Governing the Internet

Freedom and Regulation in the OSCE Region

OSCE Organization for Security and Co-operation in Europe

The Representative on
Freedom of the Media

The publisher would like to thank the Governments of France and Germany for their generous support to this publication.

The views expressed by the authors in this publication are their own and do not necessarily reflect the views of the OSCE Representative on Freedom of the Media.

Edited by Christian Möller and Arnaud Amouroux

Organization for Security and Co-operation in Europe (OSCE)
Kärtnerring 5-7, Top 14, 2. DG
A-1010 Vienna, Austria
tel +43-1-512 21 45-0
fax +43-1-512 21 45-9
e-mail pm-fom@osce.org
www.osce.org/fom

Design & Layout: Phoenix Design Aid, Denmark

ISBN 3-9501955-4-8

Contents

I. Internet Governance

II. Experiences from the OSCE Region

III. The Multi-stakeholder Approach to Internet Governance

IV. Biographies

Preface

Miklós Haraszti

“Internet Governance” is still at a “work-in-progress” stage. It might develop into a new way of policy-making on a global scale involving many different sectors, including not only governments, but also industry and civil society.

Whereas standards for previous means of communication were set by intergovernmental organizations, for the Internet this is often done by the online community or expert bodies with an open membership. Technical standards for the emerging networks of the Internet have been set by requests for comments and consensus building.

But Internet Governance is not only about technical standards or the Domain Name System. It also has commercial, cultural and social implications, concerning issues like the free flow of information, freedom of expression and freedom of the media online.

Recent moves against free speech on the Internet in a number of countries have provided a bitter reminder of the ease with which some regimes — democracies and dictatorships alike — seek to suppress speech that they disapprove of, dislike, or simply fear.

Speaking out has never been easier than on the Web. Yet at the same time we are witnessing the spread of Internet censorship. According to research by the OpenNet Initiative, a transatlantic group of academic institutions, censorship is being practised by about two dozen countries and applied to a far wider range of online information and applications.

Governments do play an important role in Internet Governance. Although "governance" is not synonymous with "government", this does not mean that governments should be excluded. Governments have a function that cannot be filled by other actors, for example in guaranteeing an independent judiciary, protecting human rights or establishing antitrust measures.

On the other hand there are many fields in which the State should leave governance of the Internet to civil society or the private sector, for example when it comes to the technical functioning, administration, or organization of networks.

The freedom dimension of this issue has encouraged the OSCE media freedom Office to take a more detailed look at how the Internet is governed in the OSCE region. In this book the concept of Internet Governance is addressed from a number of different sides and examples from various countries in the OSCE region show how diverse issues of Internet Governance are being tackled by different stakeholders.

Reflecting these diverse approaches to Internet Governance is the aim of this publication. I hope that it will contribute in the OSCE region to raising awareness about Internet Governance and its impact on freedom of the media.

I would like to warmly thank the Governments of France and Germany for their generous support to the experts' workshop and to this book.

“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.”

Working definition of Internet Governance elaborated by the UN Working Group on Internet Governance (WGIG) in its report of July 2005.[1]

[1] Report of the Working Group on Internet Governance, June 2005 <http://www.wgig.org/docs/WGIGREPORT.doc>.

Introduction

Arnaud Amouroux and Christian Möller

This publication aims to undertake a difficult task, namely to freeze a particular moment in the history of a medium that is changing so quickly and so dramatically. And it can only mirror a certain moment in the ongoing process. The process is called “governance” and the medium is the “Internet”.

The moment we seek to capture is important in the development of the Internet as it is the very moment when permanent governing rules for the networked world are being debated, for the first time at the international level and in institutionalized fora.

Increasing attention has been paid to the question of whether the Internet, which has developed outside a classic intergovernmental framework, needs governance at all, and, if yes, in what form. Do we need a formal governance structure or will informal means of governance – namely behavioural norms established by the Internet community or by the software code itself – suffice?

The disproportionate number of players involved and the myriad of different efforts raise questions about whether the current approach is the best one. According to netdialogue.org, more than a dozen intergovernmental organizations[2] are currently deciding rules – without any co-ordination

[2] To name a few: Council of Europe (CoE), International Monetary Fund (IMF), International Telecommunication Union (ITU), Organisation for Economic Co-operation and Development (OECD), World Trade Organization (WTO), World Intellectual Property Organization (WIPO), and of course Internet Corporation for Assigned Names and Numbers (ICANN) and World Wide Web Consortium (W3C).

whatsoever – for the networked world in an almost infinite array of fields (property, security, jurisdiction, infrastructure, relations between persons and the State, relations between private parties etc.). Efforts towards more harmonization, rationalization and clarification are exactly what the UN aims to achieve with its Internet Governance Forum (IGF).

And whereas television frequencies or phone numbers are governed by national broadcasting authorities or international governmental bodies like the ITU, the Domain Name System (DNS) – which could be best explained as the directory of Internet numbers – is kept by the Internet Corporation for Assigned Names and Numbers (ICANN), a private company under US law.

In the early years of the twenty-first century, Internet Governance naturally started to gain importance and came to the fore at the World Summit on the Information Society (WSIS), held in two stages under the auspices of the United Nations in Geneva in December 2003 and in Tunis in November 2005.

The UN-led Process: Internet Governance Forum

The Tunis Agenda for the Information Society invited the UN Secretary-General to convene a new forum for multi-stakeholder policy dialogue. This Internet Governance Forum (IGF) process is supported by a Secretariat which is hosted by the United Nations Office in Geneva.

The first meeting of the IGF was held in Athens in autumn 2006. Preparation for the 2007 IGF in Rio has already started. Several so-called “Dynamic Coalitions” have been founded.

At the price – or advantage – of not being able to adopt binding decisions, the IGF has managed to be very inclusive. The outcome of this process remains open, but the form of the IGF and its organization is definitely a new model of policy-making at the international level.

We still do not know whether another institutionalized body addressing all these different aspects of Internet Governance will evolve from the IGF process. Maybe it will instead be an inclusive dialogue and a process of best practices and rough consensus between the different actors. And maybe governments will recognize that not everything needs exact regulation as long as it is functioning smoothly and to everybody's benefit.

The Office of the OSCE Representative participated in the 2006 Athens IGF and, together with other actors, initiated the "Dynamic Coalition on Freedom of Expression and Freedom of the Media Online" (FOEonline)[3]. This coalition now combines more than a dozen partners, including the Council of Europe and UNESCO as well as NGOs like Amnesty International, Article 19, Reporters sans frontières and IP Justice, as well as academia.

