoxically, it is often easier to enforce arbitration awards in foreign countries by using the New York Convention regime rather than to enforce foreign court judgement.

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

Arbitration has been used extensively in commercial disputes. There is a well-developed system of rules and institutions dealing with commercial disputes. The main international instrument is the United Nations Commission on International Trade Law (UNCITRAL) 1985 Model Law on International Commercial Arbitration.[13] The leading international arbitrations are usually attached to chambers of commerce.

Arbitration and the Internet

Arbitration and other alternative dispute resolution systems are used extensively to fill the gap engendered by the inability of current international private law to deal with Internet cases. A particular example of an alternative dispute resolution method in Internet cases is the Universal Domain-Name Dispute-Resolution Policy (UDRP), which was developed by WIPO and implemented by ICANN as the primary dispute resolution procedure. Since the beginning of its work under UDRP in December 1999, the WIPO Arbitration and Mediation Center has administered more than 22,500 cases and with the introduction of new gTLDs, new challenges are expected to occur.[14]

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

Arbitration provides a faster, simpler, and cheaper way of settling disputes. However, the use of arbitration as the main Internet dispute settlement mechanism has a few serious limitations.

- *First*, since arbitration is usually established by prior agreement, it does not cover a wide area of issues when no agreement between parties has been set in advance (libel, various types of responsibilities, cybercrime).
- *Second*, many view the current practice of attaching an arbitration clause to regular contracts disadvantageous for the weaker side in the contract (usually an Internet user or an e-commerce customer).
- *Third*, some are concerned that arbitration extends precedent-based law (US/UK legal system) globally and gradually suppresses other national legal systems. In the case of e-commerce, this might prove to be more acceptable, given the already high level of unification of substantive rules of commercial law. However, an extension of precedent law has become more delicate in sociocultural issues such as Internet content, where a national legal system reflects specific cultural context.

See **Section 1** for further discussion on the DNS

Intellectual property rights (IPR)

Knowledge and ideas are key resources in the global economy. The protection of knowledge and ideas, through IPR, has become one of the predominant issues in the Internet governance debate, and has a strong development-oriented component. IPR have been affected by the development of the Internet, mainly through the digitisation of knowledge and information, as well as through new possibilities for their manipulation. Internet-related IPR include copyright, trademarks, and patents. Other IPR include designs, utility models, trade secrets, geographical indications, and plant varieties.

Copyright

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

The copyright regime has closely followed the technological evolution. Every new invention, such as the printing press, radio, television, and the VCR, has affected both the form and the application of copyright rules. The Internet is no exception. The traditional concept of copyright has been challenged in numerous ways, from those as simple as 'cutting and pasting' texts from the Web to more complex activities, such as the massive distribution of music and video materials via the Internet.

The Internet also empowers copyright holders, by providing them with more powerful technical tools for protecting and monitoring the use of copyrighted material. These developments endanger the delicate balance between authors' rights and the public's interest, which is the very basis of the copyright law.

So far, copyright holders, represented by major record and multimedia companies, have been very active in protecting their IPR. The public interest has been vaguely perceived and not sufficiently protected. This, however, has gradually been changing, mainly through numerous global initiatives focusing on the open access to knowledge and information (e.g. Creative Commons).

The current situation

Stricter copyright protection at national and international level

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

Several regulations have been enacted at national and international level, aiming to enforce a tighter control by forcing Internet intermediaries to filter or monitor the dissemination of copyrighted content. They triggered strong public protest, which stopped adption of these regulations. In 2011, in the USA, two bills were promoted – the Stop Online Piracy Act (SOPA)[15] and the PROTECT IP Act (PIPA)[16] – which provide for new means to fight against online piracy, including blocking access to infringing websites and banning search engines to link to such sites. At international level, an Anti-Counterfeiting Trade Agreement (ACTA)[17] tried to address IPR infringements in a way that might open the possibility for private (companies) enforcement and policing actions. After strong protests in Europe, the European Parliament voted against ACTA.

Figure 13

These regulatory actions have been harshly criticised by academics and civil liberties groups on human rights and freedoms grounds. Individual Internet users have joined online and offline protests.[18]

Software against copyright infringement

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

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

- A Trojan Horse redirects users to websites where they can legitimately buy the song they tried to download.
- Freeze software blocks computers for a period of time and displays a warning about downloading pirated music.
- Silence, where hard disks are scanned and an attempt is made to remove any pirated files found.
- Interdiction prevents access to the Net for those who try to download pirated music.

Professor Lawrence Lessig of Stanford Law School, has warned that such measures might be illegal.[19] 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 find legal basis in the WIPO Copyright Treaty and in the DMCA. Moreover, the DMCA criminalises 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's White Paper on Intellectual Property and the National Information Infrastructure[20] is that only minor changes are needed in existing regulation, mainly through 'dematerialising' the copyright concepts of 'fixation', 'distribution', 'transmission', and 'publication'. This approach was followed in the main international copyright treaties, including the Trade-Related aspects of Intellectual Property Rights (TRIPS) convention and the WIPO Copyright Treaty.

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 why it combined two elements: the protection of authors' rights and the protection of the public interest. The main challenge was to stipulate how the public can access copyrighted materials in order to enhance creativity, knowledge, and global well-being. Operationally speaking, the protection of the public interest is ensured through the concept of the 'fair use' of protected materials.[21]

Copyright and development

Any restriction of fair use could weaken the position of developing countries. The Internet provides researchers, students, and others from developing countries with a powerful tool for participating in global academic and scientific exchanges. A restrictive copyright regime could have a negative impact on capacity building in developing countries. Another aspect is the increasing digitisation of cultural and artistic crafts from developing countries. Paradoxically, developing countries may end up having to pay for their cultural and artistic heritage when it is digitised, repackaged, and owned by foreign entertainment and media companies.

WIPO and TRIPS

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

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

ISP's liability for copyright infringement

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

The approach taken by the US DMCA and the EU directives[22] is to exempt the service provider from liability for the information transmitted or stored at the direction of the users and demand that the service provider act upon a 'Notice and Take Down' procedure.[23] This solution provides some comfort to ISPs as they are safe from legal sanctions, but also potentially transforms them into content judges[24] and only partially solves the problem, since the contested content may be posted on another website, hosted by another ISP.

A particularly relevant case to the future of copyright on the Internet is the case against Grokster and StreamCast, two companies that produce P2P file-sharing software. Following DMCA provisions, the Recording Industry Association of America (RIAA) requested these companies to desist from the development of file-sharing technology that contributes to the infringement of copyrights. Initially, the US courts chose not to hold software companies like Grokster and StreamCast responsible for possible copyright infringement, under reasonable circumstances. However, in June 2005, the US Supreme Court ruled that software developers were responsible for any possible misuse of their software. The Electronic Frontier Foundation (EFF) noted this case as a prelude to the wave of lawsuits that followed over the next few years against individuals and ISPs reaching over 30,000 cases by 2008.[25] Although the RIAA abandoned its litigation campaign, copyright infringement lawsuits still remain in the spotlight and diversify at the same pace with technological developments.[26]

Trademarks

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

This situation compelled the business sector to place the question of the protection of trademarks at the centre of the reform of Internet governance, leading to the establishment of ICANN in 1998. In the White Paper on the creation of ICANN, the US government demanded that ICANN develop and implement a mechanism for the protection of trademarks in the field of domain names. Soon after its formation, ICANN introduced the WIPO-developed Universal Dispute Resolution Procedure (UDRP).[27]

Patents

Traditionally, a patent protects a new process or product of a mainly technical or production nature. Only recently have patents started being granted for software. More patent registrations result in more court cases among US software companies, involving huge amounts of money. Some patents have been granted for business processes, and some of these were controversial, such as British Telecom's request for licence fees for the patent on hypertext links, which it registered in the 1980s. In August 2002, the case was dismissed.[28] If British Telecom had won this case, Internet users would have to pay a fee for each hypertext link created or used. It is important to stress that the practice of granting patents to software and Internet-related procedures has not been accepted in Europe and other regions.[29]

Cybercrime

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

The drafters of the CoE Convention on Cybercrime[30] 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.

Nevertheless, the prominence of the cybercrime topic put it on the agenda of several international, regional, and local organisations, due to the continuous occurrence and diversification of crimes committed in relation to or by using electronic networking systems.[31] One of the most recent initiatives worth noting is the Commonwealth Cybercrime Initiative[32] that was born within the Commonwealth Internet Governance Forum (CIGF). The business sector has also recognised the importance of fighting cybercrime and has started private initiatives to support awareness campaigns and improvement of legal provisions.[33]

The issues

Definition of cybercrime

The definition of cybercrime has practical relevance and legal implications. If the focus is on offences committed against computer systems, cybercrime would include unauthorised access; damage to computer data or programs; sabotage to hinder the functioning of a computer system or network; unauthorised interception of data to, from, or within a system or network; as well as computer espionage. A definition of cybercrime as all crimes committed via the Internet and computer systems would include a broader range of crimes, including those specified in the Cybercrime Convention: computer-related fraud, infringements of copyright, child pornography, and network security.

Cybercrime and the protection of human rights

The Convention on Cybercrime reinforced the discussion about the balance between security and human rights. Many concerns have arisen, articulated primarily by civil society, that the convention provides state authorities with too broad a power, including the right to check hackers' computers, the surveillance of communication, and more. These broad powers could potentially endanger some human rights, particularly privacy and freedom of expression.[34] The Convention on Cybercrime was adopted by the CoE, one of the most active promoters of human rights. This may help in establishing the necessary balance between the fight against cybercrime and the protection of human rights.

Gathering and preserving evidence

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

Internet traffic data. Under the growing pressure of cyberthreats and terrorist attacks, the EU took a step further and adopted the Data Retention Directive[35] that requires ISPs to retain traffic and location data 'for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member state in its national law' (Article 1). This provision faced strong criticism on privacy grounds and several states have either failed to enact national legislation to comply with the directive or have had such laws annulled as unconstitutional.[36]

In December 2013, the European Court of Justice Advocate General declared the Data Retention Directive incompatible with the Charter of Fundamental Rights.

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), especially in multinational corporation working environment. It is increasingly difficult to distinguish where work starts and where it ends. These changes in working patterns may require new labour legislation, addressing such issues as working hours, the protection of labour interests, and remuneration.

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

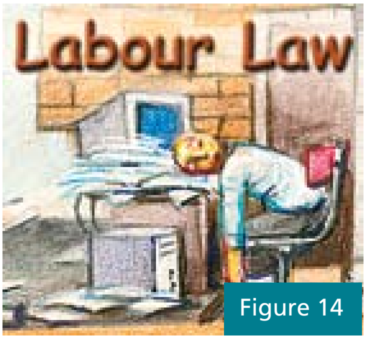


Figure 14

In France, Portugal, and Great Britain, legal guidelines and a few cases have tended to restrict the surveillance of employee e-mail.[37] The employer must provide prior notice of any monitoring activities. In Denmark, courts considered a case involving an employee'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.

An additional point of concern arising with the ever-growing use of social networking is the delimitation between private and working life. Recent cases[38] showed that employees behaviour and comments on social networking sites may address various topics, from workplace and co-workers to employer's strategies and products, deemed as personal (and private) opinions, but which may considerably affect the image and reputation of companies and colleagues.

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[39]

Privacy and data protection are two interrelated Internet governance issues. Data protection is a legal mechanism that ensures privacy. Yet, what is privacy? It is usually defined as the right of any citizen to control their own personal information and to decide about it (to disclose information or not). Privacy is a fundamental human right. It is recognised in the Universal Declaration of Human Rights,[40] the International Covenant on Civil and Political Rights,[41] and in many other international and regional human rights conventions.

National cultures and the way of life influence the practice of privacy. Although this issue is important in Western societies, it may have lesser importance in other cultures. Modern practices of privacy focus on communication privacy (no surveillance of communication) and information privacy (no handling of information about individuals). Privacy issues, which used to focus on governmental activities, have been extended and now include the business sector.[42]

The issues

The main privacy issues are analysed in a triangle among individuals, states, and businesses as presented in Figure 15.

Individuals and states

Information has always been an essential tool for states to exercise authority over their territories and populations. Governments collect vast amounts of personal information (birth and marriage records, social security numbers, voting registration, criminal records, tax information, housing records, car ownership, etc.). It is not possible for an individual to opt out of providing personal data, short of emigrating to another country, where they would confront the same problem. Information technology, such as that used in data mining,[43] aids in the aggregation and correlation of data from many specialised systems (e.g. taxation, housing records, car ownership) to conduct sophisticated analyses, searching for usual and unusual patterns and inconsistencies. One of the main challenges of e-government initiatives is to ensure a proper balance between the modernisation of government functions and the guarantee of citizens' privacy rights, including restricting the collection of information to what is strictly necessary to perform the government's role or the public service. However, recent years have witnessed an increased appetite of governments for collecting and association of more personal data for compulsory identification (such as biometric data).

After the events of 11 September 2001 in the USA, the US Patriot Act[44] and comparable legislation in other countries broadened governments' authority to collect information, including a provision for lawful interception of information. The concept of lawful interception in gathering evidence is also included in the CoE Convention on Cybercrime[45] (Articles 20 and 21). Moreover, the EU requested the adoption of national legislation allowing the retention of data necessary to identify a user for a period of 6 to 24 months.

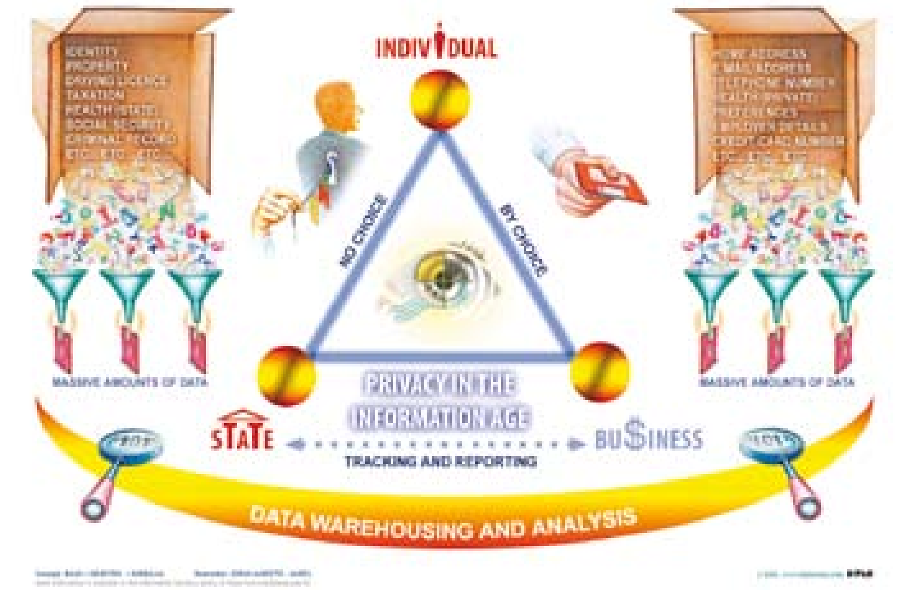
Privacy protection: individuals and businesses

As depicted in the privacy triangle image, the second, and increasingly important relationship is that between individuals and the business sector. A person discloses personal data when opening a bank account, booking a flight or a hotel, paying online with a credit card, or even browsing or searching the Internet. Multiple traces of data are often left in each of these activities.

The success and sustainability of electronic commerce, both business-to-customer and business-to-business, depend on the establishment of extensive trust in both business privacy policies and the security measures they establish to protect clients' confidential information from theft and misuse.[46] With the expansion of social networking platforms (e.g. Facebook, Twitter), concerns arise over the eventual misuse of personal data – not only by the owner or administrator of a social networking platform, but also by other individuals participating in it. [47]

In an information economy, data about customers, including their preferences and purchase profiles, becomes an important market commodity. For some companies, such as Facebook, Google, and Amazon, information about customers' preferences constitutes a cornerstone of their business model. Basically the currency that users pay for (online) services rendered 'for free' is personal data, whether in a form of a browser cookie indicating their online behaviour or a specific information requested in filling in a webform or making a payment. And with the increased amount of information users reveal about themselves, the privacy violations become as frequent and more sophisticated.[48]

Figure 15



Privacy protection: states and businesses

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

Privacy protection: individuals and individuals

The last aspect of privacy protection, not represented within the privacy triangle, is the potential risk to privacy coming from individuals. Today, any person with sufficient funds may own powerful surveillance tools. Even a simple mobile phone equipped with a camera can become such a tool. Technology has 'democratised surveillance' to quote *The Economist*.[49] Many instances of the invasion of privacy have occurred, from simple voyeurism to the sophisticated use of cameras for recording card numbers in banks and for economic espionage.

The main problem for protection from this type of privacy violation is that most legislation focuses on the privacy risks stemming from the state. Faced with this new reality, a few governments have taken some initial steps. The US Congress adopted the Video Voyeurism Prevention Act,[50] prohibiting the taking of photos of unclothed people without their approval. Germany and a few other countries have adopted similar privacy laws, preventing individual surveillance.

The international regulation of privacy and data protection

One of the main international instruments on privacy and data protection is the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[51] of 1981. Although it was adopted by the regional organisation (CoE), it is open for accession by non-European states. Since the Convention is technology neutral, it has withstood the test of time.

The EU Data Protection Directive[52] (Directive 45/46/EC) has also formed an important legislative framework for the processing of personal data in the EU and has had a vast impact on the development of national legislation not only in Europe but also globally. This regulation has also entered a reform process in order to cope with the new developments and to ensure an effective privacy protection in the current technological environment.[53]

Another key international – non-binding – document on privacy and data protection is that of the OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data[54] from 1980. These guidelines and the OECD's subsequent work have inspired many international, regional, and national regulations on privacy and data protection. Today, virtually all OECD countries have enacted privacy laws and empowered authorities to enforce those laws.

While the principles of the OECD guidelines have been widely accepted, the main difference is in the way they are implemented, notably between the European and US approaches. In Europe there is comprehensive data protection legislation, while in the USA the privacy regulation is developed for each sector of the economy including financial privacy (the Graham-Leach-Bliley Act[55]), children's privacy (the Children's Online Privacy Protection Act[56]) and medical privacy (under the Health Insurance Portability and Accountability Act). [57]

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

Safe Harbor Agreement between the USA and the EU

These two approaches – US and EU – to privacy protection have started to conflict. The main problem stems from the use of personal data by business companies. How can the EU ensure that data about its citizens is protected according to the rules specified in its Directive on Data Protection? According to whose rules (the EU's or the USA's) is data transferred through a company's network from the EU to the USA handled? The EU threatened to block the transfer of data to any country that could not ensure the same level of privacy protection as spelled out in its directive. This request inevitably led to a clash with the US self-regulation approach to privacy protection.

This deep-seated difference made any possible agreement more difficult to achieve. Moreover, adjusting US law to the EU data protection law 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 in 1998 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 USA.