These "dynamic coalitions" are endorsed by the Internet Governance Forum, but do not constitute formal entities in any way. Instead, they serve as informal, open and inclusive platforms for state and non-state actors to share their views and contribute to the IGF process.[4]

They might shape policy-making in the field of Internet Governance, but this still remains to be seen. For the time being, the contributions outlined below aim at describing the involvement and co-operation of different stakeholders in some countries of the OSCE region.

Structure of the Publication

In contrast to the 2004 *Media Freedom Internet Cookbook*, this publication does not offer "recipes" about how to guarantee media freedom online. Instead it serves as a showcase of examples of multi-stakeholder

[3] <http://foeonline.wordpress.com>

[4] A complete list of all dynamic coalitions can be found at <http://www.intgovforum.org/Dynamic%20Coalitions.php>.

approaches to Internet Governance. A workshop on Internet Governance was held at the Forum des droits sur l'Internet in Paris in December 2006 in preparation for this publication.

Involving all of society's actors is a difficult task and there is no ready-made approach for all OSCE countries. These case studies show good practices, but also where there is room for improvement.

Bertrand de la Chapelle, the French Government's Special Envoy for the Information Society, outlines how a United Nations Summit produced a new governance paradigm for the Internet Age, setting the scene for the following contributions.

Christian Möller goes into the details of the Internet's underlying technical infrastructure and the Domain Name System, which is necessary in order to follow the ongoing discussion, for example on the role of ICANN.

Wolfgang Kleinwächter takes us from the technical level to policy-making and traces the history of institutionalizing Internet Governance from ICANN to the World Summit on the Information Society.

Nico van Eijk and Katerina Maniadaki cover most of the relevant "national" governance issues of the Domain Name System (DNS) based on the example of the .eu top level domain (TLD). This may serve as an example or a checklist for the regulation of national domain names.

The second part, on experiences from the OSCE region, takes a look at approaches to governing and countering hate speech on a European level as well as regulatory experiences from two countries in the Southern Caucasus and Central Asian region.

The choice of Georgia and Kazakhstan was motivated by the fact that there is already considerable legislative activity in spite of the still nascent Internet infrastructure. The articles show the necessity of a liberal legal framework and a competitive market for the development of the information society.

Yaman Akdeniz addresses freedom of expression and freedom of the media online. He takes a detailed look at the governance of hate speech on the Internet at an international level and argues that education about racism and how to foster tolerance is the single most effective way of combating racism on the Internet.

Rachid Nougmanov takes a look at the situation in Kazakhstan. He focuses on the importance of the technical infrastructure and affordable access to the Internet but also the challenges national legislation might face in combating illegal content while at the same time guaranteeing freedom of expression online.

Ana Dolidze analyses Georgian legislation that is governing the media and free expression online. She looks at the perils freedom of the media on the Internet might face if treated and regulated in the same way as classic broadcast media.

The third part provides examples of the so-called multi-stakeholder approach to Internet Governance, meaning that all parts of society should be involved in their respective roles. This includes governments, NGOs and other civil society actors, the industry and last but by no means least the Internet users themselves.

Jennifer Siebert uses the German example to demonstrate how children can be protected from possibly harmful content without restricting legitimate access for adults.

Isabelle Falque-Pierrotin and **Laurent Baup** from the French Forum des droits sur l'internet give an example of how a private body supported by the Government can help in the dialogue and collaborative process between public and private actors, helping them to draft public policies and make decisions. They argue that Internet Governance requires a new way of thinking and decision-making tailored to the complex digital world and discuss how this has affected the roles and status of public and private actors.

Viesturs Pless and **Ina Gudele**, the Special Assignments Minister for Electronic Government Affairs in Latvia, introduce the history and the preconditions for the successful development of an information society based on the example of Latvia.

Jon Thorhallsson looks at things from a user perspective as stakeholders who should not be neglected when discussing the Internet. He also gives some examples of how everybody could use the Web a little more safely.

We hope that this collection of diverse contributions provides some useful information for OSCE participating States, but also for other interested parties, and will help them trace the development of Internet Governance. Working together with all relevant actors to improve the free flow of ideas on the Internet, to guarantee media freedom online and to enable users to participate in the information society should be our shared aim in "governing the Internet".

Christian Möller, Arnaud Amouroux
Vienna, May 2007

I. Internet Governance

The Internet Governance Forum: How a United Nations Summit Produced a New Governance Paradigm for the Internet Age

Bertrand de la Chapelle

Introduction

The World Summit on the Information Society (2003–2005) did not seem to generate much media coverage or much interest from citizens. It may nonetheless go down in history as having planted the seeds of a new architecture of global governance.

The multi-stakeholder Internet Governance Forum (IGF) created by the Tunis Summit in 2005 can be considered as the major outcome of this four-year United Nations process and a laboratory for a new paradigm of interaction between governments, civil society and private actors on public policy issues at the global level.

At first glance, the World Summit on the Information Society was a UN summit like any other: two large conferences at the level of Heads of State or Government in Geneva in 2003 and in Tunis in 2005 gathered more than 15,000 participants each and produced four official documents after long and painful diplomatic negotiations.

Upon closer examination though, this process can better be described by: four years for four words. The first two years have indeed witnessed the emergence of the expression “Internet Governance” and the two following ones the concept of “multi-stakeholder Forum”.

The apparent simplicity of these two formulations should not hide two major perspective shifts. First, the recognition that the recent evolution of the Internet raises public policy issues that cannot be addressed in the framework of the traditional notions of government or regulation, hence the progressive acceptance of the term Internet Governance. Second, the confirmation that all categories of actors: governments, civil society and business are stakeholders that must be associated in open and inclusive discussion spaces if we really want to address the challenges ahead of us, hence the notion of a multi-stakeholder Forum.

During four years, civil society and business actors made important efforts to be accepted and recognized as legitimate participants in a process that started as purely intergovernmental. Their success in that regard was a first in the history of UN summits. It creates a precedent, the consequences of which will only become visible with time. Explaining why this was possible and how the four words “multi-stakeholder Internet Governance Forum” emerged is the purpose of this paper.

The Internet as the Embryo of a “Global Polity”

A progressive recognition by governments of civil society and business actors was possible because of their undisputable competence and legitimacy with regards to the Internet. Having invented and developed on their own a network with global reach and success at a time when most governments were not even paying attention, civil society and business actors needed to be involved in the WSIS process to provide information to diplomats who initially lacked a correct understanding of the technical dimensions and policy challenges.

But, simultaneously, the so-called “Internet community” of techies and businesses was forced to admit that beyond the first transformation which made the initial academic network progressively support commercial activities, the nature of the Internet had changed for a second time. Today, interactions between close to a billion people through blogs and social networks have turned the Internet into a complete social, economic and political space at the international level. The common rules to organize this embryo of a "global polity" cannot remain the sole province of technical actors (through standards) or companies (self-regulation): elaboration and implementation of these rules must also involve public authorities and in particular national governments.