When it was signed in 2000, the Safe Harbor Agreement was received with a great hope as the legal tool that could solve similar problems with other countries. However, the record is not very encouraging. It has been criticised by the European Parliament for not sufficiently protecting the privacy of EU citizens. US companies were not particularly enthusiastic about using this approach. According to a study done by Galexia, out of 1597 companies registered in the Safe Harbor Framework, only 348 meet the basic requirements (e.g. privacy policy).[58] Given the high importance of privacy and data protection in the relations between the USA and the EU after the Snowden revelations, it is likely to expect higher pressure to find some solution for the dysfunctional Safe Harbor Agreement. In his policy speech at the European Parliament, Jean-Claude Juncker, the newly elected President of the European Commission mentioned a 'safe harbour' agreement as one of possibility for solving data protection problems between the European Union and the United States.

Endnotes

[1] One of the strongest supporters of the 'real-law' approach is Judge Frank Easterbrook who is quoted as saying: 'Go home; cyberlaw does not exist.' In the article *Cyberspace and the law of the horse*, he argues that although horses were very important there was never a 'Law of the Horse'. Judge Easterbrook argues that there is a need to concentrate on the core legal instruments, such as contracts, responsibility, etc. Available at: **http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf** **[accessed 9 August 2014].**

Easterbook who is quoted as saying: 'Go home, cyberlaw does not exist.' In the article Cyberspace and the Law of the Horse, he argues that although horses were very important there was never a Law of the Horse. Judge Easterbrook argues that there is a need to concentrate on the core legal instruments, such as contracts, responsibility, etc. Available at **http://www.law.upenn.edu/law619/f2001/week15/easterbrook.pdf** [accessed 13 February 2014]. Judge Frank Easterbrook's argument provoked several reactions, including one from Lawrence Lessig in The Law of the Horse: What Cyberlaw Might Teach. Available at **http://cyber.law.harvard.edu/works/lessig/LNC_Q_D2.PDF** [accessed 13 February 2014].

[2] NTIA (1988) Statement of Policy on the Management of Internet Names and Addresses. Available at **http://www.ntia.doc.gov/federal-register-notice/1998/statement**-policy-management-internet-names-and-addresses [accessed 13 February 2014].

[3] Vienna Convention on the Law of Treaties. Available at **http://www.ilsa.org/jessup/jessup11/basicmats/VCLT.pdf** [accessed 13 February 2014].

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

[5] Salis RP (2001) A Summary of the American Bar Association's (ABA) Jurisdiction in Cyberspace Project: Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet. Available at **http://www.jstor.org/discover/10.2307/40687955?uid=3738216&uid=2&uid=4&sid=21103388060741** [accessed 13 February 2014].

[6] Among the most important resources in this field is the *Princeton Principles on Universal Jurisdiction* (2001). Available at **http://www1.umn.edu/humanrts/instree/princeton.html** [accessed 13 February 2014].

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

[8] For an overview of cases involving extraterritorial jurisdiction related to Internet content, see Timofeeva YA (2005) Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis. *Connecticut Journal of International Law*, 20, 199. Available at **http://ssrn.com/abstract=637961** [accessed 13 February 2014].

[9] EDRI-gram (2006) French anti-hate groups win case against Yahoo! Available at **http://edri.gn.apc.org/edrigram/number4.1/yahoocase** [accessed 17 February 2014].

[10] Other court cases include the German Federal Court of Justice case against Fredrick Toben, former German national with Australian nationality who had posted at an Australian-based

website, materials questioning the existence of the holocaust. Available at **http://www.ihr.org/jhr/v18/v18n4p-2_Toben.html** [accessed 13 February 2014].

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

[12] UNCITRAL(1958) The New York Convention. Available at **http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html** [accessed 13 February 2014].

[13] UNCITRAL (1985) Model Law in International Commercial Arbitration. Available at **http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/1985Model_arbitration.html** [accessed 13 February 2014].

[14] WIPO (2012) WIPO Prepares for Launch of New gTLDs while Cybersquatting Cases Continued to Rise. Available at **http://www.wipo.int/pressroom/en/articles/2012/article_0002.html** [accessed 13 February 2014].

[15] Mashable (no date) Stop Online Piracy Act. Available at **http://mashable.com/category/stop**-online-piracy-act/ [accessed 17 February 2014].

[16] US Senate (no date) Protect IP Act. Available at **http://www.leahy.senate.gov/imo/media/doc/BillText-PROTECTIPAct.pdf** [accessed 17 February 2014].

[17] Anti-Counterfeiting Trade Agreement. Available at **http://trade.ec.europa.eu/doclib/docs/2011/may/tradoc_147937.pdf** [accessed 10 April 2014].

[18] La Quadrature du Net, a civil rights advocacy group, has followed closely the developments on HADOPI law and has instrumented a comprehensive file on ACTA. Available at http://www.**laquadrature.net/en/ACTA** [accessed 13 February 2014]. On protests against US bills see Vijayan J (2012) Protests against SOPA, PIPA go viral, Computerworld. Available at **http://www.computerworld.com/s/article/9223496/Protests_against_SOPA_PIPA_go_viral** [accessed 13 February 2014].

[19] Sorkin AR (2003) Software bullet is sought to kill musical piracy. *New York Times* 4 May. Available at **http://www.nytimes.com/2003/05/04/business/04MUSI.html** [accessed 13 February 2014].

[20] US Patents and Trademark Office (no date) Intellectual Property and the National Information Infrastructure. Available at **http://www.uspto.gov/web/offices/com/doc/ipnii** [accessed 13 February 2014].

[21] For an explanation of the concept of 'fair use' and examples see The UK Copyright Service (no date) Copyright Law fact sheet P-09 : Understanding Fair Use. Available at **http://www.copyrightservice.co.uk/copyright/p09_fair_use** [accessed 13 February 2014].

[22] European Union [EU] (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce' and Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. More information available at **http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l24204_en.htm** [accessed 13 February 2014].

[23] The 'Notice and Take Down' procedure refers to the obligation of service providers to remove content from websites under their administration if they receive a notification or complaint regarding the legality of that specific content.

[24] For fear of facing potential legal sanctions, some ISPs prefer to restrict access to indicated content even when no infringement has taken place. For details please consult the following case studies: For Europe (the Netherlands): Nas S (2004) The Multatuli Project ISP Notice & Take Down, Bits of Freedom. Available at **https://www-old.bof.nl/docs/researchpaperSANE.pdf** [accessed 13 February 2014]. For the USA: Urban J and Quilter L (2006), Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. Available at **http://static.chillingeffects.org/Urban-Quilter-512-summary.pdf** [accessed 13 February 2013].

[25] EFF (2008) RIAA v. The People: Five Years Later. Available at **https://www.eff.org/wp/riaa-v-people-five-years-later** [accessed 13 February 2014].

[26] See for example the latest trend in the USA – the copyright trolling: Kravets D (2012) Judge Orders Failed Copyright Troll to Forfeit 'All' Copyrights. **Wired.com**. Available at **http://www.wired.com/threatlevel/2012/03/troll-forfeits-copyrights** [accessed 13 February 2014].

[27] For a comprehensive survey of the main issues involving UDRP please consult WIPO (2011) WIPO Overview of WIPO Panel Views on Selected UDRP Questions, Second Edition (WIPO Overview 2.0) Available at **http://www.wipo.int/amc/en/index.html** [accessed 13 February 2014].

[28] Loney M (2002) Hyperlink patent case fails to click. CNET **News.com**. Available at **http://news.cnet.com/2100-1033-955001.html** [accessed 13 February 2014].

[29] For more information about the debate in Europe on software patentability, please consult **http://eupat.ffii.org** [accessed 13 February 2014].

[30] Council of Europe Convention on Cybercrime (2001) Available at **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm** [accessed 13 February 2014].

[31] For a listing of anti-cybercrime networks, organisations and initiatives worldwide see the Council of Europe's resources page, available at **http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/networks/Networks_en.asp** [accessed 13 February 2014].

[32] Commonwealth Internet Governance Forum (2012) Commonwealth Cybercrime Initiative. Available at **http://www.commonwealthigf.org/cigf/cybercrime** [accessed 13 February 2014].

[33] As an example see McAfee Initiative to Fight Cybercrime site and its Multipoint Strategy. Available at **http://www.mcafee.com/us/campaigns/fight_cybercrime/strategy.html** [accessed 13 February 2014].

[34] For critical views of the Cybercrime Convention expressing the concern of civil society and human rights activists, please consult: The Association for Progressive Communication Report on the Cybercrime Convention. Available at **http://rights.apc.org/privacy/treaties_icc_bailey.shtml** [accessed 13 February 2014].

[35] European Parliament (2006) Data Retention Directive. Available at **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF** [accessed 13 February 2014].

[36] For a detailed overview of the data retention issues in EU see European Commission (2011) Evaluation report on the Data Retention Directive (Directive 2006/24/EC). Available at **http://www.publications.parliament.uk/pa/cm201012/cmselect/cmeuleg/428-xxix/42816.htm** [accessed 13 February 2014].

[37] The Register (2007) EU court rules monitoring of employee breached human rights. 5 April. Available at **http://www.theregister.co.uk/2007/04/05/monitoring_breached_human_rights** [accessed 13 February 2014].

[38] See the following articles for example: Holding R (2011) Can You Be Fired for Bad-Mouthing Your Boss on Facebook? Time U.S. Available at **http://www.time.com/time/nation/article/0,8599,2055927,00.html** [accessed 13 February 2014]. Broughton A *et al.* (2009) Workplaces and Social Networking. The Implications for Employment Relations, Acas. Available at **http://www.acas.org.uk/media/pdf/d/6/1111_Workplaces_and_Social_Networking.pdf** [accessed 13 February 2014].

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

[40] UN (no date) Universal Declaration of Human Rights. Available at **http://www.un.org/en/documents/udhr/index.shtml#**a12 [accessed 13 February 2014].

[41] UNHCR (no date) International Covenant on Civil and Political Rights. Available at **http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx** [accessed 27 March 2014].

[42] A report issued by the American Civil Liberties Union: Stanley J (2004). The surveillance-industrial complex: How the American government is conscripting businesses and individuals in the construction of a surveillance society. This report explains the problem of the privatisation of surveillance and new challenges linked to the protection of privacy. Available at **https://www.aclu.org/files/FilesPDFs/surveillance_report.pdf** [accessed 13 February 2014].

[43] UCLA (no date) What is data mining? Available at **http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm** [accessed 17 February 2014].

[44] **Epic.org** (no date) US Patriot Act. Available at **http://epic.org/privacy/terrorism/hr3162.html** [accessed 13 February 2014].

[45] Council of Europe (2001) Convention on Cybercrime. Available at **http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm** [accessed 13 February 2014].

[46] TRUSTe, the organisation that developed a privacy seal mark to certify compliance of websites with the privacy requirements, is also monitoring consumer confidence online. For the latest results of their survey see: TRUSTe Launches New Privacy Index Measuring Consumer Privacy Insights and Trends. San Francisco, California, 13 February 2012. Available at **http://www.truste.com/about-TRUSTe/press-room/news_truste_launches_new_trend_privacy_index** [accessed 13 February 2013].

[47] The privacy focus and concern related to social networking sites are very well illustrated by the attentive monitoring and pressure exerted by media civil rights advocates on Facebook. For an overview of the wide range of privacy issues raised in relation to the use of this platform see Wikipedia (2012) Criticism of Facebook. Available at **http://en.wikipedia.org/wiki/Criticism_of_Facebook** [accessed 13 Facebook 2013].

[48] For an overview of the most prominent privacy breaches over time (though with a US focus) see Marsan C (2012) 15 worst Internet privacy scandals of all time. Network World 26 January. Available at **http://www.networkworld.com/news/2012/012612-privacy-scandals-255357.html?page=1** [accessed 13 February 2014].

[49] *The Economist* (2004) Move over, Big Brother. 2 December. Available at **http://www.economist.com/node/3422918** [accessed 13 February 2014].

[50] **Gov.track.us** (no date) Video Voyeurism Prevention Act. Available at **http://www.govtrack.us/congress/bills**/108/s1301 [accessed 13 February 2014].

[51] Council of Europe (no date) Convention for the protection of individual with regard to automatic processing of personal data. Available at **http://conventions.coe.int/treaty/en/treaties/html/108.htm** [accessed 13 February 2014].

[52] Europa (no date) Protection of personal data. Available at **http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm** [accessed 11 April 2012].

[53] More details about the reform process are available at **http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm** [accessed 13 February 2014].

[54] OECD (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at **http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm** [accessed 13 February 2014].

[55] Graham-Keach-Bliley Act. Available at **http://www.ftc.gov/privacy/glbact/glbsub1.htm** [accessed 13 February 2014].

[56] Children's Online Privacy Protection Act. Available at **http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule** [accessed 13 February 2014].

[57] Health Information Privacy. Available at **http://www.hhs.gov/ocr/privacy**/ [accessed 13 February 2014].

[58] Connolly C (2008) The US Safe Harbor – Fact or Fiction? Galexia. Available at **http://www.galexia.com/public/research/articles/research_articles-pa08.html** [accessed 13 February 2014].

Section 4

The economic basket

The economic basket

We know how to route packets.
What we don't know how to do is route dollars

David Clark

This quote from David Clark, chief Internet protocol architect, reflected the spirit of the early Internet community, where the non-profit Internet project was supported mainly by US research grants. But, in the 1990s and early 2000s new business models for 'routing dollars' started to emerge in Silicon Valley centred on income from advertising.

Economic issues in Internet governance are mainly related to this evolution from the Internet as a non-profit project to one of the main business facilities and engines of economic growth of modern society. The flow of ideas and creativity of the early Internet has been complemented by and, increasingly, finds itself in competition for the flow of money. More money has introduced more tangible business and policy interests. The creative 'blue sky is the limit' approach of the early Internet community has begun to converse with the 'bottom line' logic of the business community.

Internet economic practice is presently considered efficient, because of the Internet's smooth functionality and, in general, its affordable cost. The primary criticism of the current Internet economy is a risk of a monopoly of the main Internet and telecom companies that could lead towards distortion of the market.

Nguyen and Armitrage argue that the Internet should have a proper and optimal balance between three elements: technical efficiency, economic efficiency, and social effects.[1] Other authors highlight the challenges of replacing the existing, simple, flat-rate pricing structure with a more complex one, such as accounting based on the traffic of packets.[2] With regard to practical changes, some believe that changing the current Internet economic policies could open a Pandora's box.

The bottom line in governance analysis is often an analysis of the flow of money.[3] The answer to the simple question – who pays for the Internet – is complex. A number of monetary and non-monetary transactions occur between the many parties involved with the Internet. We will address them in four main domains:

- E-commerce: traditional commercial activities conducted via the Internet.
- Internet CONTENT economy: new advertising-based business model.
- Internet ACCESS economy: telecommunication industry in the Internet era.
- E-payments and cybercurrency.

In addition, we will address the following policy issues of economic relevance: customer protection, taxation, and digital signatures.

E-commerce

E-commerce has been one of the main engines promoting the growth of the Internet over the past 15 years. The importance of e-commerce is illustrated by the title of the document that initiated the reform of Internet governance and established ICANN: the 1997 Framework for Global Electronic Commerce,[4] which states that 'the private sector should lead' the Internet governance process and that the main function of this governance will be to 'enforce a predictable, minimalist, consistent, and simple legal environment for commerce'. These principles are the foundation of the ICANN-based Internet governance regime.

Definition

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

For the US government, the key element distinguishing traditional commerce from e-commerce is the online commitment to selling goods or services. This means that any commercial deal concluded online should be considered an e-commerce transaction, even if the realisation of the deal involves physical delivery. For example, purchasing a book via Amazon.com is considered an e-commerce transaction even though the book is usually delivered via traditional mail. The WTO defines e-commerce more precisely as: 'the production, distribution, marketing, sale, or delivery of goods and services by electronic means'.[5] The EU approach to e-commerce deals with 'information society services' that cover 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service'.[6]

E-commerce takes many forms:

- Business-to-consumer (B2C) – the most familiar type of e-commerce (e.g. Amazon.com).
- Business-to-business (B2B) – economically the most intensive, comprising over 90% of all e-commerce transactions.[7]
- Business-to-government (B2G) – highly important in the area of procurement policy.
- Consumer-to-consumer (C2C) – for example, ebay auctions.

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

The WTO and e-commerce

As the key policy player in modern global trade, the WTO has established a system of agreements regulating international trade. The major treaties are the General Agreement on Tariffs and Trade (GATT)[8] dealing with the trade in goods, the General Agreement on Trade in Services (GATS), and the Agreement on Trade-related Aspects of Intellectual Property Rights (TRIPS).[9] Within this framework, the WTO regulates many relevant e-commerce issues, including telecommunication liberalisation, IPR, and some aspects of ICT development. E-commerce figures in the following WTO activities and initiatives:

- A temporary moratorium on custom duties on e-transactions, introduced in 1998, has rendered all e-transactions globally free of custom duties.
- The establishment of the WTO Work Programme for Electronic Commerce promotes discussion on e-commerce.[10]
- A dispute resolution mechanism; e-commerce was particularly relevant in the USA/Antigua Online Gambling case.[11]

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

Should e-commerce transactions be categorised under services (regulated by GATS) or goods (regulated by GATT)?

Does the categorisation of music as a good or a service change depending on whether it is delivered on a CD (tangible) or via the Internet (intangible)? Ultimately, the same song could have different trade status (and be subject to different customs and taxes) depending on the medium of delivery. The issue of categorisation has considerable implications, because of the different regulatory mechanisms for goods and services.

What should the link be between TRIPS and the protection of IPR on the Internet?

Since the WTO's TRIPS agreement provides much stronger enforcement mechanisms for IPR, developed countries have been trying to extend TRIPS coverage to e-commerce and to the Internet by using two approaches. First, by citing the principle of 'technological neutrality', they argue that TRIPS, like other WTO rules, should be extended to any telecommunication medium, including the Internet. Second, some developed countries have requested the closer integration of WIPO's 'digital treaties' into the TRIPS system. TRIPS provides stronger enforcement mechanisms than WIPO conventions. Both issues remain open and they will become increasingly important in future WTO negotiations. During the current stage of trade negotiations, it is not very likely that e-commerce will receive prominent attention on the WTO agenda. The lack of global e-commerce arrangements will be partially compensated by some specific initiatives (e.g. regarding 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 the United Nations Commission on International Trade Law[12] (UNCITRAL) Model Law on Electronic Commerce.[13] The focus of the Model Law is on mechanisms for the integration of e-commerce with traditional commercial law (e.g. recognising the validity of electronic documents). The Model Law has been used as the basis for e-commerce regulation in many countries. Another initiative designed to develop e-commerce is the introduction of e-business XML (ebXML)[14] by the United Nations Centre for Trade Facilitation and Electronic Business (UN/

CEFACT), which is a set of standards based on XML technology. While these standards are still developing new versions, and the previous set – the Electronic Data Interchange (EDI) – is still widely deployed, it remains to be seen if and how they will be adjusted to cope with new trends and technological developments.[15]

The OECD's activities touch on various aspects related to e-commerce, including consumer protection and digital signatures. The OECD emphasises promotion and research regarding e-commerce through its recommendations and guidelines.

UNCTAD is particularly active in research and capacity-building, focusing on the relevance of e-commerce to development. Every year it monitors the evolution of the information economy in a report which assesses the role of new technologies in trade and development.[16] In the business sector, the most active international organisations are the International Chamber of Commerce,[17] which produces a wide range of recommendations and analyses in the field of e-commerce; and the Global Business Dialogue,[18] which promotes e-commerce in both the international and the national context.

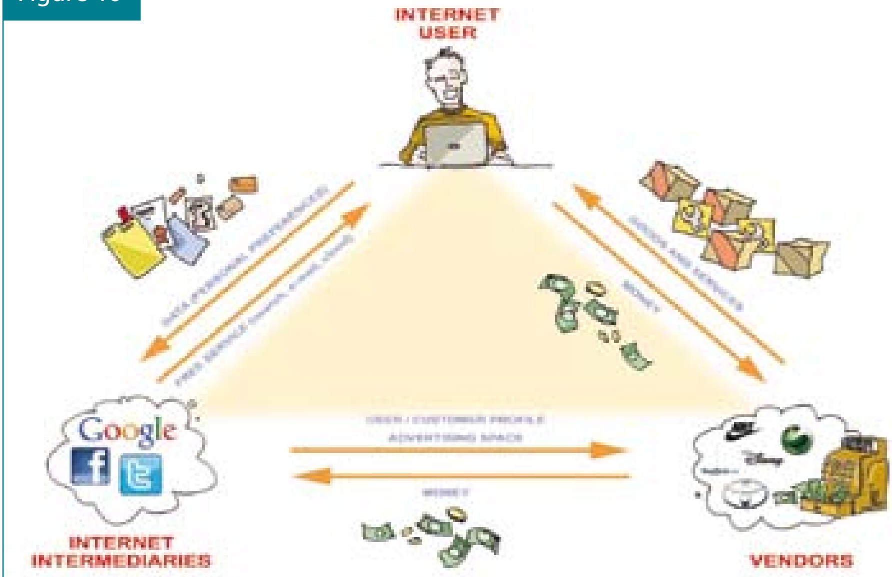
Regional initiatives

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[19] 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 the Asia-Pacific Economic Co-operation (APEC). APEC established the E-Commerce Steering Group, which addresses various e-commerce issues, including consumer protection, data protection, spam, and cybersecurity. The most prominent initiative is APEC's Paperless Trading Individual Action Plan,[20] which aims to create paperless systems in cross-border trade.

Internet CONTENT economy

Figure 16



The new business model of the Internet industry, developed mainly by companies based in Silicon Valley, started emerging in the late 1990s and took full shape in the 2010s. The growth of the Internet in the 1990s could not be sustained on previous public funding; it required a more robust business model. A few attempts to charge for access to Internet services and content failed. The new Internet business model does not charge users for the use of the Internet services; it generates income from sophisticated advertising.

Users 'pay' for provided services with their data, including information they generate – their 'electronic footprint' – as they search and interact on the Internet. Internet companies analyse user data in order to extract bits of information about their preferences, tastes, and habits. They also mine the data to extract information about a group; for instance the behaviour of teenagers in a particular city or region. Internet companies can predict with high certainty what a person with a certain profile is going to buy or do. This valuable block of data about Internet users has different commercial uses. Mainly, it is purchased by vendors who use it for their marketing activities. For example, in 2013, 90% of Google's US $55.5 billion annual revenue came from advertising and related services.[21]

Issues

Protection of users and transparency

Formally speaking, by clicking 'I agree' to usually long and fine-print contracts, users accept conditions of services. The question remains whether users are making informed decisions, especially in view of the potential use of their data for commercial purposes. It is very likely that – in many cases – users will accept the 'deal' of exchanging their data for valuable Internet services. The more transparent and easier to comprehend Internet arrangements are, the more beneficial it is not only for users but also for Internet companies who can ensure a more sustainable business model.

Risk of market monopolies

The nature of the Internet industry is prone to the establishment of market monopolies (e.g. Google's share of Internet searches is more than 80% in Europe). In addition, there are not global anti-monoply policy regimes which may deal with the potential global market monopoly of the Internet industry. Huston argues that establishing monopolies and losing the diverse market of Internet resources would inevitably affect the price and quality of Internet services.[22]

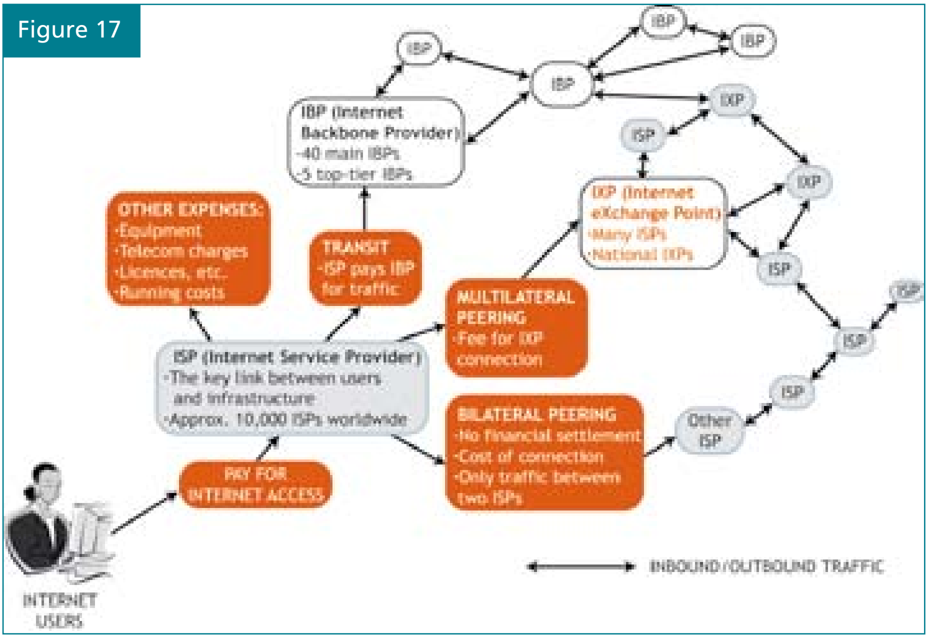
Currently, the EU is the strongest anti-monopoly player globally. With a market of 500 million people, the EU can force Internet companies to follow its market regulations and prevent monopolistic practices. The EU initiated anti-monopoly action against Google, focusing on – among other issues – the positioning of paid advertisement on the list of search results. Other countries with smaller Internet markets and less policy leverage are likely to follow an arrangement negotiated between the EU and Internet companies.

Internet ACCESS economy

Internet users and companies pay ISPs for Internet access and services. Typically ISPs have to cover the following expenses from the fees collected:

- Cost of telecommunication expenses and Internet bandwidth to the next major Internet hub.
- Cost of IP addresses obtained from regional Internet registries (RIRs) or local Internet registries (LIRs). An IP address is needed by a device to access the Internet.
- Cost of equipment, software, and maintenance of their installations.

Figure 17



Increasingly, Internet ACCESS business is complicated by regulatory requirements of governments such as data-retention. More regulation requires more expenses which could be either passed to Internet users through subscription or buffered by reduced profit for the ISPs.

The issues

Re-distribution of revenue between telecommunication and Internet companies

Telecommunication operators are raising the question of re-distribution of the revenue generated by the Internet. They are trying to increase their share of the 'revenue pie' generated by the Internet boom. So far, the main business beneficiaries of the Internet boom are Internet content companies due to their innovative business model based on online advertising. The main argument by the telecommunication companies is that *they* facilitate access to Internet content through *their* cables and telecommunication infrastructure.

The telecommunication industry usually justifies requests for a higher income from Internet-generated revenue by the need to invest in the upgrading of the telecommunication infrastructure. Content companies, on the other hand, argue that access providers already charge the end users for Internet access, and that the main reason for their alleged lower incomes are their obsolete business models ('all-you-can-eat' charges such as flat rates). European telecommunication operators, organised into the European

Telecommunications Network Operators' Association (ETNO), created a lot of waves during the preparation for WCIT-12 in Dubai by making a concrete proposal that would alter the current revenue model by proposing that content providers (e.g. Facebook, Google) pay for access to their services.

The proposal did not gain support in the preparation for WCIT-12, but it is likely to remain an open issue in future Internet governance negotiations. This discussion on the redistribution of Internet revenue strongly underpins the network neutrality debate – for example, should all Internet traffic have the same status as it does today, or should it be segregated into different Internet(s) depending on the quality of services, payment, and reliability (e.g. having a range of Internets from VIP Internet to an Internet for the poor).

Sharing telecommunication revenue with developing countries

Many developing countries have been complaining about the unfavourable economic conditions of the Internet economy. 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 – the developing countries that have to finance connection to Internet backbones located mainly in developed countries. As a result, paradoxically, small and poor countries may end up subsidising the Internet in developed countries.

The problem of financial settlement is particularly relevant for the poorest countries, which rely on income from international telecommunications as an important budgetary source. The situation has been further complicated with the introduction of VoIP – Internet telephony – which shifts telephone traffic from national telecommunications operators to the Internet.

Developing countries have been raising the question of fairer Internet access business models during WSIS, ITU working groups, and, more recently, at WCIT-12 in Dubai.

E-banking, e-money, and virtual currencies

> *Digital cash is a threat to every government on this planet that wants to manage its own currency.*
>
> **David Saxton**[23]

E-banking involves the use of the Internet to conduct conventional banking operations, such as card payments or fund transfers. The novelty is only in the medium; the banking service remains essentially the same. E-banking provides advantages to customers by introducing new services and reducing the costs of transactions. For example, it is estimated that customer transactions, which cost $4 in traditional banking, cost only $0.17 in Internet banking.[24]

E-money is defined by the Bank for International Settlements (BIS) as ‘stored value or prepaid payment mechanisms for executing payments via point-of-sale terminals, direct transfers between two devices, or over open computer networks such as the Internet’.[25] E-money is usually associated with so-called smart cards issued by companies such as Mondex and Visa Cash. E-money is anchored in the existing banking and monetary system (financial legal tender).

Unlike e-money, virtual currencies are not part of a national financial system. Issuing virtual currencies would be akin to printing money without the control of a central banking institution. Bitcoin is the most well-known virtual currency, and is also described as a cryptocurrency, since it is created through a special process based on cryptography.[26]

The issues

Changes to the worldwide banking system

The further use of both e-banking and e-money could bring about changes to the worldwide banking system, providing customers with additional possibilities while simultaneously reducing banking charges. Bricks-and-mortar banking methods will be seriously challenged by more cost-effective e-banking.[27] It should be noted that many traditional banks have already adopted e-banking. In 2002, there were only 30 e-banks in the United States. Today it is difficult to find a bank without e-banking services.

Mobile commerce

E-payments and e-money are currently undergoing fast changes at the same pace as technology and devices evolve and develop. Mobile payments have already surpassed the simple orders placed via SMS at the beginning, as mobile phones became more sophisticated and ‘intelligent’ (like smart phones and iPhones) allowing for diverse applications, including for mobile commerce.[28]

Cybersecurity

Cybersecurity is one of the main challenges to the wider deployment of e-payments. How can the safety of financial transactions via the Internet be ensured? Cybersecurity has been already been discussed. On this point, it is important to stress the responsibility of banks and other financial institutions for the security of online transactions. The main development in this respect was the Sarbanes-Oxley Act (SOXA),[29] adopted by the US Congress as a reaction to the Enron, Arthur Andersen, and WorldCom financial scandals. This act tightens financial control and increases the responsibility of financial institutions for the security of online transactions. It also shares the burden of security responsibility between customers – who have to demonstrate certain prudence – and financial institutions.[30]

See **Section 2** for further discussion on cybersecurity

Lack of payment methods

A lack of payment methods is often viewed as one of the main impediments to the faster development of e-commerce. Currently, e-commerce is conducted primarily by credit card. This is a significant obstacle for developing countries that do not have a developed credit card market. The governments in those countries would have to enact the necessary legal changes in order to enable the faster introduction of card payments.

National initiatives

In order to foster the development of e-commerce, governments worldwide 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[31] in 2000 (it was revised in 2009). Unlike e-money, there is no regulation of virtual currency in the EU. Currently, it is left to the member states to regulate virtual currencies such as Bitcoin. Germany considers Bitcoin as 'private money' exchanged between two persons or entities. In the UK, it is a considered a means of exchange but not money. Most countries have chosen a 'wait and see' approach. Currently, Bitcoin does not present a major risk for the monetary system in the form of various misuses (money laundering, theft, etc.). However, some countries, such as Russia and Thailand, have taken more radical steps by banning Bitcoin.

Addressing the issue at international level

Due to the nature of the Internet, it is likely that e-money and virtual currencies will become global phenomena, thus providing a reason to address this issue at international level. One potential player in the field of e-banking is the Basel Committee E-Banking Group. This group has already started addressing authorisation, prudential standards, transparency, privacy, money laundering, and cross-border supervision, which are key issues for the introduction of e-money.[32]

Regarding virtual currency, the main international initiative has been taken in the Financial Action Task Force (FATF) which addresses the questions of money laundering and the financing of terrorism.[33] The USA has initiated discussions in the FATF on how to apply rules against money laundering and the financing of terrorism in the field of virtual currencies.

The law enforcement link

The 2002 request from the New York State Attorney General to Pay-Pal and Citibank not to execute payments to Internet casinos directly links electronic payment to law enforcement.[34] What the law enforcement authorities could not achieve through legal mechanisms, they could accomplish through the control of electronic payments.

Privacy

The use of e-payment systems leaves a trace of every transaction performed which is recorded by the issuers of the e-payment instrument (credit card companies, banks). While the keeping of such records is needed and justifiable for clearing purposes and evidence of payments, the aggregation of such data may pose serious threats to users' privacy if data mining is used for tracking purchasing and spending habits or scoring clients for provision of future financial services.[35]

Risks and misuse of virtual currencies

The risks of virtual currency became clear after the closure of Mt Gox, one of the biggest Bitcoin companies, in February 2014.[36] A large number of investors lost close to US$ 500 million.

There are many warnings that virtual currencies could be misused for illegal goods and services, fraud, and money laundering. The anonymity of Bitcoin transactions increases the potential for possible misuse. So far, there have only been a few cases of reported misuse. The FBI closed the Silk Road website which was used to trade in stolen card data, drugs, and other illegal products; the website used Bitcoin as its payment method.

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:

- Online handling of payment card information.
- Misleading advertising.
- Delivery of defective products.

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

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

The main disadvantage for e-commerce companies is the potential for exposure to a wide variety of legal jurisdictions. One possible solution to this dilemma is a more intensive harmonisation of consumer protection rules, making the question of jurisdiction less relevant. As with other e-commerce issues, the OECD assumed the lead by adopting the 1999 Guidelines for Consumer Protection in the Context of E-commerce[37] and the 2003 Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders.[38] The main principles established by the OECD are still valid and have been adopted by other business associations, including the International Chamber of Commerce and the Council of Better Business Bureaus.[39]

The EU offers a high level of e-commerce consumer protection and promotes awareness campaigns on online shopping issues. The problem of jurisdiction has been solved via the Brussels I Regulation,[40] which stipulates that consumers will always have recourse to local legal protection. The recast Brussels I Regulation,[41] applicable as of January 2015, further harmonises the rules of jurisdiction by extending the situations under which individuals not domiciled in the EU can be sued by consumers in the courts of EU member states.

More than half of EU consumers (53%) made at least one purchase online in the 12 months to September 2012, almost doubling since 2006. Yet just 15% purchased online from vendors outside their own country. This is reflected in the confidence rating: while 53% feel comfortable purchasing from online domestic retailers, only 36% feel comfortable buying online from another EU country.[42]

At global level, no apposite international legal instruments have been established. One of the most apt, the 1980 UN Convention on Contracts for the International Sale of Goods,[43] does not cover consumer contracts and consumer protection.

A number of private associations and non-governmental organisations also focus on consumer e-commerce protection, including Consumers International, the International Consumer Protection and Enforcement Network, and Consumer Reports WebWatch.

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

Taxation

After Faraday discovered the basic principle of electricity in 1831 (electromagnetic induction), a sceptical politician asked him about the purpose of his invention. Faraday responded with: 'Sir, I do not know what it is good for. But of one thing I am quite certain, some day you will tax it.' [44]

With the Internet moving into the mainstream of modern society, the question of taxation has come into sharper focus. It has become even more important since the financial crisis in 2008. Many governments have been trying to increase fiscal income in order to reduce growing public debt. The most comprehensive report on Internet taxation was presented by the French Ministry of Economy and Finance in January 2013.[45] The taxation of economic activities on the Internet became one of the first possibilities for increasing fiscal income.

The Internet governance dilemma of whether cyber issues should be treated differently from real-life issues is clearly mirrored in the question of taxation.[46] Since the early days, the USA has been attempting to declare the Internet a tax-free zone. In 1998, the US Congress adopted the Internet Tax Freedom Act,[47] which was extended for another three years in December 2004. In October 2007, the Act was extended until 2014, in spite of some fears that it could lead to a substantial revenue loss.[48]

The OECD and the EU have promoted the opposite view, i.e., that the Internet should not have special taxation treatment. The OECD's Ottawa Principles specify that taxation of e-commerce should not be based on the same principles as taxation for traditional commercial activities.[49] By applying this principle, the EU introduced a regulation in 2003 requesting non-EU e-commerce companies to pay value added tax (VAT) if they sold goods within the EU. The main motivation for the EU's decision was that non-EU (mainly US) companies had an edge over European companies, which had to pay VAT on all transactions, including electronic ones.

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

Digital signatures

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

When it comes to digital signatures, the main challenge is that governments are not regulating an existing problem, such as cybercrime or copyright infringement, but creating a new regulatory environment in which they have no practical experience. This has resulted in a variety of solutions and a general vagueness in the provisions on digital signatures. Three major approaches to the regulation of digital signatures have emerged.[50]

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

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

The third approach, adopted within the EU Electronic Signatures Directive,[51] combines these two approaches. It has a minimalist provision for the recognition of signatures supplied via an electronic medium. The maximalist approach is also recognised through granting that 'advanced electronic signatures' will have stronger legal effect in the legal system (e.g. easier to prove these signatures in court cases). The EU regulation on digital signatures was one of the responses at multilateral level. While it has been adopted in all EU member states, a difference in the legal status of digital signatures still remains.[52]

At global level, in 2001, UNCITRAL adopted the Model Law on Electronic Signatures,[53] which grants the same status to digital signatures as to handwritten ones, providing some technical requirements are met. The International Chamber of Commerce (ICC) issued a General Usage in International Digitally Ensured Commerce (GUIDEC), which provides a survey of the best practices, regulations, and certification issues.[54]

Public key infrastructure (PKI) initiatives are directly related to digital signatures. Two organisations, the ITU and the IETF, are involved with PKI standardisation.