No single category of actors can address – let alone solve – on its own the challenges raised by the Internet and its uses. Understanding that the Internet is as much a political space as a technical network was a prerequisite for mutual recognition between actors who did not usually speak to one another and finally had to accept their interdependence and joint responsibility.

Governance "of" the Internet and "on" the Internet

"Internet Governance" was a term initially used in the technical community to designate the technical management of the Domain Name System and the corresponding root servers. In a certain way, it mostly meant governance "of" the Internet, for example of the network infrastructure itself.

But as recognition grew that the Internet is also a space, many public policy questions arose related to the activities conducted in that space. Electronic commerce, intellectual property, spam and cybercrime, freedom of expression, protection of privacy are only some of the numerous domains where global common rules become necessary, if only to address conflicts of jurisdictions. Unfortunately, the traditional framework based in the exclusive sovereignty of nation-states appears ill-adapted to such a transnational network.

In search of a simple expression to encompass the diversity of these issues without prejudging the structure to address them or the ultimate solutions, actors involved in the WSIS accepted after two years of discussions to consider that "Internet Governance" would, from then on, cover the two complementary dimensions: the governance of the network itself and of the activities conducted on it. In other words, "Internet Governance" became both the governance "of" the Internet and "on" the Internet.

The Tunis Agenda for the Information Society (TAIS) adopted in 2005 sanctified this interpretation with its clear and extremely innovative definition: "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."

In a quiet and inconspicuous way, the term governance became therefore included – probably for the first time – in UN documents with a whole different meaning than the traditional "good governance" related to the fight against corruption in developing countries.

The Concept of "Stakeholders"

The term "stakeholders" is at the core of the perspective shift the Summit introduced regarding the respective roles and responsibilities of the different categories of actors. The present international architecture, often qualified as "Westphalian", is based on a community of nation-states with equal rights. Their public authorities (however designated) are the depositaries of an absolute national sovereignty that they exercise through diplomatic envoys in intergovernmental institutions such as United Nations Agencies.

We all know that a heated debate persists regarding the role, legitimacy and representativity of civil society actors in that framework. This controversy clearly had an impact on the first years of the WSIS. In spite of explicit requirements in the UN resolution establishing the Summit for a full involvement of non-governmental actors, several governments in the initial phases of the negotiations tried to protect the intergovernmental nature of the exercise, for fear of establishing a precedent for other discussions. Accordingly, civil society and business representatives were repeatedly expelled from negotiating rooms.

Nevertheless, four years of regular interaction between actors from the three “orders” greatly reduced initial mistrust and allowed the mutual recognition described above. This explains why the word “stakeholders” progressively established itself to designate the diversity of actors involved in Information Society issues. The use of a single term implicitly established a form of equal status among the different groups.

The documents adopted in Tunis in 2005 were a consecration for this lexical innovation, through the recurrent mention of the term “multi-stakeholder” to designate processes requiring the interaction and engagement of all actors concerned with a given issue. This certainly constituted a first in official documents adopted by more than 180 countries.

An Open Forum as Dialogue Space

The term governance prejudged neither the rules to be adopted nor the framework within which they would be discussed. Similarly, the use of the terms “stakeholder” or “multi-stakeholder” did not prejudge either the respective roles and responsibilities of the different categories of actors or the ways they were supposed to interact.

Accordingly, as soon as the right of the different actors to participate in governance activities related to the Internet was established, the question of the appropriate framework became central. After lengthy debates, the notion of an open forum naturally imposed itself as the appropriate solution, because of its flexibility (some might say its fuzziness) and its light institutional constraints. The Tunis phase of WSIS therefore established for five years a very innovative and multi-stakeholder Internet Governance Forum (IGF).

Although directly attached to the United Nations Secretary General, the IGF is not constrained by the traditional procedure rules of the UN system and its practical operational modalities have to be invented as it goes. Participants in WSIS also agreed that the Forum should be a dialogue space between actors and not a decision-making structure.

Some actors have expressed regret that the Internet Governance Forum was not granted decision-making capacity. But this was obviously a prerequisite for governments to accept the principles of openness and equal status of all participants. Furthermore, the very absence of pre-established rules of procedure allowed the IGF to design its own and they are by far the most open ever used in any organization related to the UN system and welcoming government representatives.

During its inaugural meeting in Athens in November 2006, the Internet Governance Forum welcomed more than 1,300 delegates with no other accreditation constraint than online registration and they participated in four days of discussions on a strict equal footing basis around four major themes (Security, Openness, Diversity and Access).

Interestingly, beyond the four main thematic sessions, more than 30 specialized workshops were organized at the initiative of participants. This established de facto the right of all participants to informally set up the Agenda of the Forum, a prerogative normally requiring complete consensus among governments in traditional intergovernmental organizations.

In addition, spontaneous groupings of stakeholders concerned with specific issues were formed as one of the outcomes of the first inaugural meeting. These so-called “Dynamic Coalitions” are expected to informally help structure the work of the IGF during the periods between the annual meetings.

Behind the apparent modesty of a simple dialogue space with no decision-making power, the IGF establishes for the first time at the international level an official thematic deliberation space, mixing government representatives and concerned citizens, to discuss public policy issues as diverse and potentially controversial as freedom of expression or protection of privacy.

Conclusion: Governance for the Internet Age?

This multi-stakeholder governance approach is a major conceptual innovation. But it only became practicable at the global level because of the existence of online tools: access to information (websites without costs of paper duplication), remote participation (webcasts, blogs), iterative consultation processes (mailing lists and forums) and soon, collaborative drafting (wikis). Indeed, multi-stakeholder governance requires a combination of physical interactions and "intersessional" online collaboration that is only imaginable on the Internet.

Internet Governance is therefore not only the governance "of" the Internet and "on" the Internet. It is also, in a certain way, governance "enabled by" the Internet, or in other terms, the embryo of a "Governance for the Internet Age". The global network demands a new type of governance; but it is also the tool that makes this new governance possible and shapes it in its own image: real-time, participatory and distributed.

Furthermore, the multi-stakeholder principles and methods experimented with by the IGF may very well be applicable in the future to other domains such as Environment or Health, by merely changing the stakeholders involved. In particular, the definition adopted in Tunis could be transposed, mutatis mutandis, to other resources, according to the formula: "The governance of [resource or domain X] is the elaboration and the application by States, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programs, that shape the [management or exploitation] of [resource of domain X]". As a consequence, a pragmatic evolution of the international system could emerge through the progressive implementation of successive thematic governance regimes.