The issues

Privacy and digital signatures

Digital signatures are part of a broader consideration of the relationship between privacy and authentication on the Internet. Digital signatures are just one of the important techniques used to identify individuals on the Internet.[55]

For instance, in some countries where digital signature legislation or standards and procedures have not yet been set up, SMS authentication via mobile phones is used by banks for approving customers' online transactions.

The need for detailed implementation standards

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

The risk of incompatibility

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

Endnotes

[1] Thuy T, Nguyen T, Armitage GJ (2005) Evaluating Internet Pricing Schemes: A Three-Dimensional Visual Model. *ETRI Journal* 27(1) pp. 64-74. Available at **http://etrij.etri.re.kr/etrij/journal/article/article.do?volume=27&issue=&page=64**? [accessed 13 February 2014].

[2] Hayel Y, Maille P, Tuffin B (2005) Modelling and analysis of Internet Pricing: introduction and challenges in *Proceedings of the International Symposium on Applied Models and Data Analysis* (ASMDA), Brest, France. Available at **http://conferences.telecom-bretagne.eu/asmda2005/IMG/pdf/proceedings/1389.pdf** [accessed 13 February 2014].

[3] Andrew Odlyzko views the question of pricing and architecture on the Internet from a historical perspective. Identifying the thread in the pricing policy from the pricing of transportation systems in the ancient world, he links with the current Internet pricing policy. For more information, consult: Odlyzko A (2004) Pricing and Architecture of the Internet: Historical Perspectives from Telecommunications and Transportation. Available at **http://www.dtc.umn.edu/~odlyzko/doc/pricing.architecture.pdf** [accessed 13 February 2014].

[4] The White House (1997) Framework for Global Electronic Commerce. Available at **http://clinton4.nara.gov/WH/New/Commerce/** [accessed 17 February 2014].

[5] WTO (1998) Work programme on electronic commerce. Available at **http://www.wto.org/english/tratop_e/ecom_e/wkprog_e.htm** [accessed 17 February 2014].

[6] European Union [EU] (2000) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Available at **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:NOT** [accessed 17 February 2014].

[7] Global Web Index. GlobalWebIndex e-Commerce Report: Online Plays a Role in 90% of Transactions. Available at **http://blog.globalwebindex.net/globalwebindex-e-commerce-report-online-plays-a-role-in-90-of-transactions/** [accessed 10 August 2014].

[8] WTO (no date) GATT and the Goods Council. Available at **http://www.wto.org/english/tratop_e/gatt_e/gatt_e.htm** [accessed 17 February 2014].

[9] WTO (1994) Agreement on Trade-related Aspects of Intellectual Property Rights. Available at **http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm** [accessed 17 February 2014].

[10] This section of the WTO website focuses on e-commerce. Available at **http://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm** [accessed 17 February 2014].

[11] For more information about the USA/Antigua Online Gambling Case, please consult **http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm** [accessed 17 February 2014].

[12] UNCITRAL website. Available at **http://www.uncitral.org/uncitral/index.html** [accessed 17 February 2014].

[13] UNCITRAL (1996) Model Law on Electronic Commerce. Available at **http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html** [accessed 17 February 2014].

[14] ebXML website. Available at **http://www.ebxml.org/** [accessed 17 February 2014].

[15] See for example a discussion about the relevance of ebXML standard today. Available at **http://www.infoq.com/news/2012/01/ebxml** [accessed 17 February 2014].

[16] UNCTAD (no date) Economic reports. Available at **http://unctad.org/en/Pages/Publications/InformationEconomyReportSeries.aspx** [accessed 17 February 2014].

[17] International Chamber of Commerce website. Available at **http://www.iccwbo.org/** [accessed 17 February 2014].

[18] The Global Business Dialogue website. Available at **http://www.gbdinc.org/** [accessed 17 February 2014].

[19] European Commission (no date) E-commerce directive. Available at **http://ec.europa.eu/internal_market/e-commerce/directive_en.htm** [accessed 17 February 2014].

[20] APEC (no date) Paperless Trading Individual Action Plan. Available at **http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Paperless-Trading-Individual-Action-Plan.aspx** [accessed 17 February 2014].

[21] Google (no date) Investor relations. Available at **http://investor.google.com/financial/tables.html** [accessed 10 August 2014].

[22] Huston G (2005) *Where's the Money? – Internet Interconnection and Financial Settlements.* The ISP Column. Available at **http://www.potaroo.net/ispcol/2005-01/interconn.pdf** [accessed 13 February 2014].

[23] As quoted in Holland K and Cortese A (1995) The future of money: e-cash could transform the world's financial life. Available at **http://www.businessweek.com/1995/24/b3428001.htm** [accessed 17 February 2014].

[24] As reported in Olson T (2012) Higher costs, new laws mean no more free rides on some bank services, accounts. *Pittsburgh Tribune-Review,* April 1. Available at **http://www.pittsburghlive.com/x/pittsburghtrib/business/s_789300.html** [accessed 17 February 2014].

[25] Basel Committee on Banking Supervision (1998) *Risk Management for Electronic Banking and Electronic Money Activities.* Basel March 1998 Available at **http://www.bis.org/publ/bcbs35.pdf** [accessed 17 February 2014]. Final version published in 2003 and available at **http://www.bis.org/publ/bcbs98.htm** [accessed 17 February 2014].

[26] Kamberi A (2014) Cryptocurrencies and bitcoin. Available at **http://www.diplomacy.edu/blog/cryptocurrencies-and-bitcoin** [accessed 10 August 2014].

[27] This article provides an introduction to online banking and a survey of the advantages and disadvantages in comparison to traditional banking. Available at **http://www.bankrate.com/brm/olbstep2.asp** [accessed 17 February 2014].

[28] appsworldblog (2011) 5 Reasons why you need to be ready for Mobile Payments. August 10. Available at **http://www.apps-world.net/blog/2011/08/10/5-reasons-why-you-need-to-be-ready-for-mobile-payments/** [accessed 17 February 2014].

[29] Soxlaw (no date) A guide to the Sarbanes Oxley Act. Available at **http://www.soxlaw.com/** [accessed 17 February 2014].

[30] For more information, consult: Jacobs E (no date), Security as a Legal Obligation: About EU Legislation Related to Security and Sarbanes-Oxley in the European Union. Available at **http://www.arraydev.com/commerce/JIBC/2005-08/security.htm** [accessed 17 February 2014].

[31] European Commission (no date) E-money. Available at **http://ec.europa.eu/internal_market/payments/emoney/index_en.htm** [accessed 17 February 2014].

[32] The Basel Group is based at the Bank for International Settlements. It provides a *Survey of Developments in Electronic Money and Internet and Mobile Payments*. Available at **http://www.bis.org/publ/cpss62.pdf** [accessed 17 February 2014].

[33] FATF website. Available at **http://www.fatf-gafi.org/pages/aboutus/** [accessed 10 August 2014].

[34] Richtel M (2002) PayPal and New York in Accord on Gambling. The *New York Times*, August 22. Available at **http://www.nytimes.com/2002/08/22/business/technology-paypal-and-new-york-in-accord-on-gambling.html?src=pm** [accessed 17 February 2014].

[35] Prater C (2009) What you buy, where you shop may affect your credit. Available at **http://www.creditcards.com/credit-card-news/how-shopping-can-affect-credit-1282.php** [accessed 17 February 2014].

[36] Villar R, Knight S, Wolf B (2014) Bitcoin exchange Mt. Gox goes dark in blow to virtual currency. Available at **http://www.reuters.com/article/2014/02/25/us-mtgox-website-idUSBREA1O07920140225** [accessed 10 August 2014].

[37] OECD (1999) Guidelines for Consumer Protection in the Context of Economic Commerce. Available at **http://www.oecd.org/internet/consumer/oecdguidelinesforconsumerprotectioninthecontextofelectroniccommerce1999.htm** [accessed 17 February 2014].

[38] OECD (2003) Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices. Available at **http://www.oecd.org/sti/consumer/oecdguidelinesforprotectingconsumersfromfraudulentanddeceptivecommercialpracticesacrossborders2003.htm** [accessed 17 February 2014].

[39] Better Business Bureaus website. Available at **http://www.bbb.org/us/cbbb/** [accessed 17 February 2014].

[40] European Union (no date) Regulation (EC) No 44/2001 (Brussels I Regulation). Available at **http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32001R0044** [accessed 11 August 2014].

[41] European Union (no date) Regulation (EU) No 1215/2012 (Recast Brussels I Regulation). Available at **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:351:0001:0032:en:PDF** [accessed 11 August 2014].

[42] The Gallup Organisation (2013) *Consumer attitudes towards cross-border trade and consumer protection. Analytical Report.* Flash Eurobarometer. Available at **http://ec.europa.eu/public_opinion/flash/fl_358_sum_en.pdf** [accessed 14 August 2014].

[43] UNCITRAL (1980) UN CISG. Available at **http://www.uncitral.org/uncitral/uncitral_texts/sale_goods/1980CISG.html** [accessed 17 February 2014].

[44] Maastricht Economic Research Institute on Innovation and Technology (MERIT) (1999). Cybertax. Available at **www.merit.unu.edu/publications/rmpdf/1998/rm1998-020.pdf** [accessed 17 February 2014].

[45] Collin P, Colin N (2013) *Mission d'expertise sur la fiscalité de l'économie numérique.* Available at **http://www.redressement-productif.gouv.fr/files/rapport-fiscalite-du-numerique_2013.pdf** [accessed 10 August 2014].

[46] For a discussion on various aspects of taxation policy and the Internet, please consult: Cockfield AJ (2001) Transforming the Internet into a Taxable Forum: A Case Study in E-Commerce Taxation, 85 *Minn. L. Rev.* 1171, 1235-1236; Morse EA (1997) State Taxation of Internet Commerce: Something New under the Sun? 30 *Creighton L. Rev.* 1113, 1124-1227; Williams WR (2001) The Role of Caesar in the Next Millennium? Taxation of E-Commerce: An Overview and Analysis, 27 Wm *Mitchell L. Rev.* 1703, 1707.

[47] Internet Tax Freedom Act. Available at **http://legacy.gseis.ucla.edu/iclp/itfa.htm** [accessed 17 February 2014].

[48] Mazerov M (2007) Making the 'Internet Tax Freedom Act' permanent could lead to a substantial revenue loss for states and localities. Available at **http://www.cbpp.org/7-11-07sfp.htm** [accessed 17 February 2014].

[49] The Ottawa Taxation Principles are: Neutrality, Efficiency, Certainty and simplicity, Effectiveness and fairness, Flexibility. See OECD (2003) Implementation of the Ottawa Taxation Framework Conditions. The 2003 Report. Available at **http://www.oecd.org/tax/administration/20499630.pdf** [accessed 17 February 2014].

[50] For a more detailed explanation of these three approaches, please consult: ILPF (no date) Survey of International Electronic and Digital Signature Initiatives. Available at **http://www.ilpf.org/groups/survey.htm#IB** [accessed 17 February 2014].

[51] European Commission (1999) Directive on Electronic Signatures. Available at **http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:en:HTML** [accessed 17 February 2014].

[52] European Commission (2006) Report on the Operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures. Available at **http://eur-lex.europa.eu/LexUriServ/%20LexUriServ.do?uri=COM:2006:0120:FIN:EN:PDF** [accessed 17 February 2014].

[53] UNCITRAL (2001) Model Law on Electronic Signatures. Available at **http://www.uncitral.org/uncitral/uncitral_texts/electronic_commerce/2001Model_signatures.html** [accessed 17 February 2014].

[54] More information on GUIDEC elaboration can be found on the ICC dedicated webpage. Available at **http://www.iccwbo.org/policy/ebitt/id2340/index.html** [accessed 17 February 2014].

[55] Longmuir G (2000) *Privacy and Digital Authentication.* Available at **http://caligula.anu.edu.au/~gavin/ResearchPaper.htm** [accessed 17 February 2014]. This paper focuses on the personal, community, and governmental aspects of the need for authentication in a digital world.

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

- Will the Internet reduce or broaden the existing divide between developed and developing worlds?
- How and when will developing nations be able to reach the digital levels of more industrially developed countries?

The answers to these and other questions require an analysis of the relevance of development within the context of Internet governance. Almost every Internet governance issue has a developmental aspect:

- The existence of a telecommunication infrastructure facilitates access, the first precondition for overcoming the digital divide.
- The current economic model for Internet access, which places a disproportionate burden on those developing countries that have to finance access to backbones based in developed countries.
- The global regulation of intellectual property rights, which directly affects development, because of the reduced opportunity of developing countries to access knowledge and information online.

The developmental aspect of WSIS has been frequently repeated, beginning with the first 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'.[1] The WSIS Geneva Declaration and Plan of Action highlighted development as a priority and linked it to the UN Millennium Declaration[2] and its promotion of access of all countries to information, knowledge, and communication technologies for development.

With the link to the millennium development goals (MDGs),[3] WSIS is strongly positioned in the development context.

This axis of concern was continued within the IGF, where the development theme was highlighted starting with the first meeting in Athens (2006) and continued to be present with dedicated workshops and even a main session in Vilnius (2010). Development-related concerns were among the top five most frequently raised issues in the context of the debate on the continuation of the IGF, notably improving participation from developing countries and increasing the priority given to development.[4]

How does ICT affect the development of society?

The main dilemmas about ICT and development were summarised in an article in *The Economist*,[5] which proposes arguments for and against the thesis that ICT provides specific impetus for development.

Table 3

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. ● ICT quickly diffuses across borders compared to earlier technologies. Previous technologies (railways and electricity) took decades to spread to developing countries, but ICT is advancing in leaps and bounds. ● ICT offers the opportunity to leapfrog old technologies by skipping intermediate stages, such as copper wires and analogue telephones, and encourages development. ● ICT's propensity to reduce the optimal size of a firm in most industries is much closer to the needs of developing countries.

The digital divide

The digital divide can be defined as a rift between those who, for technical, political, social, or economic reasons, have access and capabilities to use ICT/Internet, and those who do not. Various views have been put forward about the size and relevance of the digital divide. Digital divide(s) exist at different levels: within countries and between countries, between rural and urban populations, between the old and the young, as well as between men and women. The OECD refers to the digital divide as 'the gap between individuals, households, businesses and geographic areas at different socioeconomic levels with regard both to their opportunities to access information and communication technologies (ICTs) and to their use of the Internet for a wide variety of activities'.[6]

Digital divides are not independent phenomena. They reflect existing broad socio-economic inequalities in education, healthcare, capital, shelter, employment, clean water, and food. This was clearly stated by the G8 Digital Opportunity Task Force (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.'[7]

Is the digital divide widening?

ICT/Internet developments leave the developing world behind at a much faster rate than advances in other fields (e.g. agricultural or medical techniques) and, as the developed world has the necessary tools to successfully use these technological advances, the digital divide appears to be continuously and rapidly widening. This is frequently the view expressed in various highly regarded documents, such as the United Nations Development Programme (UNDP) Human Development Reports and the ILO Global 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 the available bandwidth should be replaced with a focus on the broader impact of ICT/Internet on societies in developing countries. Frequently quoted examples are the digital successes of Brazil, India, and China. However, the criteria for assessing the digital divide gaps are also changing and becoming more complex in order to better capture the development realities. Current assessments take into account aspects like ICT readiness and overall ICT impact on society. The World Economic Forum has developed the Networked Readiness Index (NRI) as a new approach in measuring the Internet-level of countries worldwide.[8] It also provides new perspectives on how the digital divide is addressed.

Universal access

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

Unlike universal access at global level, in some countries universal access is a well-developed economic and legal concept. Providing telecommunication access to all citizens has been the basis of US telecommunication policy. The result has been a well-developed system of various policy and financial mechanisms, the purpose of which is to subsidise access costs in remote areas and regions with high connection costs. The subsidy is financed by regions with low connection costs, primarily the big cities. The EU has also taken a number of concrete steps towards achieving universal access by promoting policies to ensure every citizen has access to basic communication services, including Internet connection, and enacting specific regulations thereof.[9]

Strategies for overcoming the digital divide

The technologically centred development theory, which has dominated policy and academic circles over the past 50 years, argues that development depends on the availability of technology. The more technology … the more development. However, this approach failed in many countries (mainly former socialist countries) where it became obvious that the development of society is a much more complex process. Technology is a necessary but not self-sufficient precondition for development. Other elements include a regulatory framework, financial support, available human resources, and other sociocultural 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

Access to the Internet is one of the main challenges to overcoming the digital divide. The Internet penetration rate in 2012 in Africa was 16.6%, compared to 78.6% in North America or 63.2% in Europe, but it registered the highest growth in the last decade.[10] There are two main aspects related to access to the Internet in developing countries. First is access to international Internet backbones. Second is connectivity within developing countries.

Access to international Internet backbones depends mainly on the availability of submarine fibre-optic cables. For a long time, only Western Africa, as far as South Africa, was serviced by submarine cable SAT-3. East Africa has much faster access with the East African Submarine Cable System (EASSy) which began operation in July 2010. It creates a digital ring around Africa which substantially increases the available Internet bandwidth for the African continent.

Small and remote islands face similar challenges in accessing the Internet, as many depend on expensive satellite connectivity. Efforts are underway to find the most efficient solutions for connectivity in such areas.[11]

Another solution for improved access is the introduction of Internet exchange points (IXPs) which keep local traffic within the country and reduce both usage and cost of international bandwidth. IXPs are technical facilities through which different ISPs exchange Internet traffic through peering (without paying). IXPs are usually established in order to keep Internet traffic within smaller communities (e.g. city, region, country), avoiding unnecessary routing over remote geographical locations. IXPs can also play an important role in reducing the digital divide. Still, many developing countries do not have IXPs, which means a considerable part of traffic between the clients within the country is routed through another country. This increases the volume of long-distance international data traffic and the cost of providing Internet service. Various initiatives seek to establish IXPs in developing countries.[12] One that has achieved considerable success is that of the African Internet Service Provider Association, which established several IXPs in Africa.

Connectivity within developing countries is another major challenge. The majority of Internet users were concentrated in major cities. Rural areas usually had no access to the Internet. The situation started changing with the rapid growth of mobile telephony and wireless communication. 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 context, the radio spectrum policies are of utmost importance in ensuring spectrum availability and creating the conditions of an open wireless Internet that can be shared among users. 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 ITU through its Telecommunication Development Sector (ITU-D).

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

When an end-user in Africa sends an e-mail to a correspondent in Europe or the USA, it is the African ISP who bears the cost of international connectivity from Africa to the USA. Conversely, when a European end-user sends an e-mail to Africa, it is still the African ISP who bears the cost of international connectivity, and ultimately the African end-user who bears the brunt by paying higher subscriptions.

The main argument in discussions about changes to the current system of Internet charges uses the analogy of the telephone financial settlement system, which shares the cost and income between communication end-points. However, Geoff Huston argues that this analogy is not sustainable. In the telephony system, only one clearly identifiable commodity[13] – a phone call establishing human conversation between two telephone sets – has a price. The Internet does not have an equivalent, single commodity; it has packets, which take different routes through the network. This fundamental difference makes this analogy inappropriate. It is also the main reason why the telephone financial settlement model cannot be applied to the Internet.

The ITU initiated discussions on possible improvements to the current system for the settlement of Internet expenses, with the main objective of having a more balanced distribution of costs for Internet access. Due to opposition from developed countries and telecom operators, the adopted ITU Recommendation D. 50, is practically ineffective.[14] Unsuccessful attempts were also made to introduce this issue during WTO negotiations. The need for adjustments in interconnection charges was reiterated in the WSIS final documents and in the WGIG report.

Financial support

During the WSIS process, the importance of financial support for bridging the digital divide was clearly recognised. One idea proposed at WSIS was the establishment of a UN-administered Digital Solidarity Fund to help technologically disadvantaged countries build telecommunication infrastructures. However, the proposal to establish a Digital Solidarity Fund did not garner broad support from the developed countries, which favoured direct investment instead of the establishment of a centralised development fund.

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

Sociocultural aspects

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

The existence of communications infrastructure is useless unless people possess the means (devices) and the knowledge (ICT literacy) to access and benefit from the Internet. International initiatives and organisations such as One Laptop per Child or Computer Aid International aim at providing refurbished and low-cost equipment to under-served communities in developing countries. Local initiatives to provide affordable computer devices took off as well, but challenges still remain with respect to performance.[15]

For developing countries, one of the main issues has been brain drain, described as the movement of highly skilled labour from developing to developed countries. Through brain drain, developing countries lose out in a number of ways. The main loss is in skilled labour. Developing countries also lose their investment in the training and education of the migrating skilled labour.

It is likely that brain drain will continue, given the various employment/emigration schemes that have been introduced in the USA and other developed countries in order to attract skilled, mainly ICT-trained, labour.

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

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

Policy and institutional aspects

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

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

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

Institutionally speaking, one of the first steps is to establish independent and professional telecommunication regulatory authorities. Experience from developed countries shows that solid regulators are a precondition for fast growth in telecommunication infrastructure. In developing countries, the development of regulatory authorities is at a very early stage. Regulatory authorities are generally weak, lack independence, and are often part of a system in which state-owned telecom operators are influential in regulatory and political processes.

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

Endnotes

[1] United Nations General Assembly [UNGA] (2002) Resolution 56/183. *World Summit on the Information Society* (A/RES/56/183). Available at **http://www.itu.int/wsis/docs/background/resolutions/56_183_unga_2002.pdf** [accessed 24 February 2014].

[2] United Nations (2000) Millennium Declaration. Available at **http://www.un.org/millennium/declaration/ares552e.htm** [accessed 24 February 2014].

[3] United Nations (no date) Millennium Development Goals. Available at **http://www.un.org/millenniumgoals/** [accessed 24 February 2014].

[4] auDA (no date) Continuation of the Internet Governance Forum. Analysis of the Note of the Secretary-General. Available at **http://www.intgovforum.org/cms/2010/contributions/Open%20Consultation%20on%20Enhanced%20Cooperation%20-%20auDA%20submission.pdf** [accessed 24 February 2014].

[5] *The Economist* (2000) A survey of the new economy: Falling through the Net? For the developing world, IT is more of an opportunity than a threat. Available at **http://www.economist.com/node/375645** [accessed 24 February 2014].

[6] OECD (2001) *Understanding the Digital Divide.* p. 5. Available at **http://www.oecd.org/internet/ieconomy/1888451.pdf** [accessed 24 February 2014].

[7] G8 (2001) *Digital Opportunities for All: Meeting the Challenge*. Report of the Digital Opportunity Task Force (DOT Force) including a proposal for a Genoa Plan of Action. Available at **http://www.g7.utoronto.ca/summit/2001genoa/dotforce1.html** [accessed 24 February 2014].

[8] WEF (2013) *Global Information Technology Report*. Available at **http://www.weforum.org/reports/global-information-technology-report-2013** [accessed 10 August 2014].

[9] European Union [EU] (no date) Universal Service. Available at **http://ec.europa.eu/digital-agenda/en/universal-service** [accessed 24 February 2014].

[10] Internet World Stats (2012) Internet Usage Statistics. The Internet Big Picture. Available at **http://www.internetworldstats.com/stats.htm** [accessed 24 February 2014].

[11] For more information on the Pacific Islands situation, see the Economic and Social Commission for Asia and Pacific (2014). Available at **http://www.unescap.org/about** [accessed 28 March 2014].

[12] For a study on the impact of IXPs implementation in Kenya and Nigeria, see Internet Society (no date) Internet exchange points (IXPs). Available at **http://internetsociety.org/what-we-do/issues/internet-exchange-points-ixps** [accessed 24 February 2014].

[13] Huston G (2005) Where's the Money? Internet Interconnection and Financial Settlement *The ISP Column*, January 2005, Internet Society, pp. 7-9. Available at **http://www.potaroo.net/ispcol/2005-01/interconn.pdf** [accessed 24 February 2014].

[14] One of the limitations of negotiating this issue between governments is that most interconnection agreements are concluded between private telecommunication operators. They are often confidential. ITU recommendations are available at **http://www.itu.int/rec/T-REC-D.50/e** [accessed 10 August 2014].

[15] India announced the launch of a government-subsidised tablet computer of only $35, according to *BBC News South Asia* (2011) India launches Aakash tablet computer priced at $35. 5 October. Available at **http://www.bbc.co.uk/news/world-south-asia-15180831** [accessed 24 February 2014].

Section 6

The sociocultural basket

The sociocultural basket

The Internet has made a considerable impact on the social and cultural fabric of modern society. It is difficult to identify any segment of our social life that is not affected by it. It introduces new patterns of social communication, breaks down language barriers, and creates new forms of creative expressions – to name but a few of its effects. Today, the Internet is as much a social phenomenon as it is a technological one.

Human rights

A basic set of Internet-related human rights includes privacy; freedom of expression; the right to receive information; various rights protecting cultural, linguistic, and minority diversity; and the right to education. It is not surprising that human-rights-related issues have very often been hotly debated in both WSIS and IGF processes. While human rights are usually explicitly addressed, they are also involved in cross-cutting issues appearing when dealing with net neutrality (right to access, freedom of expression, anonymity), cybersecurity (observing human rights while carrying out cybersecurity and protection activities), content control, etc. The Snowden revelations of mass surveillance triggered the diplomatic process on online privacy within the UN General Assembly and the UN Human Rights Council.

Online vs offline human rights

The principle that the same human rights that people enjoy *offline* must also be protected *online* has been firmly established by the UN General Assembly and UN Human Rights Council resolutions. The Association for Progressive Communications (APC) in the Internet Rights Charter argues that Internet-related human rights are strongly embodied in the UN human rights system based on the Universal Declaration of Human Rights (UDHR) and other related instruments.[1] Online human rights specificities are related to their implementation.

Right to access the Internet

Estonia was the first country to legally guarantee the right to access the Internet through a universal services legislation.[2] As of July 2010 all citizens in Finland have the right to a one-megabit broadband connection.[3] Yet the right to Internet access is argued more in relation to the freedom of expression and information than the actual speed of Internet connection. And opinions are still nuanced regarding a firm worldwide recognition of access to the Internet as a human right, since access involves different valences – from access to infrastructure to access to content – as the United Nations Human Rights Council report points out.[4]

Still, there are reluctant opinions to considering broadband as a basic human right, when there are people still fighting for clean water, medical attention, and food. Will this take effort and resources away from addressing more basic human rights?

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

One of the main players in the field of human rights and the Internet is the CoE. The CoE is the core institution dealing with pan-European human rights, with the Convention for the Protection of Human Rights and Fundamental Freedoms[5] as its main instrument. Since 2003, the CoE has adopted several declarations highlighting the importance of human rights on the Internet.[6] The CoE is also the depository of the Convention on Cybercrime[7] as the main global instrument in this field. This may position it as one of the key institutions in finding the right balance between human rights and cybersecurity considerations in the future development of the Internet.

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

Online freedom of expression has featured high on the diplomatic agenda in the last few years; it is on the agenda of the UN Council of Human Rights. Freedom of expression on the Internet has also been discussed at numerous international conferences. The discussion on online freedom of expression has been a contentious policy area. This is one of the fundamental human rights, usually appearing in the focus of discussions on content control and censorship. In the UN Universal Declaration of Human Rights,[8] freedom of expression (Article 19) is counterbalanced by the right of the state to limit freedom of expression for the sake of morality, public order, and general welfare (Article 29). Thus, both the discussion and implementation of Article 19 must be put in the context of establishing a proper balance between two needs. This ambiguous situation opens many possibilities for different interpretations of norms and ultimately different implementations. The controversy around the right balance between Articles 19 and 29 in the real world is mirrored in discussions about achieving this balance on the Internet.

Freedom of expression is the particular focus of human rights NGOs such as Amnesty International and Freedom House. Freedom House evaluates the level of Internet and mobile phone freedom experienced by average users in sample countries around the world. The latest study notes that Internet freedom worldwide is in decline, with 34 out of 60 countries experiencing a negative trajectory, driven by broad surveillance, new laws controlling web content, and growing arrests of social-media users. However, the study also notes that activists are becoming more effective at raising awareness of emerging threats and, in several cases, have helped forestall new repressive measures.[9]

Rights of people with disabilities[10]

According to UN estimates, there are 1 billion people with disabilities in the world.[11] The factors that contribute to increasing this number include war and destruction by natural as well as human causes; poverty and unhealthy living conditions; and the absence of knowledge about disability, its causes, prevention, and treatment.

The Internet provides new possibilities for social inclusion of people with disabilities. In order to maximise technological possibilities for people with disabilities, there is a need to develop the necessary Internet governance and policy framework. The main international instrument in this field is the Convention on the Rights of Persons with Disabilities,[12] adopted by UN in 2006 and signed by 159 countries (April 2014), which establishes rights that are now in the process of being included in national legislation, which will make them enforceable.

Awareness of the need for technological solutions that include people with disabilities is increasing with the work of organisations that teach and foster support for the disabled community, such as the IGF Dynamic Coalition on Accessibility and Disability,[13] the Internet Society Disability and Special Needs Chapter,[14] and the International Center for Disability Resources on the Internet.[15]

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

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

In the field of Internet governance, the main focus is on web content, as it is in rapid development and constitutes a kind of infrastructure. Many web applications do not comply with accessibility standards due to a lack of awareness or perceived complexity and high costs (which is far from today's reality). International standards in web accessibility are developed by W3C within its Web Accessibility Initiative.[16]

Content policy

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

- Content that has a global consensus for its control. Included here are child pornography, [17] justification of genocide, and incitement or organisation of terrorist acts.
- Content that is sensitive for particular countries, regions, or ethnic groups due to their particular religious and cultural values. Globalised online communication poses challenges for local, cultural, and religious values in many societies. Most content control in Middle Eastern and Asian countries is officially justified by the protection of specific cultural values. This often means that access to pornographic and gambling websites is blocked.[18]
- Political censorship on the Internet. Reporters without Borders issues annual reports on freedom of information on the Internet. Till 2012 the report used to list countries that run censorship and surveillance programmes. The 2014 Report focuses on institutions that run censorship and surveillance activities.[19]

How content policy is conducted

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

Governmental filtering of content

Governments that filter access to the content usually create an Internet Index of websites blocked for citizen access. Technically speaking, filtering utilises mainly router-based IP blocking, proxy servers, and DNS redirection.[20] Filtering of content occurs in many countries. In addition to the countries usually associated with these practices, such as China, Saudi Arabia, and Singapore, other countries are increasingly adopting the practice.

Private rating and filtering systems

Faced with the potential risk of the disintegration of the Internet through the development of various national barriers (filtering systems), W3C and other like-minded institutions made proactive moves proposing the implementation of user-controlled rating and filtering systems.[21] In these systems, filtering mechanisms can be implemented by software on personal computers or at server level controlling Internet access.[22]

Content filtering based on geographical location

Another technical solution related to content is geo-location software, which filters access to particular web content according to the geographic or national origin of users. The Yahoo! case was important in this respect, since the group of experts involved, including Vint Cerf, indicated that in 70–90% of cases Yahoo! could determine whether sections of one of its websites hosting Nazi memorabilia were accessed from France.[23] This assessment helped the court come to a final decision, which requested Yahoo! to filter access from France to Nazi memorabilia. Since the 2000 Yahoo! case, the precision of geo-location has increased further through the development of highly sophisticated geo-location software.

Content control through search engines

The bridge between the end-user and Web content is usually a search engine. The filtering of searches was a source of tension between Google and Chinese authorities[24] which culminated with the decision taken by Google in January 2010 to redirect searches performed on Google.cn to its Hong Kong-based servers. However, later that year, Google reversed its decision under pressure of refusal by the Chinese government to renew its Internet Content Provider licence.[25]

The risk of filtering of search results, however, doesn't come only from the governmental sphere; commercial interests may interfere as well, more or less obviously or pervasively. Commentators have started to question the role of search engines (particularly Google, considering its dominant position in users' preferences) in mediating user access to information and to warn about their power of influencing users' knowledge and preferences.[26]

Web 2.0 challenge: users as contributors

With the development of Web 2.0 platforms – blogs, document-sharing websites, forums, and virtual worlds – the difference between the user and the creator has blurred. Internet users can create large portions of Web content, such as blog posts, videos, and photo galleries. Identifying, filtering, and labelling 'improper' websites is becoming a complex activity. While automatic filtering techniques for texts are well developed, automatic recognition, filtering, and labelling of visual content are still in the early development phase.[27]

One approach, used on a few occasions by Morocco, Pakistan, Turkey, and Tunisia, is to block access to YouTube and Twitter throughout the country. This maximalist approach, however, results in unobjectionable content, including educational material, being blocked. During the Arab Spring events, governments took the extreme measure of cutting Internet access completely in order to hinder communication via social network platforms.[28]

The need for an appropriate legal framework

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

International initiatives

At international level, the main initiatives arise in European countries with strong legislation in the field of hate speech, including anti-racism and anti-Semitism. European regional institutions have attempted to impose these rules on cyberspace. The primary legal instrument addressing the issue of content is the CoE Additional Protocol to the Convention on Cybercrime,[29] concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (2003). On a more practical level, the EU introduced the EU Safer Internet programme which includes the following main points:

- Setting up a European network of hotlines to report illegal content.
- Encouraging self-regulation.
- Developing content rating, filtering, and benchmark filtering.
- Developing software and services.
- Raising awareness of the safer use of the Internet.[30]

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

The issues

Content control vs freedom of expression

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

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

Illegal offline – illegal online

As with human rights, the dominant view is that rules of the offline world apply to the Internet when it comes to content policy.

One of the arguments of the cyber approach to Internet regulation is that quantity (intensity of communication, number of messages) makes a qualitative difference. In this view, the problem of hate speech is not that no regulation against it has been enacted, but that the sharing and spreading through the Internet makes it a different kind of legal problem. More individuals are exposed and it is difficult to enforce existing rules. Therefore, the difference that the Internet brings is mainly related to problems of enforcement, not to the rules themselves.

The effectiveness of content control

In discussions on Internet policy, one of the key arguments is that the decentralised nature of the Internet can bypass censorship. 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. Lessig provides a concise statement of this problem: 'A regulation need not be absolutely effective to be sufficiently effective.'[31]

Who should be responsible for content policy?

The main players in the area of content control are parliaments and governments. They prescribe what content should be controlled and how. ISPs, as Internet gateways, are commonly held responsible for implementation of content filtering, either according to government prescriptions or to self-regulation (at least in regard to issues of broad consensus, such as child pornography). Some groups of users, such as parents, are keen to introduce a more efficient content policy to protect children. Various rating initiatives help parents to find child-friendly content. New versions of Internet browser software usually include many filtering options. Private companies and universities also perform content control. In some cases, content is controlled through software packages; for example, the Scientology movement has distributed a software package, Scienositter, to members, preventing access to websites critical of Scientology.[32]

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 physical attendance in class.

Traditionally, education has been governed by national institutions. The accreditation of educational institutions, the recognition of qualifications, and quality assurance are all governed at national level. However, cross-border education requires the development of new governance regimes. Many international initiatives aim at filling the governance gap, especially in areas such as quality assurance and the recognition of academic degrees.

The issues

WTO and education

One controversial issue in the WTO negotiations is the interpretation of Articles I (3)b and (3)c of GATS,[33] which specify exceptions from the free trade regime for government-provided services. According to one view, supported mainly by the USA and the UK, these exceptions should be treated narrowly, *de facto* enabling free trade in higher education. This view is predominantly governed by interests of the English-speaking educational sector to gain global market coverage in education, and has received considerable opposition from many countries.[34]

The forthcoming debate, likely to develop within the context of the 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.

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. This aspect prompted education organisations to start to develop standards and guidelines for evaluating the design and the content of lectures delivered online.[35]

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 global level.

The EU has developed a regulatory framework with the European Credit Transfer and Accumulation System (ECTS).[36] The Asia-Pacific region has introduced its own regional model for the exchange of students and a related credit system – the University Mobility in Asia and the Pacific (UMAP) programme.[37]

The standardisation of online learning

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

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

Child safety online[38]

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

The issues

Cyber-bullying

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

Abuse and sexual exploitation

Harmful conduct targeting minors can be particularly dangerous when conducted by adults. The masked identity is one of the most frequent approaches undertaken by paedophiles on the Internet – while pretending to be peers, these online predators collect information and steadily groom the child, easily managing to win the child's trust, even aiming to establish a physical meeting. The virtual conduct thereby transforms to real contact and can go as far as the abuse and exploitation of children, paedophilia, the solicitation of minors for sexual purposes, and even child trafficking.

Violent games

The impact of violent games on the behaviour of young people is being widely debated. The most infamous games involve sophisticated weapons (showing features of real weapons, and/or other fantasy features) and bloodshed, and are usually tagged as 'stress eliminators'. The top 10 best-selling games for different hardware platforms, including Microsoft Xbox, Nintendo DS, Nintendo Wii, PC, Playstation, were dominated by action/violent games.[39]

Addressing the challenges

The major challenge that educators and parents are facing in protecting children online is the fact that the 'digital natives' are much more knowledgeable in how to use ICT – they know more than their parents, yet they understand less. Close cooperation between peers – parents, educators, and the community – is most important for developing initiatives for safeguarding children in computer-mediated environments.

To raise awareness among the stakeholders, the European Commission has launched the InSafe project[40] as a European network of e-safety awareness nodes, providing awareness-building materials for parents and educators in several languages free for download and dissemination. The Polish media campaign on cyber-bullying resulted in sets of video clips and an e-learning course on Internet safety for kids. The NetSafe initiative in New Zealand, founded in 1998, is among the first national initiatives on Internet safety which gathers key stakeholders including ministries, the business sector, and the media.

A much-needed step beyond awareness building and training of youth, parents, and educators is capacity building in the area of Internet safety, targeted at the multistakeholder composition of policymakers: government officials, business entities, media, academia, think-tanks, and non-governmental organisations, etc. Various international organisations are discussing possible models of cooperation in establishing such programmes, among them the CoE, the ITU, CPI, and DiploFoundation.