The Internet has transformed social and economic activities in ways that were hard to predict only ten years ago. It is now poised to also transform the way human communities organize themselves, that is: policy-making at the different levels. This recognition of the “multi-stakeholder principle” for Internet Governance is therefore a limited but essential step towards the global governance system our interdependent world needs, and the Internet Governance Forum constitutes a laboratory for new modalities to organize the international community.

This fragile experiment is just a beginning. Its future is not set in stone and the IGF will certainly be confronted by major challenges. But it offers a glimmer of hope in the debate on global governance and points towards a potential paradigm shift in the way the international community will address the global issues it is confronted with.

Governing the Domain Name System: An Introduction to Internet Infrastructure

Christian Möller

Introduction[5]

Although the Internet seems to be slowly coming of age, many of us still don't know too much about its origins[6] or the way it functions. And there is no getting away from the fact that the description of complex digital networks tends to be complex itself. Of course, this paper cannot be a comprehensive explanation or replace an academic textbook, but maybe it will help to create a clearer picture of the different Internet applications, the DNS, and the many institutions dealing with Internet Governance, for example ICANN.

The Internet

The Internet is the publicly accessible worldwide system of interconnected computer networks that transmit data by packet switching using a standardized Internet Protocol (IP) and many other protocols. It is made up of thousands of smaller commercial, academic, domestic and government networks. It carries various information and services, such as electronic mail, newsgroups, online chat, and the interlinked web pages and other documents of the World Wide Web.

[5] Much of the following information has been compiled using <www.wikipedia.org>, the free online encyclopedia. The whole text is available under the terms of the GNU Free Documentation Licence.

[6] Also see: Christian Möller, "From C64 to WWW", in: OSCE Representative on Freedom of the Media (ed.) Freedom and Responsibility. *Yearbook 2001/2002*. (Vienna: OSCE, 2002), pp. 161-170.

Apart from the incredibly complex physical connections that make up its infrastructure, the Internet is held together by bi- or multilateral commercial contracts (for example peering agreements) and by technical specifications or protocols that describe how to exchange data over the network.

Unlike older communications systems, the Internet protocol suite was deliberately designed to be independent of the underlying physical medium. Any communications network, wired or wireless, that can carry two-way digital data can carry Internet traffic. Thus, Internet packets flow through wired networks like copper wire, coaxial cable, and fibre optic, and through wireless networks like Wi-Fi. All these networks that share the same protocols form the Internet.

Some of the popular services on the Internet that make use of these protocols are e-mail, file sharing, Instant Messenger, and the World Wide Web. Of these, e-mail and the World Wide Web are clearly the most used, and many other services are built upon them, such as mailing lists. Increasingly, companies and individuals are making use of web-logs or blogs, which are largely used as easily updatable online diaries, which are also based on the WWW and underlying databases.

Furthermore, the Internet makes it possible to provide real-time services such as online radio and even TV (IPTV) that can be accessed from anywhere in the world, provided that there is broadband access to the Internet.

The World Wide Web (WWW)

The term WWW is often mistakenly used as a synonym for the Internet, but the Web is actually a service that operates over the Internet. At the same time, without the WWW the Internet would not be the way we know it today. Websites are identified by global identifiers called Uniform Resource Identifiers (URLs, e.g. www.osce.org).

To understand this distinction, remember that

- The World Wide Web, sometimes referred to as the Web, is an interconnected set of documents and files linked together by hyperlinks whereas
- The Internet, or sometimes just the Net, is an interconnected set of computers and computer networks, linked to each other by copper wires, fibre-optic cables, or wireless links etc.

Through keyword driven Internet research using search engines like Google, millions worldwide have easy, instant access to a vast and diverse amount of online information. Compared to encyclopedias and traditional libraries, the World Wide Web has enabled a sudden and extreme decentralization of information and data, most of which can be accessed through websites.

Domain Name and IP Address

Every website, e-mail account, etc., on the Internet is hosted on a computer (server). Each server has a unique IP address which is just a set of numbers, such as 194.8.63.155. To access a particular Internet service, one can type in this IP address in an appropriate application, such as web browsers like Safari, Internet Explorer or Firefox, to reach a website.

However, because it is difficult to remember numbers, an IP address can be associated with a domain name, e.g. osce.org. A domain name is a name of a computer on the Internet that distinguishes it from the other systems on the network. They are sometimes colloquially referred to as web addresses.

Translating numeric addresses to alphabetical ones, domain names allow Internet users to localize and visit websites. Converting a number address (194.8.63.155) to a more readable domain name (www.osce.org) is done via the Domain Name System (DNS). The process of conversion is known as resolution of the domain name.

The Domain Name System – An Introduction

Top Level Domains (TLDs)

The right-most section of a domain name is called the top-level domain (TLD), e.g. .com, .biz, .uk, .de. Some exhibit no affiliation with a particular country (like .com) others consist of a country code. Thus, the top-level domains classified by the Internet Assigned Numbers Authority (IANA) are:

- Country code top-level domains (ccTLD): Used by a country or a dependent territory. It is two letters long, for example .de for Germany or .fr for France. These ccTLDs are operated by so-called registries or Network Information Centers (NICs), some of which have signed a contract with ICANN, some which have not.
- Generic top-level domains (gTLD): Used (at least in theory) by a particular class of organization (for example, .com for commercial organizations). It is three or more letters long. These are operated by registrars appointed by ICANN. Most gTLDs are available for use worldwide, but for historical reasons .gov and .mil are restricted to the government and military of the USA.

ICANN has overall responsibility for managing the DNS. It controls the root domain, delegating control over each top-level domain to a domain name registry.

ICANN

ICANN is the Internet Corporation for Assigned Names and Numbers. It is a private Californian non-profit corporation consisting largely of Internet Society Members, and was created under US Government contract on 18 September 1998 in order to take over a number of Internet-related tasks previously performed on behalf of the US Government by other organizations, notably IANA.[7]

[7] Further information about ICANN can be found in the articles by Nico van Eijk and Wolfgang Kleinwächter.

ICANN is responsible for co-ordinating the management of the technical elements of the DNS to ensure universal resolvability so that all users of the Internet can find all valid addresses. It does this by overseeing the distribution of unique technical identifiers used in the Internet operations, and delegation of Top Level Domain names (such as .com, .info, etc.).

ICANN is also responsible for accrediting the domain name registries. “Accredit” means to identify and set minimum standards for the performance of registration functions, to recognize persons or entities meeting those standards, and to enter into an accreditation agreement that sets forth the rules and procedures applicable to the provision of registry services.