On a longer time scale, educational curriculum updates are also needed, to include in-school programmes on Internet safety issues such as protecting personal privacy and security, minding personal reputations and those of others, ethics, reporting abuse, transferring real-life morals and skills to the online world, etc. Several such initiatives exist worldwide, such as Cyber Smart!,[41] iKeepSafe,[42] i-Safe,[43] and NetSmartz.[44]

Synchronised national and international legal and policy mechanisms are an indispensable component as well. One example is the successful pan-European Prague Declaration for a Safer Internet for Children adopted at the Ministerial Conference (Prague, April 2009).[45] The ITU's Global Cybersecurity Agenda (GCA)[46] presents the Child Online Protection (COP) initiative as its integral part. There are many other international forums where child protection is a debated issue high on the agenda, including the IGF with its Dynamic Coalition on Child Online Safety.

International cooperation in the field of child protection has been successful for a long time in the area of international emergency and hotlines. Some of the successful initiatives are:

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

Multilingualism and cultural diversity

Since its early days, the Internet has been a predominantly English-language medium. According to some statistics, approximately 56% of Web content is in English,[47] whereas 75% of the world's population does not speak English.[48] This situation has prompted many countries to take concerted action to promote multilingualism and to protect cultural diversity. The promotion of multilingualism is not only a cultural issue; it is directly related to the need for the further development of the Internet.[49] If the Internet is to be used by wider parts of society and not just national elites, content must be accessible in more languages.

The issues

Non-Roman alphabets

The promotion of multilingualism requires technical standards that facilitate the use of non-Roman alphabets. One of the early initiatives related to the multilingual use of computers was undertaken by the Unicode Consortium – a non-profit institution that develops standards to facilitate the use of character sets for different languages.[50] In their turn, ICANN and the IETF took an important step in promoting Internationalised Domain Names (IDN). IDN facilitate the use of domain names written in Chinese, Arabic, and other non-Latin alphabets.

Machine translation

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

Appropriate government frameworks

The promotion of multilingualism requires appropriate governance frameworks. The first element of governance regimes has been provided by organisations such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO), which has instigated many initiatives focusing on multilingualism, including the adoption of important documents, such as the Universal Declaration of Cultural Diversity.[51] Another key promoter of multilingualism is the EU, since it embodies multilingualism as one of its basic political and working principles.[52]

The evolution and wide usage of Web 2.0 tools, allowing ordinary users to become contributors and content developers, offers an opportunity for greater availability of local content in a wide variety of languages. Nevertheless, without a wider framework for the promotion of multilingualism, the opportunity might end up creating an even wider gap, since users feel the pressure of using the common language in order to reach a broader audience.

Global public goods

The concept of global public goods can be linked to many aspects of Internet governance. The most direct connections are found in areas of access to the

Internet infrastructure, protection of knowledge developed through Internet interaction, protection of public technical standards, and access to online education.

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

One of the key features of the Internet is that through worldwide interaction of users, new knowledge and information are produced. Considerable knowledge has been generated through exchanges on mailing lists, social networks, and blogs. With the exception of creative commons,[53] there is no mechanism to facilitate the legal use of such knowledge. Left in a legal uncertainty, it is made available for modification and commercialisation. This common pool of knowledge, an important basis of creativity, is at risk of being depleted. The more Internet content is commercialised, the less spontaneous exchanges may become. This could lead towards reduced creative interaction.

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

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

The issues

The balance between private and public interests

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

Protecting the Internet as a global public good[54]

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 international level to global public goods. A public good has two critical properties: non-rivalrous consumption and non-excludability. The former stipulates that the consumption of one individual does not detract from that of another; the latter, that it is difficult, if not impossible, to exclude an individual from enjoying the good. Access to Web-based materials and many other Internet services fulfils both criteria.

Endnotes

[1] The *APC Internet Rights Charter* includes Internet access for all; freedom of expression and association; access to knowledge; shared learning and creation – free and open source software and technology development; privacy, surveillance and encryption; governance of the Internet; awareness, protection and realisation of rights. Available at **http://www.apc.org/en/node/5677** [accessed 10 August 2014].

[2] Borg-Psaila S (2011) Right to access the Internet: the countries and the laws that proclaim it. Available at **http://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it** [accessed 10 August 2014].

[3] CNN Tech (2010) First nation makes broadband access a legal right. Available at **http://articles.cnn.com/2010-07-01/tech/finland.broadband_1_broadband-access-internet-access-universal-service?_s=PM:TECH** [accessed 10 August 2014].

[4] UN General Assembly (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. Available at **http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf** [accessed 10 August 2014]. For a discussion of the UN report see Wagner A (2012) Is Internet access a human right? *The Guardian.* Available at **http://www.guardian.co.uk/law/2012/jan/11/is-internet-access-a-human-right** [accessed 10 August 2014].

[5] Council of Europe (2010) Convention for the Protection of Human Rights and Fundamental Freedoms. Available at **http://conventions.coe.int/treaty/en/treaties/html/005.htm** [accessed 10 August 2014].

[6] The Council of Europe adopted the following main declarations of relevance for human rights and the Internet: The Declaration on Freedom of Communication on the Internet *(28* May *2003).* Available at **https://wcd.coe.int/ViewDoc.jsp?id=37031** [accessed 10 August 2014]; The Declaration of Human Rights and the Rule of Law in the Information Society *(13* May 2005). Available at **https://wcd.coe.int/ViewDoc.jsp?id=849061** [accessed 10 August 2014]. The Declaration on the Digital Agenda for Europe *(29* September *2010).* Available at **https://wcd.coe.int/ViewDoc.jsp?Ref=Decl%2829.09.2010_1%29&Language=lanEnglish&Ver=original** [accessed 10 August 2014].

[7] Council of Europe (2001) Convention on Cybercrime. Available at **http://conventions.coe.int/Treaty/en/Treaties/html/185.htm** [accessed 30 April 2014].

[8] United Nations (no date) The Universal Declaration of Human Rights. Available at **http://www.un.org/en/documents/udhr/** [accessed 30 April 2014].

[9] Freedom House (2013) *Freedom on the Net. A Global Assessment of Internet and Digital Media*. Available at **http://freedomhouse.org/report/freedom-net/freedom-net-2013#.Uz7L3VcZes1** [accessed 4 April 2014].

[10] Valuable comments and input were provided by Jorge Plano.

[11] UN Enable (no date) Factsheet on Persons with Disabilities. Available at **http://www.un.org/disabilities/default.asp?id=18** [accessed 4 April 2014].

[12] Convention on the Rights of Persons with Disabilities. Available at **http://www.un.org/disabilities/default.asp?navid=14&pid=150** [accessed 30 April 2014].

[13] IGF, Dynamic coalition on accessibility and disability. Available at **http://www.intgovforum.org/cms/index.php/dynamic-coalitions/80-accessibility-and-disability** [accessed 30 April 2014].

[14] ISOC Disability and Special Needs Chapter. Available at **http://www.isocdisab.org/** [accessed 30 April 2014].

[15] ICDRI. Available at **http://www.icdri.org/** [accessed 30 April 2014].

[16] WAI. Available at **http://www.w3.org/WAI/** [accessed 30 April 2014].

[17] Zick T (1999) Congress, the Internet, and the intractable pornography problem: the Child Online Protection Act of 1998, *Creighton Law Review,* 32, pp. 1147, 1153, 1201. Available at **http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1873&context=facpubs** [accessed 2 April 2014].

[18] For a discussion of Internet gambling, see: Girdwood S (2002) Place your bets ... on the keyboard: Are Internet casinos legal? *Campbell Law Review* 25. Available at **http://scholarship.law.campbell.edu/cgi/viewcontent.cgi?article=1398&context=clr** [accessed 2 April 2014].

[19] Reporters without Borders (2014). Enemies of the Internet. Available at **http://12mars.rsf.org/wpcontent/uploads/EN_RAPPORT_INTERNET_BD.pdf** [accessed 10 August 2014].

[20] The OpenNet Initiative has documented network filtering of the Internet by national governments in over forty countries worldwide. See Noman H and York J (2011) *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011* OpenNet Initiative Bulletin. Available at **http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011** [accessed 2 April 2014].

[21] PICS has now been replaced by POWDER: **http://www.w3.org/2009/08/pics_superseded.html**. Details about POWDER are available at **http://www.w3.org/standards/techs/powder#w3c_all** [accessed 10 August 2014].

[22] For an overview of available filtering types, see the National Academy of Sciences dedicated page available at **http://www.nap.edu/netsafekids/pro_fm_filter.html** [accessed 2 April 2014].

[23] Although Vint Cerf participated in the panel, he objected to the final report, which he said 'did not focus on the flaws or the larger implications of installing online gates'. Source: Guernsey L (2001) Welcome to the world wide web, passport, please? *New York Times,* 15 March 2001. Available at **http://www.nytimes.com/2001/03/15/technology/welcome-to-the-web-passport-please.html?pagewanted=all&src=pm** [accessed 2 April 2014].

[24] Knight W (2002) On-off access for Google in China. *New Scientist Internet edition,* 13 September. Available at **http://www.newscientist.com/article/dn2795-onoff-access-for#.U-fUu2PCfMU** [accessed 8 August 2014].

[25] Drummond D (2010) An update on China, 28 June 2010. The Official Google Blog. Available at **http://googleblog.blogspot.com/2010/06/update-on-china.html** [accessed 2 April 2014].

[26] A good starting point to this debate is Mary Murphy's blog post on DiploFoundation's Internet Governance blog channel and the comments raised upon: *Google...stop thinking for me!* Available at **http://www.diplomacy.edu/blog/googlestop-thinking-me** [accessed 10 April 2012].

[27] Jiang Y (2011) Consumer Video Understanding: A Benchmark Database and An Evaluation of Human and Machine Performance ICMR'11. April 17-20, Trento, Italy. Available at **http://www.ee.columbia.edu/~yjiang/publication/icmr11-consumervideo.pdf** [accessed 2 April 2012].

[28] Crete-Nishihata M and York J (2011) Egypt's Internet Blackout: Extreme Example of Just-in-time Blocking. OpenNet Initiative. Available at **http://opennet.net/blog/2011/01/egypt%E2%80%99s-internet-blackout-extreme-example-just-time-blocking** [accessed 2 April 2014].

[29] Council of Europe (2003) Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Available at **http://conventions.coe.int/Treaty/en/Treaties/html/189.htm** [accessed 30 April 2014].

[30] EU Information Society (no date) Safer Internet action plan. Available at http://**ec.europa.eu/information_society/activities/sip/index_en.htm** [accessed 8 August 2014].

[31] Lessig L (1996) The Zones of Cyberspace. *Stanford Law Review* 48 pp. 1403, 1405.

[32] Steve A (no date) Church of Scientology censors net access for members. Available at **http://www.xenu.net/archive/events/censorship** [accessed 2 April 2012].

[33] GATS. Available at **http://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_01_e.htm#article1A** [accessed 30 April 2014].

[34] For a comprehensive study of the interpretation of GATS related to higher education see Tilak J (2011) *Trade in higher education: The role of the General Agreement on Trade in Services (GATS).* UNESCO: International Institute for Educational Planning, Paris. Available at **http://unesdoc.unesco.org/images/0021/002149/214997e.pdf** [accessed 3 April 2014].

[35] For a sample list of organisations and works dealing with recommendations and standards for e-learning see Bates T (2010) *E-learning quality assurance standards, organizations and research.* Available at **http://www.tonybates.ca/2010/08/15/e-learning-quality-assurance-standards-organizations-and-research/** [accessed 3 April 2014].

[36] European Commission (no date) ECTS. Available at **http://ec.europa.eu/education/tools/ects_en.htm** [accessed 3 April 2014].

[37] UMAP (no date) UMAP. Available at **http://www.umap.org/en/cms/detail.php?id=106** [accessed 3 April 2014].

[38] This text was prepared by Vladimir Radunovic for the advanced thematic course on Cybersecurity (Internet Governance Capacity Building Programme – DiploFoundation).

[39] Reilly J (2012) *The Best-Selling U.S. Games Of 2011.* gameinformer. Available at http://**www.gameinformer.com/b/news/archive/2012/01/12/these-are-the-10-best-selling-u-s-games-in-2011.aspx** [accessed 12 April 2014].

[40] Insafe. Available at **http://www.saferinternet.org/web/guest/home** [accessed 30 April 2014].

[41] CyberSmart. Available at **http://www.cybersmart.org/** [accessed 30 April 2014].

[42] IKeepSafe. Available at **http://www.ikeepsafe.org/** [accessed 30 April 2014].

[43] I-Safe. Available at **http://www.isafe.org/** [accessed 30 April 2014].

[44] NetSmartz. Available at **http://www.netsmartz.org/Parents** [accessed 30 April 2014].

[45] EU2009. Prague Declaration for a Safer Internet for Children. Available at **http://ec.europa.eu/information_society/activities/sip/docs/events/prague_decl.pdf** [accessed 30 April 2014].

[46] ITU (no date) Global Cybersecurity Agenda. Available at **http://www.itu.int/osg/csd/**cybersecurity/gca/ [accessed 30 April 2014].

[47] W3Techs (2014) Usage of content languages for websites. Available at http://**w3techs.com/technologies/overview/content_language/all** [accessed 3 April 2014].

[48] British Council (no date) How many people speak English. Available at **http://www.britishcouncil.org/learning-faq-the-english-language.htm** [accessed 10 August 2014].

[49] For more information regarding multilingualism on the Internet please consult the following study: AlShatti Q, Aquirre R and Cretu V (2007) *Multilingualism – the communication bridge*. DiploFoundation's Internet Governance Research Project, 2006/2007. Available at **http://textus.diplomacy.edu/thina/TxFsetW.asp?tURL=http://textus.diplomacy.edu/thina/txgetxdoc.asp?IDconv=3241** [accessed 3 April 2014].

[50] Unicode Consortium. Available at **http://unicode.org/** [accessed 30 April 2014].

[51] UNESCO (2001) Universal Declaration on Cultural Diversity. Available at http://**portal.unesco.org/en/ev.php-URL_ID=13179&URL_DO=DO_TOPIC&URL_SECTION=201.html** [accessed 30 April 2012].

[52] European Commission (no date) Languages. Available at **http://ec.europa.eu/languages/index_en.htm** [accessed 10 August 2014].

[53] Creative Commons is a non-profit organisation that develops, supports, and stewards legal and technical infrastructure that maximizes digital creativity, sharing, and innovation. Available at **http://creativecommons.org/** [accessed 3 April 2014].

[54] For more information regarding the Internet as a global public good, please consult the following study: Seiiti A and Psaila S (2006) *The Protection of the Public Interest with regards to the Internet*. DiploFoundation's Internet Governance Research Project, 2005/2006. Available at **http://archive1.diplomacy.edu/poolbin.asp?IDPool=128** [accessed 3 April 2014].

Section 7

Internet governance actors

Internet governance actors

At the moment, Internet governance involves a wide variety of actors, or stakeholders, as they are often called. Internet actors include national governments, international organisations, the business sector, civil society, and the technical community (as specified in the Article 49 of the 2005 Tunis WSIS Declaration). While multistakeholderism is adopted as a principle, the main debate is on the specific role of each actor, focusing mainly on the relation between state and non-state actors.

What is the difference between Internet governance and other global policy processes?

In Internet governance, governments had to enter an already existing non-governmental regime, built around the IETF, ISOC, and ICANN. In other policy areas (e.g. climate change, trade, migration), it has been the other way around. Inter-governmental negotiations had to open gradually to non-governmental actors. Since WSIS 2003, most of the time and energy in Internet governance has been dedicated to convergence of non-governmental and traditional diplomatic regimes. This convergence has also been the source of the main controversies.

Governments

The last decade – since the introduction of Internet governance to the global diplomatic agenda in 2003 – has been a learning process for many governments. Even for big and wealthy countries, dealing with Internet governance issues has posed numerous challenges, such as management of the multidisciplinary nature of Internet governance (i.e., technological, economic, and social aspects) and involvement of a wide variety of actors. Many governments have had to simultaneously train officials, develop policy, and actively participate in various international Internet meetings.

National coordination

In 2003, at the beginning of the WSIS process, most countries addressed Internet governance issues through telecommunication ministries, usually those that had been responsible for relations with the ITU. Gradually, as they realised that Internet governance was more than 'wires and cables', governments started involving officials from other ministries, such as those of foreign affairs, culture, media, and justice.

The principal challenge for many governments has been to develop a strategy to gather and effectively coordinate support from non-state actors such as universities, private companies, and NGOs that often have the necessary expertise to deal with Internet governance issues. In the years after WSIS 2003, most big and medium-sized G20 countries have managed to develop sufficient institutional capacity to follow global Internet governance negotiations. Some of them, such as Brazil, have developed an innovative national structure for following the Internet governance debate, involving telecom ministries, the diplomatic service, the business sector, civil society, and academia.[1]

Policy coherence

Given the multidisciplinary nature of Internet governance and the great diversity of actors and policy forums, it is particularly challenging to achieve policy coherence. For example, the question of data protection and privacy is addressed from human rights, trade, standardisation, and security perspectives, among others. Achieving policy coherence in the field of Internet governance requires a flexible form of policy coordination, including horizontal communication between different ministries, the business sector, and other actors.

Cable geo-strategy and policy (in)coherence

The Anglo-French Entente[2] was established in 1904. By establishing close cooperation with Germany, however, the French Telegraph Ministry did not follow the country's foreign policy. The main reason for this was to reduce British dominance in the global cable geo-strategy while laying new telegraph cables in cooperation with Germany. French historian Charles Lesage made the following comment on this policy (in)coherence: 'The prolonged disagreement between the general principles of French diplomacy and the procedures of the telegraphic policies come, I believe, from the fact that in this country, each ministry has its own foreign policy: the Ministry of Foreign Affairs has one, the Ministry of Finance has another.... The Postal and Telegraph Administration also has, from time to time, a foreign policy; as it so happened, in these past few years, without being entirely hostile to England, it demonstrated a strong inclination to Germany.'[3]

Apart from the management challenge, the achievement of policy coherence is usually limited by the existence of competing policy interests. This is especially true in countries with well-developed and diversified Internet economies. For example, net neutrality is one of the issues in which the US government has become involved in a delicate balancing act between the Internet industry (Google, Facebook ,Yahoo!) which supports net neutrality, and the telecommunication/entertainment sector (Verizon and AT&T, Hollywood lobby), which sees net neutrality as an obstacle to developing a new business model based on, for example, faster Internet(s) for delivery of multimedia content.

See **Section 2** for further discussion on network neutrality

The importance of Geneva-based permanent missions

For many governments, their permanent missions in Geneva have been important, if not vital, players in the WSIS and Internet governance processes. Most activities took place in Geneva, home to the ITU, which had the main role in the WSIS processes. The first WSIS took place in Geneva in 2003, where all but one of the preparatory meetings was held, keeping permanent missions based there directly involved. Currently, the IGF Secretariat is based in Geneva and most IGF preparatory meetings are held in the city.