For ccTLDs, the domain registries take different forms, some are run by a university, an independent authority or institution, an industry association or exist in many other forms. ICANN has a consultation role in these domain registries but is in no position to regulate the terms and conditions of how a domain name is allocated or who allocates it in each of these country level domain registries. On the other hand, generic top-level domains (gTLDs) are governed directly by ICANN which means all terms and conditions are defined by ICANN with the co-operation of the gTLD registries.

Domain Name Registry

In the Domain Name System on the Internet there is a need for databases to be kept of which domain name maps to which IP address. A domain name registry has two main tasks:

1. Allocating domain names under their top level domain to those who ask for them; and
2. Making the database of domain name registrations available to the world at large.

Registries can only operate if the top level domain they run has been delegated to them by IANA, nowadays a part of ICANN. Hence, there can only be one registry for each top level domain. If there was more than one index, confusion would result.

Registries make the index available to the world via their name servers for the direction of Internet traffic. Such systems have to be fully redundant because a loss of name servers would affect all Internet traffic sent to that domain.

Registry, Registrar, Registrant

There are over 243 ccTLDs, most of which correspond to the two-letter country codes. Each country appoints a registry for its ccTLD and sets the rules for allocating domains. Some countries allow anyone in the world to acquire a domain in their ccTLD, for example Armenia (am), Austria (at), Germany (de), Tonga (to), or Tuvalu (tv). This has resulted in domain names like I.am, start.at and go.to. Other countries or dependent territories allow only residents to acquire a domain in their ccTLD, for example Canada (ca).

The registry holds the central register and operates the name servers for that domain. They will generally set policies for the names it controls. Some restrict certain names for political, religious, historical or local legal reasons. Equally, ccTLD registries set the dispute policies for their names. Those that have signed up with ICANN generally have to use the Uniform Domain Name Dispute Resolution Policy (UDRP), while for example German DENIC requires people to use the normal German civil courts, and Nominet UK deals with intellectual property and other disputes through its specific dispute resolution service.

The ccTLD registries may also decide whether matters of interest to their local communities are introduced: for example, the Japanese and Polish registries have introduced internationalized domain names to allow use of local non-ASCII[8] characters.

In the gTLD system registries are not as unified, although the Public Interest Registry which runs .org comes close. Normally, in the gTLD system ICANN holds a basic register which records the name, other important details, and which registrar (agent of the registry) runs that name. The registrar holds the other details like the registrant's contact details.

Operation of Registries

Domain name registries, also known as NICs (Network Information Centers) are run in many different ways. Some are government departments (e.g. the registry for Norway norid.no). Some are co-operatives of Internet service providers (such as DENIC nic.de), academia, or non-profit companies (such as Nominet UK nic.uk). Others are commercial organizations, such as the US registry (nic.us). In certain repressive countries, control over the registry and ISPs can effectively dictate what access their citizens have to the Internet. For this reason and to protect freedom of the media on the Internet, the OSCE Media Freedom Representative has repeatedly recommended that there should not be any form of licensing for domain names and that NICs should only take care of the necessary technical procedures in a non-discriminatory fashion.

Domain name registries operate all sorts of systems in order to allot names. Generally they operate a first-come-first-served system of allocation. Some registries sell the names directly and others rely on ISPs or registrars to sell them. All registries have rules about which domain names can be registered. Some of these rules are technical, and therefore universal, but many are cultural, or depend on the nature of the registry. For example, registries differ hugely in their attitude to obscene or libellous domain names.

[8] ASCII is the American Standard Code for Information Interchange, one of the standard sets of characters in information technology.

The level of charges for a domain name depends on the nature of the registry. Commercial registries naturally tend to charge what the market will bear, whereas non-commercial registries tend to charge less. Especially in countries where the Internet community is still small, prohibitively high prices might hinder the development of networks and access to the Internet.

Some domain name registries also impose a system of second level domains on users (e.g. amnesty.org.uk). The argument for such domains is that it allows more space and certainty in the system; for example, individuals cannot occupy governmental organizations' domains (e.g. homeoffice.gov.uk) and individuals are given domain names that differ from that given to companies. The argument against this is that it leads to less memorable names and fragments the system.

Contrasting approaches can be seen in three of Europe's biggest registries. For example, DENIC, the registry for Germany (.de) does not impose second level domains. AFNIC, the registry for France (.fr) has some second level domains, but not all registrants have to use them, and Nominet UK, the registry for the United Kingdom (.uk) requires all names to have a second level domain.

The Domain Name System (DNS)

The Domain Name System or DNS is a system that stores information about hostnames and domain names in a type of distributed database on the Internet. Of the many types of information that can be stored, most importantly it provides a physical location (IP address) for each domain name, and lists the mail exchange servers accepting e-mail for each domain.

The DNS provides a vital service on the Internet as it allows the transmission of technical information in a user-friendly way. While computers and network hardware work with IP addresses to perform tasks such as addressing and routing, we generally find it easier to work with hostnames and domain names in URLs and e-mail addresses (such as osce.org instead of 194.8.63.155). It could be said that the DNS mediates between the needs and preferences of humans vs. those of computers.

How the DNS Works in Theory

Meet the Players

The practical operation of the DNS system consists of three players:

- The DNS resolver, a DNS client program which runs on a user's computer and generates DNS requests on behalf of software programs;
- The recursive DNS server, which searches through the DNS in response to queries from resolvers and returns answers to those resolvers; and,
- The authoritative DNS server which answers queries from recursors, or refers them to another authoritative DNS server.

The DNS consists of a hierarchical set of DNS servers. Each domain or subdomain has one or more authoritative DNS servers that publish information about that domain and the name servers of any domains beneath it. The hierarchy of authoritative DNS servers matches the hierarchy of domains. At the top of the hierarchy are the root servers: the servers to query when looking up (resolving) a top-level domain name.

As part of the process of registering a domain name, a registrant provides the registry with the name servers that will be authoritative for that domain name; therefore, when registering osce.org, that domain is associated with name servers at the .org registry. As a result, when a server receives a request, the DNS server scans its list of domains, locates osce.org, and returns the name servers associated with that domain.

Root Server

A root nameserver is a DNS server that answers requests from all over the world and redirects requests for a particular top-level domain to that TLD's nameservers. Root servers are hierachically seen on the top of the Domain Name System. They are run by different institutions and co-ordinated by ICANN. The root servers hold the list of addresses for the authoritative servers for the top-level domains. Every name that is looked up must either start with access to a root server, or use information that was once obtained from a root server.

There are 13 root nameservers (named from A to M) on the Internet, the maximum number possible. No more names can be used because of protocol limitations. However, the C, F, I, J and K servers now exist in multiple locations on different continents, using so-called anycast announcements to provide a decentralized service. As a result most of the physical, rather than nominal, root servers are now outside the United States. Thus, an additional level of redundancy is provided by the fact that a single root server name, and its corresponding IP address, may correspond with many physical servers around the world. For example, root server K, run by RIPE, consists of 16 computers on all continents except for Africa.

Root server A in Herndon/Virginia run by VeriSign plays a central role. It contains the data basis for all other root servers and transmits these data twice a day to all other servers. The root DNS servers are essential to the functioning of the Internet, as so many protocols use DNS, either directly or indirectly. They are potentially points of failure for the entire Internet.

The Future of the DNS

The Domain Name System is certainly one of the main means governing the Internet on the technical level. At the same time, Internet Governance goes far beyond these technical issues. But social or cultural implications of technical innovations are hard to understand without an insight into the underlying technology.

ICANN does have the ultimate control on the root zone and approves (or disapproves) new TLDs. For example the rejection of the gTLD .xxx has sparked off vivid discussions among Internet technicians but also free speech activists, who fear content-based restrictions of originally technical procedures, like adding TLDs to the root zone.

At the same time it can be noted that ICANN isn’t an Internet government, but has a – technically important – limited role. What is more, the debate about TLDs and the root zone might become more and more irrelevant in the future, some experts say, because websites are increasingly accessed through search engines and less by means of memorizing domain names and through the DNS. The future will show how technology affects our online environment and to what extent policy makers can influence this process.

The History of Internet Governance

Wolfgang Kleinwächter

When the term “Internet Governance” was introduced in the 1980s it was used mainly to describe the specific type of technical management of the global core resources of the Internet: domain names, IP addresses, Internet protocols and the root server system.

The term “Governance” was used to draw a distinction with “Government”. While earlier technological innovations like the telegraph in the nineteenth century or radio broadcasting in the early twentieth century immediately prompted governmental regulation in the form of telecommunication and broadcasting laws, there were no comparable governmental activities when the Internet emerged. The necessary regulation was mainly technical by nature and done by the technicians, the providers and users of the Internet themselves.

Governance without Governments

The mainstream philosophy in these early days of the Internet among the Internet pioneers was that there is no need for the involvement of governments. Furthermore, many Internet experts rejected any role for governments in the emerging cyberspace. Dave Clark from the Laboratory of Computer Science at the Massachusetts Institute of Technology (MIT) set the tone in a speech to the Internet Engineering Task Force (IETF) in 1992, titled “A Cloudy Crystal Ball – Visions of the Future”. In his paper he formulated a principle which became the Leitmotiv for the global Internet community:

"We do not believe in kings, presidents and voting. We believe in rough consensus, factual approach and running code."[9]

Tim Berners-Lee, the inventor of the World Wide Web said later: "There is the idea that society can run without a hierarchical bureaucratic government being involved at every step, if only we can hit on the right set of rules for peer-peer interaction. So where design of the Internet and the Web is a search for a set of rules which will allow computers to work together in harmony, so our spiritual and social quest is for a set of rules which allow people to work together in harmony."[10]

The most outspoken and radical concept came later from John Peter Barlow in his "Declaration of Cyber Independence" which he published in Davos in Switzerland on 8 February 1996.[11] In his declaration he described cyberspace as "the new home of mind" where governments are not welcome.

The fear was that as soon as governments started exercising control over the Internet, they would restrict rights and freedoms – in particular the right to freedom of expression and the right to privacy. It was also feared that they would introduce time-consuming and costly procedures which would reduce the speed of innovation on the Internet and block the creation of new Internet services and applications. The preservation of the end-to-end

[9] David D. Clark, "A Cloudy Crystal Ball for the Future", Speech at IETF, 1992, <http://ietf20.isoc.org/videos/future_ietf_92.pdf>.

[10] Tim Berners-Lee, *The World Wide Web and the "Web of Life"* <http://www.w3.org/People/Berners-Lee/UU.html>.

[11] John Peter Barlow, "Declaration of Cyber Independence", Davos, 8 February 1996: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders." <http://www.worldtrans.org/sov/cyberindependence.html>.

principle or the P2P communication model for the Internet was seen as a guarantee of the Net's freedom.

Self-Regulation, private sector leadership and bottom-up policy development were the key elements of the proposed regulatory framework for the Internet. The understanding of "Internet Governance" was based on a concept of "governance without governments".

The reason and justification for such a non-governmental approach came from the practical and successful experiences of the first 20 years of the Internet. The absence of specific governmental legislation was seen by many observers as one of the main reasons for the incredible success of the Internet.

The necessary technical regulation, mainly in the form of codes, standards and protocols, was discussed among the technicians in a bottom-up policy development process which led to a new type of "law", known as a RFC (Request for Comment). Later Lawrence Lessig described Code as the "Law of Cyberspace" and analysed the pros and cons of such an approach. Lessig argued that "in real space we recognize, how laws regulate – through constitution, statutes and other legal codes. In cyberspace we must understand how code regulates – how the software and hardware that makes cyberspace what it is, regulate cyberspace as it is." And he continued: "This code presents the greatest threat to liberal or libertarian ideals, as well as their greatest promise. We can build, or architect, or code cyberspace to protect values that we believe are fundamental, or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground. There is no choice that does not include some kind of building. Code is never found, it is only ever made, and only ever made by us."[12]

[12] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999), p. 6.

Although Internet research and development was continuously financed by the US Government via its "Defence Advanced Research Project Agency" (DARPA), the administration's interference in the day-to-day operations of the researchers and service providers, in particular with governmental regulatory activities, remained low. The role of the US Government was mainly funding the project and retaining ultimate oversight over the process.[13]

The Institutionalization of Internet Governance

An important milestone in the development of Internet self-regulation was the creation of the "Internet Configuration Control Board" (ICCB) in 1979, which was initiated by DARPA. The ICCB became the platform for collaboration of engineers and other groups involved in the development of the Internet at that time. In 1984 the ICCB was transformed into the "Internet Advisory Board", later into the "Internet Activities Board" and in 1992 into the "Internet Architecture Board" (IAB). To this day the IAB oversees the activities of a number of Task Forces like the "Internet Engineering Task Force" (IETF), the main body for the standardization of Internet Protocols and host of the RFC Editor, and the "Internet Research Task Force" (IRTF) which also gradually emerged bottom-up in the 1980s.