For large and developed countries, the permanent missions were part of the broad network of institutions and individuals that dealt with the WSIS and Internet governance processes. For small and developing countries, permanent missions were the primary and, in some cases, the only players in the processes. Internet governance issues have added to the agenda of the usually small and over-stretched missions of developing countries. In many cases, the same diplomat had to undertake the tasks associated with WSIS along with other issues such as human rights, health, trade, and labour.

Positions of governments

United States

The Internet was developed as part of a US-government-sponsored scientific project. From the origin of the Internet until today, the US government has been involved in Internet governance through various departments and agencies, initially, the Department of Defense, later the National Science Foundation, and most recently the Department of Commerce. The FCC has also played an important role in creating the Internet regulatory framework.

One constant of US government involvement has been its hands-off approach, usually described as a 'distant custodian'. It sets the framework while leaving the governance of the Internet to those directly working with it, mainly the technical community. However, the US government has intervened more directly on a few occasions, as occurred in the mid-1990s when the CORE project could have moved the root server and management of the core Internet infrastructure from the USA to Geneva. This process was stopped by a famous (at least in the history of the Internet) diplomatic note sent by US Secretary of State Madeleine Albright to the ITU Secretary General.[4] In parallel to stopping the CORE initiative, the US government initiated consultations that resulted in the establishment of ICANN.

In 2009, the US Department of Commerce issued the Affirmation of Commitments[5] aimed at withdrawing from the supervisory function of ICANN. The next phase in this process started on 14 March 2014 when the NTIA initiated the process of reviewing the special relationship between the US Department of Commerce and ICANN.[6] The core of this relationship – supervision of the IANA function – should be passed from the US government to some other global arrangement by 30 September 2015. The NTIA announcement sets out requirements that supervision of the IANA function cannot be passed to an inter-governmental body. The outcome of this process will influence the future role of the United States in the global Internet governance.

European Union

The European Union has a unique mix of hard and soft digital power for forging future Internet governance compromise. The EU's hard digital power is based on the attraction of a wealthy 500-million-person market with high Internet penetration (73%).[7] As the concentration of the Internet industry lobby in Brussels shows, this type of hard power matters. By negotiating with the EU on anti-monopoly and data protection issues, Google and Facebook, among others, negotiate with the rest of the world (the EU's arrangements with the Internet industry often inspire other countries and regions to take similar action). In a situation when, for example, Google controls more than 90% of the European search market, the EU is the only international institution that could effectively address the risk of Google's market monopoly.[8]

The EU's soft digital power is based on some sort of digital aikido diplomacy of turning weaknesses into strengths. Namely, the EU does not have any major Internet company since Skype was bought by Microsoft. Paradoxically, this weakness could be turned into a strength in Internet governance.

Without the need to protect the economic interests of the Internet industry, the EU has more freedom to promote and protect public interests (user rights, inclusion, network neutrality). In this way, the EU can become the guardian of

'Internet users', and the promoter of an enabling environment for the growth of the EU's (and the world's) Internet industry. The EU can achieve both ethical and strategic goals, which is not often the case in international politics.

The EU's approach of developing different issue-based alliances has begun to emerge. At WCIT-12, Europe supported the USA; while in discussions about ICANN's status, the EU often allies itself with BRICS and developing countries. On data protection and privacy, the EU's position is close to the position of the Latin American countries. Switzerland and Norway have a close position to the EU on most Internet governance issues.

Brazil

Brazil has been one of the most active countries in global digital politics. As a democratic and developing country with a vibrant digital space, Brazil has great potential to facilitate a compromise between the two camps in the Internet governance debate (inter-governmental and non-governmental). This role became obvious in the aftermath of the Snowden revelations. Brazil took strong diplomatic action. In her speech at the 68th Session of the United Nations General Assembly, Brazilian president Dilma Rousseff made this request: '[t]he United Nations must play a leading role to regulate the conduct of states with regard to these technologies.' In addition, she defined the surveillance as 'a breach of international law' and 'a case of disrespect to the national sovereignty' of Brazil.[9] When it seemed that Brazil was insisting on an inter-governmental approach, President Rousseff shifted back to the middle of the policy spectrum by proposing to co-organise a NETmundial aimed at further developing multistakeholder Internet governance. Brazil had a complex role to play where its main aim was to ensure a successful outcome of the meeting.

On the substantive side, as an example, Brazil did not succeed in achieving stronger language in the NETmundial Multistakeholder Statement[10] on net neutrality and mass surveillance, two priority areas for Brazilian Internet diplomacy. In addition, Brazil faced distancing of some core BRICS partners: Russia openly opposed the NETmundial statement; India expressed serious concerns and delayed adoption of the outcome statement; and China and South Africa kept a very low profile. It remains to be seen if Brazil's high convergence capacity to foster a middle ground in Internet governance negotiations will be maintained in the post-NETmundial phase.

China

With the highest number of Internet users, China is an important player in Internet governance. It has been balancing digital politics between the economy-driven free communication with the rest of the world and politically driven filtered access to the Internet for Chinese users. The protection of sovereignty as a cornerstone of Chinese foreign policy is also mirrored in cyberspace. Adam Segal, reporting on a speech by Lu Wei, Minister of China's State Internet Information Office, to the Second China-South Korea Internet Roundtable, quotes Wei: 'Just as the seventeenth century saw the extension of national sovereignty over parts of the sea, and the twentieth over airspace, national sovereignty is now being extended to cyberspace […] "but cyberspace cannot live without sovereignty".'[11]

China achieved a high level of digital sovereignty by banning and/or restricting access to the Chinese market for foreign Internet companies (Facebook, Google, Twitter) and developing Chinese social media companies such as RenRen and Sina Weibo. Most of the data belonging to Chinese individuals and institutions are stored on servers in China. In foreign digital politics, China supports an inter-governmental approach. However, it keeps a low profile, leaving Russia and other countries to lead the inter-governmental initiatives in global forums.

India

India is one of the swing countries in the Internet governance debate with diverse – sometimes conflicting – positions. India's complex Internet governance policy reflects the complexity of its national digital policy-making. It has one of the most diverse and vibrant civil society scenes in global Internet governance. Its diplomatic service inclines towards an inter-governmental approach to Internet governance. Its business sector is closer to a non-governmental approach to Internet governance. This dichotomy has created some surprising moves. For example, India proposed the establishment of the UN Committee for Internet-Related Policies (CIRP) as a way to achieve inter-governmental oversight of critical Internet resources. It shifted to the other side of the Internet policy spectrum, however, by siding with the USA and other developed countries at WCIT-12. India did not sign the amended ITRs and departed from the position of the G77 countries. This surprising move was explained by the considerable lobbying power of the Indian ICT industry.

Russia

Russia has been the most vocal and consistent promoter of an inter-governmental approach to Internet governance. At WCIT-12, Russia tried to include the Internet in the ITU's work through the ITRs. It also has a strong focus on cybersecurity through the work of the first committee of the UN General Assembly.

Small states

The complexity of the issues and the dynamics of activities made it almost impossible for many small and, in particular, small developing countries, to follow Internet governance policy processes. As a result, some small states have supported a one-stop-shop structure for Internet governance issues.[12] The sheer size of the agenda and the limited policy capacity of developing countries in both their home countries and in their diplomatic missions remains one of the main obstacles for their full participation in the process. The need for capacity building in the field of Internet governance and policy was recognised as one of the priorities for the WSIS Tunis Agenda for the Information Society.

Internet governance – a variable geometry approach

Internet governance requires the involvement of a variety of stakeholders who differ in many aspects, including international legal capacity, interest in particular Internet governance issues, and available expertise. Such variety may be accommodated by using the variable geometry approach implied in Article 49 of the WSIS Declaration,[13] which specifies the following roles for the main stakeholders:

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

The business sector[14]

When ICANN was established in 1998, one of the main concerns of the business sector was the protection of trademarks. Many companies were faced with cybersquatting and the misuse of their trademarks by individuals who were fast enough to register them first. In the process of creating ICANN, business circles clearly prioritised dealing with the protection of trademarks and, accordingly, this issue was immediately addressed once ICANN was created, by the establishment of the Universal Dispute Resolution Procedures (UDRP).

The International Chamber of Commerce (ICC)

The International Chamber of Commerce (ICC), well known as the main association representing business across sectors and geographic borders, positioned itself as one of the main representatives of the business sector in the global Internet governance processes. The ICC was actively involved in the early WGIG negotiations and WSIS, and continues to be an active contributor in the current IGF process.

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

Domain-name companies

Domain-name companies include registrars and registries who sell Internet domain names (e.g. .com and .net). The main actors in this sector include VeriSign and Afilias. Their business is directly influenced by ICANN's policy decisions in areas such as the introduction of new domains and dispute resolution. It makes them one of the most important actors in the ICANN policy-making process. They have also been involved in the broader Internet governance policy process (WSIS, WGIG, the IGF) with the main objective of reducing the risk of a potential take-over of ICANN's role by intergovernmental organisations.

Internet service providers (ISPs)

Since ISPs are the key online intermediaries, it makes them particularly important for Internet governance. Their main involvement is on a national level in dealing with government and legal authorities. On a global level, some ISPs, particularly from the USA and Europe, have been active in the WSIS/WGIG/IGF processes individually and through national and regional or sector-specific business organisations such as the Information Technology Association of America (ITAA), and others.

Telecommunication companies

These companies facilitate Internet traffic and run the Internet infrastructure. The main actors include companies such as Verizon and AT&T. Traditionally, telecommunication companies have been participating in international telecommunication policy through the ITU. They have been increasingly involved in the activities of ICANN and the IGF. Their primary interest in

Internet governance is to ensure a business-friendly global environment for the development of an Internet telecommunication infrastructure. Over the last few years, ETNO has positioned itself as an active actor, especially on questions such as net neutrality.[15]

Internet content companies

Google, Facebook, and Twitter are increasingly active in Internet governance. Their core business model could be directly affected, for example, by government arrangements related to data protection and privacy. Content producers, such as Disney, are also prominent players, concerned about preserving the global outreach and dominance of its products and models for local content development, as well as to protect its copyrights globally. Business priorities of these companies are closely linked to various Internet governance issues, such as intellectual property, privacy, cybersecurity, and net neutrality. Their presence is increasingly noticeable in the global Internet governance processes, including through funding to multistakeholder forums such as the IGF.

See **Section 2** for further discussion on cybersecurity and net neutrality and **Section 3** for further discussion on IPR and privacy

Civil society

Civil society has been the most vocal and active promoter of a multistakeholder approach to Internet governance. The usual criticism of civil society participation in previous multilateral forums had been a lack of proper coordination and the presence of too many, often dissonant, voices. In the WSIS process, however, civil society representation managed to harness this inherent complexity and diversity through a few organisational forms, including a Civil Society Bureau, the Civil Society Plenary, and the Content and Themes Group. Faced with limited possibilities to influence the formal process, civil society groups developed a two-track approach. They continued their presence in the formal process by using available opportunities to participate and to lobby governments. In parallel, they prepared a Civil Society Declaration as an alternative vision to the main declaration adopted at the Geneva WSIS.[16]

NGOs and WSIS

NGO participation in WSIS was relatively low. Out of close to 3000 NGOs that have consultative status with the UN ECOSOC, only 300 participated in WSIS.

Due to WGIG's multistakeholder nature, civil society attained a high level of involvement. Civil society groups proposed eight candidates for WGIG, all of whom were subsequently appointed by the UN Secretary General. In the Tunis phase (the second phase of WSIS, after Geneva), the main policy thrust of civil society organisations shifted to WGIG, where they influenced many conclusions as well as the decision to establish the IGF as a multistakeholder space for discussing Internet governance issues.

Civil society has continued to be actively involved in IGF activities. One of the *sui generis* forms of civil society representation in Internet governance processes is the Internet Governance Caucus (IGC). It includes individuals interested in sharing opinions, policy options and expertise on Internet governance issues, which are discussed in a mailing list format.

Civil society organisations are active in almost all Internet governance topics – from infrastructure development through to economic models to rights and freedoms – mainly focusing on protection of public interests. Many organisations employ experts and academics with solid knowledge and understanding of Internet specificities, which often provides valuable contributions to the decision-shaping process.

Recently, there has been division among civil society organisations concerning protection of the global public interest. Some members of civil society, in particular from developing countries, see a stronger government role as a way to counterbalance the enormous power of the Internet industry. Civil society from developed countries, on the other hand, often allies itself with the Internet industry and the technical community, especially on the issue of the free flow of data.

International organisations

The ITU was the central international organisation in the WSIS process. It hosted the WSIS Secretariat and provided policy input on the main issues. ITU involvement in the WSIS process was part of its ongoing attempt to define and consolidate its new position in the fast-changing global telecommunications arena, increasingly shaped by the Internet. The ITU's role has been challenged in various ways. It was losing its traditional policy domain due to the WTO-led liberalisation of the global telecommunications market. The latest trend of moving telephone traffic from traditional telecommunications to the Internet (through VoIP) further reduced the ITU's regulatory footprint on the field of global telecommunications.

The possibility that the ITU might have emerged from the WSIS process as the *de facto* International Internet Organisation caused concern in the USA and in some other developed countries, while garnering support in some developing countries. Throughout WSIS, this possibility created underlying policy tensions. It was particularly clear in the field of Internet governance, where tension between ICANN and the ITU had existed since the establishment of ICANN in 1998. WSIS did not resolve this tension. With the increasing convergence of various communication technologies, it is very likely that the question of the ITU's more active role in the field of Internet governance will remain on the global policy agenda; it is already active in the field of cybersecurity.

Another issue concerned the anchoring of the multidisciplinary WSIS agenda within the family of UN specialised agencies. Non-technical aspects of communications and Internet technology, such as social, economic, and cultural features, are part of the mandate of other UN organisations. The most prominent player in this context is UNESCO, which addresses issues such as multilingualism, cultural diversity, knowledge society, and information sharing. The balance between the ITU and other UN organisations was carefully managed. The WSIS follow-up processes also reflect this balance, with the main players including the ITU, UNESCO, and the UNDP.

The technical community

The technical community includes institutions and individuals who have developed and promoted the Internet since its inception. Historically, members of the technical community were mainly linked to US universities, where they worked primarily to develop technical standards and establish the basic functionality of the Internet. The technical community also created the initial spirit of the Internet, based on the principles of sharing resources, open access, and opposition to government involvement in Internet regulation. From the beginning, its members protected the initial concept of the Internet from intensive commercialisation and extensive government influence.

Terminology

Other terms are used interchangeably with technical community, such as Internet community, Internet developers, Internet founders, Internet fathers, and technologists. The term 'technical community' is used in the WSIS declarations and other policy documents.

In the context of international relations, the technical community could be described as an epistemic community.[17] The early technical community was coordinated by a few, mainly tacit, rules and one main formal procedure – Request for Comments (RFC). All main and basic standards of the Internet are described through RFCs. While they did not have a strict regulation or formal structure, the early Internet communities were governed by strong custom and peer-to-peer pressure. Most participants in this process shared similar values, appreciation systems, and attitudes.

The early management of the Internet by the technical community was challenged in the mid-1990s after the Internet became part of global social and economic life. Internet growth introduced a group of new stakeholders, such as the business sector, that came with different professional cultures and understanding of the Internet and its governance, which led to increasing tension. For example, in the 1990s, Internet communities and the company Network Solutions[18] were involved in the so-called DNS war, a conflict over the control of the root server and domain name system.

The Internet Society is one of the main representatives of the technical community. It hosts the IETF, advocates for open Internet and plays an active role in capacity building.

The technical community has been an important actor in the process of both establishing and running ICANN. One of the fathers of the Internet, Vint Cerf, was the Chair of the ICANN Board from 2000 to 2007. Members of the technical community hold important positions in various ICANN decision-making bodies.

Nowadays, with almost three billion users, the Internet has outgrown the ICANN-based policy framework focusing on the technical community as the main constituency. Following this argument, as the line between citizens and Internet users blurs, greater involvement of governments and other structures representing citizens is required, rather than those representing Internet users only, frequently described as the technical community. Those who argued for more government involvement in Internet governance used this approach of representing citizens rather than Internet users and communities.

The technical community usually justifies its special position in Internet governance by its technical expertise. It argues that ICANN is a mainly technical organisation and, therefore, technical people using technical knowledge should run it. With the growing difficulty of maintaining ICANN as an exclusively technical organisation, this justification of the special role of the technical community has faced frequent challenge. It is very likely that the members of the technical community will gradually integrate into the core stakeholder groups, mainly civil society, business, and academia but also governments.

The Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is the main Internet governance institution. Its responsibility is to manage the core Internet infrastructure, which consists of IP addresses, domain names, and root servers. Growing interest in the role of ICANN developed in parallel with the rapid growth of the Internet in the early 2000s and ICANN came to the attention of global policy circles during the WSIS process (2002–2005).

While ICANN is one of the main actors in the Internet governance field, it does not govern all aspects of the Internet. It is sometimes, although erroneously, described as the Internet government. ICANN manages the Internet infrastructure, but it does not have direct authority over other Internet governance issues, such as cybersecurity, content policy, copyright protection, protection of privacy, maintenance of cultural diversity, or bridging the digital divide.

ICANN is a multistakeholder institution involving a wide variety of actors in different capacities and roles. They fall into four main informal groups.

- Actors that have been involved since the days when ICANN was established, including the technical community, the business community, and the US government.
- International organisations, with the most prominent roles played by the ITU and WIPO.
- National governments whose increasing interest in having a bigger role in ICANN started with the WSIS process.
- Internet users (the community at large).

ICANN has experimented with various approaches in order to involve Internet users. In its early days, the first attempt was to involve Internet users through direct elections of their representatives to ICANN governing bodies. It was an attempt to secure ICANN's legitimacy. With low turnout and misuse of the process, the direct vote failed by not providing real representation of Internet users. More recently, ICANN has been trying to involve Internet users through an 'at-large' governance structure. This organisational experiment is essential for ensuring ICANN's legitimacy.[19]

ICANN's decision-making process was influenced by early Internet governance processes based on bottom-up, transparent, open, and inclusive approaches. One main difference between the early technical community of the 1980s and the current ICANN decision-making context is the level of 'social capital'. In the past, the technical community had high levels of mutual trust and solidarity that made decision-making and dispute resolution much simpler than it is now. The growth of the Internet extended to millions of new users and new stakeholders, far beyond the early technical community. Consequently, this fast growth of the Internet reduced the social capital that existed in its early days. Thus, frequent proposals by the technical community to keep the earlier, informal, decision-making process on the Internet has not been realistic. Without social capital, the main way of ensuring a fully functional decision-making process is to formalise it and to develop various checks-and-balance mechanisms.

Some corrections to decision-making procedures have already been made to reflect this changing reality. The most important was the 2002 reform of ICANN, which included strengthening the Governmental Advisory Committee (GAC) and abandoning the direct voting system.