[13] It is worth remembering that the Internet emerged as a special project within the "Advanced Research Project Agency" (ARPA). ARPA, like NASA, was established in 1958 by the Eisenhower administration to respond to the challenges of the first Soviet Sputnik which was launched on 4 October 1957. The "Sputnik Shock" had deep consequences for political and military strategic thinking in the United States as it was reflected, *inter alia*, by Henry Kissinger's analysis in his landmark book *Nuclear Weapons and Foreign Policy*, published in 1958 when he was still a professor at Harvard University. Kissinger later became the National Security Adviser and the Secretary of State under US President Richard Nixon. Part of the research at ARPA, which was financed by the US Department of Defence, was a project which aimed to explore the possibility of a decentralized (military) communication network which would make it difficult for the Soviet nuclear Intercontinental Ballistic Missiles (ICBMs) to destroy it with one hit. As a result ARPANet emerged in 1968 as a device for load sharing among the large computers serving research facilities around the country. Its design specifications called for providing secure communications in the event of an outbreak of war, so that no centralized node would be vulnerable to destroying the entire network. The experiments in the 1960s ended successfully. In December 1969 four computers at different US universities were linked together and successfully managed to communicate messages. The option to link computers for communication quickly spread beyond the military sector. When more and more networks emerged, in 1974 two researchers – Vint Cerf and Bob Kahn – developed a protocol known as Transfer Control Protocol/Internet Protocol or TCP/IP. This meant that not only computers but also different networks could communicate with each other. The TCP/IP paved the way towards building a "network of networks" which finally became the "Internet".

In 1992 activists from the various Internet groups, in particular from the IETF, created the "Internet Society" (ISOC) as a not-for-profit educational organization. ISOC also became a platform for discussing political, legal, economic and social implications in the development of the Internet.

The individuals and groups concerned enjoyed a high degree of freedom and independence despite the fact that they were being funded by the US Department of Defence. It is also interesting to note that many of the young researchers and graduate students involved in research projects at US West Coast universities like UCLA, USC, Stanford, Berkeley and others, were politically influenced by the "cultural revolution" of the 1960s, criticism against "the establishment" and the Anti-Vietnam War movement. These groups of young people soon realized the potential of the Internet to explore alternative governance mechanisms. They soon started to form their own constituencies and created non-governmental communication and collaboration mechanisms where they developed innovative organizational political principles and procedures like flat networks instead of high hierarchies and bottom-up policy development processes instead of top-down decision-making.

The majority of the basic Internet specifications and regulations we know today were developed in such bottom-up discussion processes. Pioneers like Steve Crocker, Jon Postel and others invented the "Request for Comments" (RFC) process, the "Root Server System", or the "Domain Name System" (DNS), with its underlying IP address numbering protocols, without any guidance from or consultation with governmental agencies.

These new forms of "governance" represented a rather different culture compared to the way telecommunication networks had been governed. One simple example is the different handling of the allocation of identifiers. Telephone identifiers as individual telephone numbers, including the relevant country and city codes, are heavily regulated both internationally (via the

ITU) and nationally (via telecommunication laws). In contrast the DNS was managed without any governmental regulation. In fact, until the early 1990s it was managed by one man alone: Jon Postel from the Information Science Institute (ISI) at the University of South California (USC). He was also the man who allocated the blocks of IP addresses to the new private Regional Internet Registries (RIR), delegated the management of Top Level Domains (TLD), also for country code based TLDs, and controlled one of the root servers.

While internationally country codes (like codes for car identification or post traffic) are the subject of intergovernmental negotiations and are managed by intergovernmental organizations based on an international treaty, there was no similar mechanism for country codes in the Internet. Governments were not involved in either the creation or the delegation of ccTLDs.

Jon Postel used an existing list of the International Standardization Organization (ISO) and allocated two letter country codes to individual managers in 243 countries and territories listed in ISO 3166. In RFC 1591 Postel said that he “is not in the business of deciding what is and what is not a country. The selection of the ISO 3166 list as a basis for country code top-level domain names was made with the knowledge that ISO has a procedure for determining which entities should be and should not be on that list.”
And he defined the role of a ccTLD manager as a “trustee for the delegated domain” who has “a duty to serve the community.”[14] According to RFC 1591 “the designated manager is the trustee of the top-level domain for both the nation, in the case of a country code, and the global Internet community.” Not one government objected to this process when the first zone files of ccTLDs were put to the Internet Root Server in the middle of the 1980s.

[14] Jon Postel, RFC 1591, March 1994, <http://www.isi.edu/in-notes/rfc1591.txt>.

As the Internet continued to grow at an exceptional rate, in 1988 the US Government encouraged Jon Postel to introduce more stability and security to the established processes and practices and to institutionalize the functions he had thus far executed in managing Internet core resources. As a result the "Internet Assigned Numbers Authority" (IANA) – originally a one-man organization – was established at Postel's Information Science Institute (ISI) in Marina Del Rey.

Following a recommendation by the Department of Commerce (DOC), the ISI entered into a contractual arrangement with the DOC which continued until 1998 when the Internet Corporation for Assigned Names and Numbers (ICANN) was finally established. When the US Department of Defence stopped funding via ARPANET in 1990, the US Government continued to provide financial support through the National Science Foundation (NSF) and shifted legal responsibility to the National Telecommunication and Information Administration (NTIA) of the US Department of Commerce (DOC).

Broadening the DNS: WWW, ISOC and IAHC

The environment for the development of the Internet and the management of Internet resources like root servers, IP addresses and domain names, changed dramatically when Tim Berners-Lee invented the World Wide Web at the CERN Institute in Geneva in 1990. Postel realized immediately that the new options on the Web would lead to a dramatic growth of Internet usage. While he was sure that the basic architecture of the Internet could accommodate all the expected growth, he concluded that the DNS needed further expansion. Consequently he investigated options for a more advanced management system for Internet core resources which went beyond a one-man institution and involved other emerging constituencies around the world.

His first idea was to use the "Internet Society" (ISOC), established in 1992, as an umbrella organization. In 1994 he proposed adding 150 new generic

Top Level Domains (gTLDs) to the existing Domain Name System consisting of seven gTLDs[15] and 243 ccTLDs in 1994.

Postel's initiative was not co-ordinated with the US Department of Commerce. Network Solutions Inc. (NSI), a private company based in Herndon/Virginia which managed .com, .net, and .org as well as the A Root Server, was rather angry about such an initiative. In 1992 NSI had been given a contract by the DOC to be the sole domain name registrar for the three gTLDs .com, .net and .org. Based on such a monopoly position NSI saw in the emerging domain name market a grandiose new business opportunity. Consequently, NSI opposed the Postel plan to introduce 150 competitive gTLDs at this early stage in the development of a global domain name market. NSI lobbied the US Congress and the DOC, which finally intervened with Postel's plan and stopped the handover of the DNS management to ISOC and the introduction of 150 new gTLDs.

Postel's frustration about this governmental intervention prompted him to look for other options. He approached the Geneva based International Telecommunication Union (ITU), which after its Plenipotentiary Conference in Kyoto in 1994 had started a reform process and had opened itself up to private sector members. Postel's idea was to create a new form of public-private partnership for Internet Governance by bringing technical organizations, private sector institutions and intergovernmental organizations together, launching a bottom-up policy development process and creating a new form of oversight body for the management of some of the key Internet resources. Postel pushed for the establishment of an "Interim Ad Hoc Committee" (IAHC) which was formed in summer 1996.