The issues

Technical vs policy management

The dichotomy between technical and policy management has created continuous tension in ICANN's activities. ICANN has portrayed itself as a technical coordination body for the Internet that deals only with technical issues and stays away from the public policy aspects of the Internet. ICANN officials considered this specific technical nature as the main conceptual argument for defending the institution's unique status and organisational structure. The first Chair of ICANN, Esther Dyson, stressed that: 'ICANN does not "aspire to address" any Internet governance issues; in effect, it governs the plumbing, not the people. It has a very limited mandate to administer certain (largely technical) aspects of the Internet infrastructure in general and the DNS in particular.'[20]

Critics of this assertion usually point to the fact that no technically neutral solutions exist. Ultimately, each technical solution or decision promotes certain interests; empowers certain groups; and affects social, political, and economic life. The debate on issues such as the .xxx (adult materials) clearly illustrated that ICANN has to deal with public policy aspects of technical issues. The final statement from the NETmundial meeting recommends that further discussions related to ICANN and IANA address 'the adequate relation between the policy and operational aspects'.[10] Dealing with the new gTLDs will push ICANN further towards addressing public policy issues.

ICANN's international status

The special ties between ICANN and the US government have been a major focus of criticism, which takes two main forms. The first form relates to the global accountability of ICANN and rests on principle considerations, stressing that the vital element of the global Internet infrastructure, which could affect all nations, be supervised by one country alone. This criticism was apparent during the WSIS process and was enhanced by general suspicion of US foreign policy after the military intervention in Iraq. Typical counter-argument is based on the historical fact that the Internet was created in the USA with the US government's financial support. Consequently, according to this argument, this gives the US government the moral grounds to decide on the form and tempo of the globalisation of Internet governance. This approach is particularly powerful in the US Congress, which has opposed any such globalisation – and especially the leading roles of other governments (a model referred to as internationalisation by proponents of multilateral approach).

The second criticism of special ICANN-USA ties rests on practical and legal considerations. Since ICANN is a US-based legal entity, it has to obey US law. Some of these laws may affect the regulation of ICANN's global facilities. Critics of the USA's role usually quote an example of sanctions: If the US judiciary exercises its role and properly implements the sanctions regime against Iran and Cuba, it could force ICANN – as a US private entity – to remove country domains for those two countries from the Internet. According to this argument, by retaining the Iranian and Cuban domain names, ICANN is breaching US sanctions law. While removal of country domain names has never happened, it remains a possibility given the current legal status of ICANN.

Next steps

A new phase of the status of ICANN was initiated by the NTIA announcement on 14 March 2014. Both key issues – dealing with public policy matters and globalisation – could be settled by changing the status of ICANN, which would reduce the ambiguities and improve the clarity of its mission. The future development of ICANN will require innovative solutions, including the possibility of transforming ICANN into a *sui generis* global set-up; this would preserve all the advantages of the current ICANN structure as well as address shortcomings, particularly the problems of accountability and international legitimacy. Inspirations for such creative solutions can be found in the International Red Cross and Red Crescent Movement that has proven mechanisms to integrate various stakeholders in an internationally legitimate policy framework that balances public interests and private initiatives.

Endnotes

[1] The Brazilian model of the management of its country domain name is usually taken as a successful example of a multistakeholder approach. The national body in charge of Brazilian domains – CGI – is open to all users, including government authorities, the business sector, and civil society. Brazil gradually extended this model to other areas of Internet governance, especially in the process of the preparation for IGF 2007, which was hosted in Rio de Janeiro.

[2] Géraud A (1954) The rise and fall of the Anglo-French Entente. *Foreign Affairs.* Available at **http://www.foreignaffairs.com/articles/71095/andre-geraud-pertinax/rise-and-fall-of-the-anglo-french-entente** [accessed 15 August 2014].

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

[4] US Secretary of State criticising the ITU for the initiative: 'without authorization of member governments to hold a global meeting involving an unauthorized expenditure of resources and concluding international agreements.' Quoted in Drake W. (2004) *Reframing Internet Governance Discourse: Fifteen Baseline Propositions,* p. 9. Available at **http://www.un-ngls.org/orf/drake.pdf** [accessed 14 August 2014].

[5] ICANN (no date) Affirmation of Commitments. Available at **https://www.icann.org/resources/pages/aoc-2012-02-25-en** [accessed 15 August 2014].

[6] ICANN (2014) Administrator of the Domain Name System launches global multistakeholder accountability process. Available at **https://www.icann.org/resources/press-material/release-2014-03-14-en** [accessed 15 August 2014].

[7] Internet World Stats (no date) Internet usage in the European Union. Available at **http://www.internetworldstats.com/stats9.htm** [accessed 14 August 2014].

[8] EU Commission (2013) Antitrust: Commission seeks feedback on commitments offered by Google to address competition concerns. European Commission – IP/13/371. Available at **http://europa.eu/rapid/press-release_IP-13-371_en.htm** [accessed 15 August 2014].

[9] Rousseff D (2013) Statement by H. E. Dilma Rousseff, president of the Federative Republic of Brazil, at the opening of the general debate of the 68th Session of the United Nations General Assembly. Available at **http://www.un.int/brazil/speech/13d-PR-DR-68-AG-Abertura-Ing.html** [accessed 14 August 2014].

[10] NETmundial (2014) NETmundial Multistakeholder Statement. Available at **http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf** [accessed 15 August 2014].

[11] Segal A (2013) Cyberspace cannot live without sovereignty, says Lu Wei. Available at **http://blogs.cfr.org/asia/2013/12/10/cyberspace-cannot-live-without-sovereignty-says-lu-wei/#cid=soc-twitter-at-blogs-cyberspace_cannot_live_without-121013** [accessed 14 August 2014].

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

[13] WSIS (2003) Declaration of principles. Available at **http://www.itu.int/wsis/docs/geneva/official/dop.html** [accessed 15 August 2014].

[14] Valuable comments were provided by Ayesha Hassan.

[15] ETNO Website (no date) European Telecommunications Network Operators' Association. Available at **https://www.etno.eu/** [accessed 15 August 2014].

[16] WSIS Civil Society Plenary (2003) Shaping information societies for human needs. Available at **http://www.itu.int/wsis/docs/geneva/civil-society-declaration.pdf** [accessed 15 August 2014].

[17] The technical community fulfils all the criteria in Peter Haas's definition of an epistemic community: 'a professional group that believes in the same cause and effect relationships, truth tests to accept them, and shares common values; its members share a common understanding of the problem and its solutions.' Haas P (1990) *Saving the Mediterranean: the politics of international environmental co-operation.* New York: Columbia University Press, p. 55.

[18] The technology company Network Solutions **www.networksolutions.com** was founded in 1979. The domain name registration business was the most important division of the company; the company diversified its portfolio to include web services for small businesses.

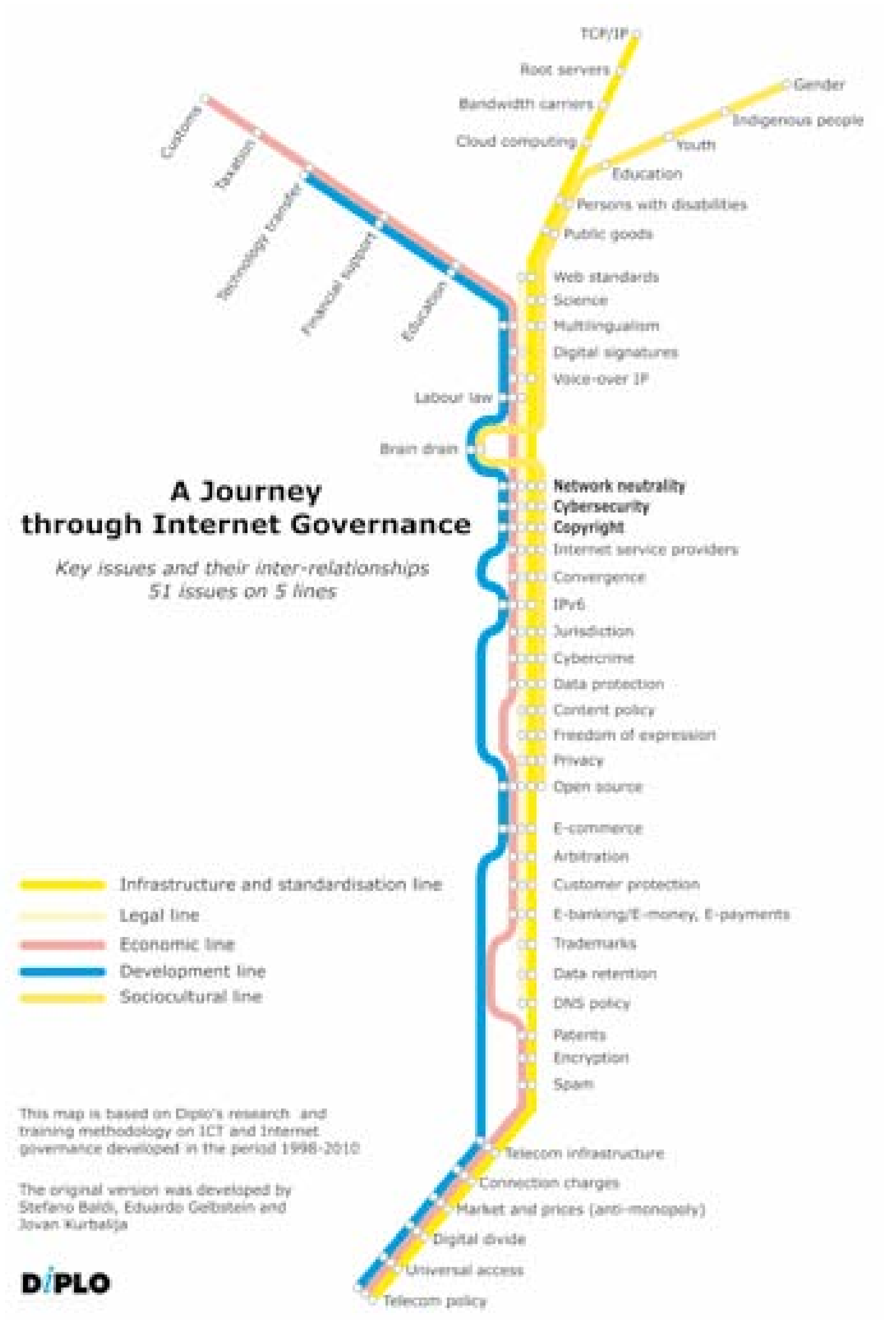
[19] ICANN (no date) ALAC. Available at **http://atlarge.icann.org/alac** [accessed 15 August 2014].

[20] Esther Dyson's response to Ralph Nader's Questions (15 June 1999). Available at **http://www.icann.org/en/correspondence/dyson-response-to-nader-15jun99.htm** [accessed 14 August 2014].

Section 8

Annex

Annex



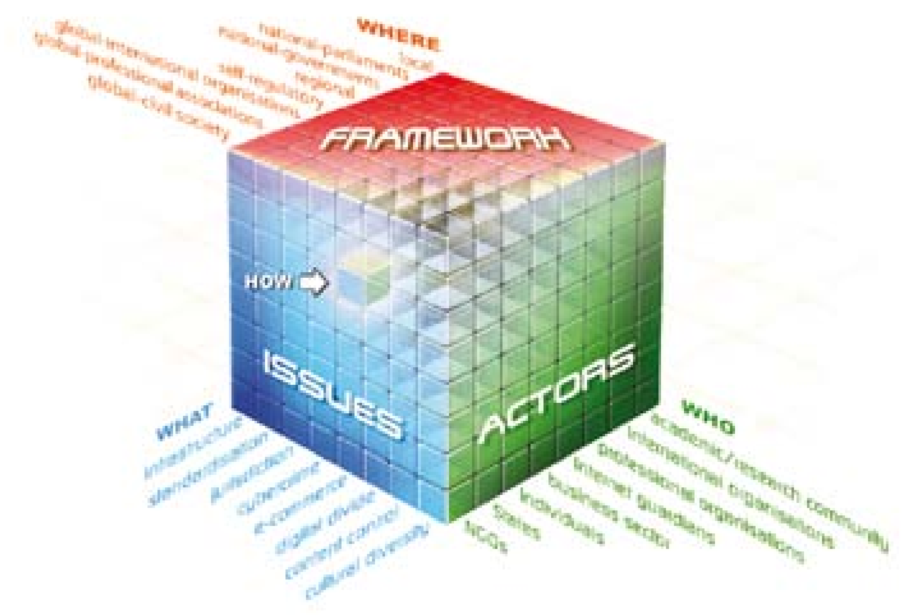
A Journey through Internet Governance

Key issues and their inter-relationships
51 issues on 5 lines

This map is based on Diplo's research and training methodology on ICT and Internet governance developed in the period 1998-2010

The original version was developed by Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija

The Internet governance cube



The Internet governance cube is a visualisation of Internet governance processes.

The WHAT axis is related to the ISSUES of Internet governance (e.g. infrastructure, copyright, and privacy). It highlights the **multidisciplinary** nature of Internet governance issues.

The WHO axis of the cube focuses on the main ACTORS (states, international organisations, civil society, the private sector). This is the **multistakeholder** aspect.

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 **multileveled** approach to Internet governance.

When we move pieces in the Internet governance 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 techniques (e.g. analogies) and in terms of legal 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 governments, business, and civil society (who) at regional level (WHERE).

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

DiPLO
www.diplomacy.edu

DiploFoundation is a non-profit organisation which works towards inclusive and effective diplomacy. It was established in 2002 by the governments of Malta and Switzerland. Diplo's activities revolve around, and feed into, our focus on education, training, and capacity building:

- **Courses:** We offer postgraduate-level academic courses and training workshops on a variety of diplomacy-related topics for diplomats, civil servants, staff of international organisations and NGOs, and students of international relations. Our courses are delivered through online and blended learning.
- **Capacity building:** With the support of donor and partner agencies, we offer capacity-building programmes for participants from developing countries in a number of topics including Internet Governance, Human Rights, Public Diplomacy and Advocacy, and Health Diplomacy.
- **Research:** Through our research and conferences, we investigate topics related to diplomacy, Internet governance, and online learning.
- **Publications:** Our publications range from the examination of contemporary developments in diplomacy to new analyses of traditional aspects of diplomacy.
- **Software development:** We have created a set of software applications custom designed for diplomats and others who work in international relations. We also excel in the development of online learning platforms.

Diplo is based in Malta, with offices in Geneva and Belgrade.

For more information about Diplo, visit http://www.diplomacy.edu

Geneva Internet Platform

The Federal Department of Foreign Affairs (EDA) and the Federal Office for Telecommunications (BAKOM) have initiated the Geneva Internet Platform (GIP), which fulfils the mission of an observatory, a capacity building centre (online and *in situ*), and a centre for discussion. The GIP is hosted and operated by DiploFoundation.

The GIP's activities are implemented based on three pillars:

- A physical platform in Geneva
- An online platform and observatory
- An innovation lab

The GIP's special focus is on assisting small and developing countries to meaningfully particpate in Internet governance processes. The support is tailored for the needs of these actors, including training, awareness building, consultations and briefings.

For more information on the GIP's activities please consult http://www.giplatform.org or write to gip@diplomacy.edu

About the author

Jovan Kurbalija is the founding director of DiploFoundation and head of the Geneva Internet Platform. He is a former diplomat with a professional and academic background in international law, diplomacy, and information technology. In 1992, he established the Unit for Information Technology and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of training, research, and publishing, in 2002 the Unit evolved into DiploFoundation.

Since 1994, Dr Kurbalija has been teaching courses on the impact of ICT/Internet on diplomacy and ICT/Internet governance. Currently, he is visiting lecturer at the College of Europe in Bruges and the University of St Gallen. He has lectured at the Mediterranean Academy of Diplomatic Studies in Malta, the Vienna Diplomatic Academy, the Dutch Institute of International Relations (Clingendael), the Graduate Institute of International and Development Studies in Geneva, the UN Staff College, and the University of Southern California. He conceptualised and currently directs DiploFoundation's Internet Governance Capacity Building Programme (2005–2014). Dr Kurbalija's main research interests include the development of an international regime for the Internet, the use of the Internet in diplomacy and modern negotiations, and the impact of the Internet on modern international relations.

Dr Kurbalija has published and edited numerous books, articles, and chapters, including: *The Internet Guide for Diplomats, Knowledge and Diplomacy, The Influence of IT on Diplomatic Practice, Information Technology and the Diplomatic Services of Developing Countries, Modern Diplomacy* and *Language and Diplomacy*. With Stefano Baldi and Eduardo Gelbstein, he co-authored the *Information Society Library,* a set of eight booklets covering a wide range of Internet-related developments.

jovank@diplomacy.edu

For easy reference: a list of frequently used abbreviations and acronyms

APEC	Asia-Pacific Economic Co-operation
ccTLD	country code Top-Level Domain
CIDR	Classless Inter-Domain Routing
DMCA	Digital Millennium Copyright Act
DNS	Domain Name System
DRM	Digital Rights Management
GAC	Governmental Advisory Committee
gTLD	generic Top-Level Domain
HTML	HyperText Markup Language
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICC	International Chamber of Commerce
aICT Technology	Information and Communications
IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
IPR	Intellectual Property Rights
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXP	Internet eXchange Point
MoU	Memorandum of Understanding
OECD	Organisation for Economic Co-operation and Development
PKI	Public Key Infrastructure
S&T	Science and Technology
SGML	Standard Generalized Markup Language
sTLD	sponsored Top-Level Domain
TCP/IP	Transmission Control Protocol/ Internet Protocol
TLD	Top-Level Domain
TRIPS	Trade-Related Aspects of Intellectual Property Rights
UDHR	Universal Declaration of Human Rights
UDRP	Uniform Domain-Name Dispute-Resolution Policy
UNECOSOC	United Nations Economic and Social Council
UNCITRAL	United Nations Commission on International Trade Law
UNESCO	United Nations Educational, Scientific and Cultural Organization
VoIP	Voice-over Internet Protocol
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WIPO	World Intellectual Property Organization
WSIS	World Summit on the Information Society
XML	eXtensible Markup Language

AN INTRODUCTION TO **INTERNET GOVERNANCE** Jovan Kurbalija

An Introduction to Internet Governance provides a comprehensive overview of the main issues and actors in this field. The book is written in a clear and accessible way, supplemented with numerous figures and illustrations. It focuses on technical, legal, economic, development, and sociocultural aspects of Internet governance, providing a brief introduction, a summary of major questions and controversies, and a survey of different views and approaches for each issue. The book offers a practical framework for analysis and discussion of Internet governance.

Since 1997 more than 1500 diplomats, computer specialists, civil society activists, and academics have attended training courses based on the text and approach presented in this book. With every delivery of the course, materials are updated and improved. This regular updating makes the book particularly useful as a teaching resource for introductory studies in Internet governance.

DiPLO
www.diplomacy.edu

9 7 8 9 9 9 3 2 5 3 2 8 0