The IAHC started drafting a text for a Memorandum of Understanding for new gTLDs. The members of the IAHC were ISOC and Postel's IANA, the

[15] .com, .net, .org, for global use, .gov, .edu and .mil for use in the US and .int for intergovernmental organizations.

Internet Architecture Board (IAB), the International Trademark Association (INTA), the ITU and the World Intellectual Property Organisation (WIPO). By inviting WIPO and INTA, Postel was reacting to the growing concerns of the IP and trademark community in the US which was confronted with the new phenomenon of cybersquatting and the misuse of registered trademark names in the DNS. By inviting the two UN specialized agencies he also wanted to respond to the concerns of a growing number of governments about their future role in the management of the Internet.

The six members of the IAHC agreed on basic aims, principles, procedures and institutions after one year of negotiations. On 2 May 1997 they signed a Memorandum of Understanding (gTLD-MoU) in Geneva which was heralded by ITU Secretary-General Pekka Tarjanne as a turning-point in international law. According to the gTLD-MoU a so-called Policy Oversight Committee (POC) with representatives from the six organizations was the main decision-making body. The POC was made responsible for key elements in the management of Internet core resources including the licensing of new gTLDs registries and registrars. A Policy Advisory Committee (PAC) was to give other stakeholders an opportunity to become part of the process by providing advice to the POC.

Within the POC, the technical community with six representatives (from IANA, ISOC and IAB) was to have the formal majority over three members from governments (ITU and WIPO) and three from the private sector (INTA and the newly established Council of Registrars/CORE). The plan was to launch seven new gTLDs as soon as possible, to license registrars for domain name registration in the gTLD name space and to move the A Root Server from Herndon/Virginia to Lac Léman in Geneva.

Again the US Government, and in particular NSI, was not amused about Postel's initiative and did not support such an approach. On the contrary, US Secretary of State, Madeleine Albright wrote a critical letter to ITU Secretary-

General Pekka Tarjanne arguing that he had gone beyond his mandate by signing such a gTLD-MoU without any formal consultations with ITU Member States, including the US Government.

The Making of ICANN

Seven weeks after the signing of the IAHC gTLD-MoU in Geneva, the Clinton administration started an alternative process aiming to privatize the management of the DNS. Referring to the termination of the contract between the DOC and the ISI, the US Government published a Green Paper in July 1997 asking for proposals for the creation of a new private not-for-profit corporation (NewCo) to become the new global manager of the Internet core resources.

The European Union supported in principle the idea of privatizing the DNS. But it criticized the US centric approach of the Green Paper. In a rather critical comment about the Green Paper the European Commission wrote: “The European Union and its Member States would wish to emphasize our concern that the future management of the Internet should reflect the fact that it is already a global communication medium and the subject of valid international interests.”[16]

Ira Magaziner, US President Clinton’s Internet adviser and the main architect of what later became ICANN, replied in a hearing before the US Congress to the European criticism: “The purpose of the Commerce Department proposal is to improve the technical management of the DNS only. The Green Paper does not propose a monolithic Internet Governance system. Frankly we doubt that the Internet should be governed by a single body or plan.” Magaziner recognized that “the Internet has become an international

[16] Reply by the EU and its Member States to the US Green Paper on Internet Governance, Brussels, 20 March 1998. The EU called “to reach a balance of interests and responsibilities, so that the international character of the Internet is recognized with respect to the relevant jurisdictions around the world”.

medium for commerce, education and communication" and "has outgrown the legacy system of technical management".[17] He accepted the idea of an "international representative body" and proposed that the composition of a board of directors of a NewCo should be balanced and represent the functional and geographic diversity of the Internet.[18] This later enabled the EU Commissioner Martin Bangemann to support the concept of privatization of the DNS.

The principles of stability, competition, bottom-up policy development and global representation emerged from the discussion of the Green Paper. Jon Postel again changed his plans and took active part in the debate which led to a White Paper, published in June 1998 by the US Department of Commerce.

The impending termination of the contract between the ISI and the DOC pushed the debate forward. The White Paper, which included the four above-mentioned principles, paved the way for the final creation of ICANN. In September 1998 Jon Postel presented a set of draft by-laws for NewCo called Internet Assigned Names and Numbers Corporation in a Hearing at the US Congress and was given the "green light" to move forward. He said in the Hearing: "We listened to everyone who wanted to offer comments or suggestions, and we then tried to turn those suggestions into actual documents. Group discussion is very valuable, group drafting less productive." And he added: "This new organization will be unique in the world – a non-governmental organization with significant responsibilities for administering what is becoming an important global resource."[19]

[17] Ira Magaziner, *Written Statement to a Hearing on Domain Name Issues before the Sub-Committee on Basic Research of the Committee of Science of the House of Representatives*, Washington, 31 March 1998.

[18] In the Interim Board, which was formed in November 1998, there were five North Americans, three Europeans and two representatives from the Asia-Pacific region.

[19] Jon Postel, Testimony before the Sub Committee on Basic Research of the Committee on Science of the House of Representatives, Washington, 7 October 1998.

In November 1998 ICANN was formally established by incorporation under the "California Nonprofit Public Benefit Corporation Law for Charitable and Public Purposes". At the same time ICANN entered into a new Memorandum of Understanding with the DOC. Unfortunately Jon Postel died just days before the creation of ICANN after heart surgery in November 1998.

ICANN was designed as a multi-stakeholder organization under private sector leadership. In its original by-laws the Board of Directors, the highest decision-making body, was to consist of nine representatives from the private sector and the technical community and nine representatives from the so-called At Large Membership (ALM), representing the Internet users and civil society. Governmental representatives were not eligible for the board. Instead the 190 governments of the UN Member States were invited to form a "Governmental Advisory Committee" (GAC) and to give advice to the board, if needed. The point was that according to ICANN by-laws, GAC advice was not legally binding for the ICANN Board.

ICANN's First Two Years

The creation of ICANN made the IAHC gTLD-MoU obsolete. Formally the gTLD-MoU was tabled during the ITU Plenipotentiary Conference at Minneapolis in October 1998. But it was not adopted. On the contrary, the US Government lobbied for an ITU resolution in which the ITU Member States recognized the principle of "private sector leadership" for Internet Governance. The Clinton administration planned to terminate the MoU with ICANN after two years and to give ICANN full independence at the end of the year 2000.

ICANN started its work in spring 1999. It soon became clear that its agenda was much more complex than expected. Although ICANN attained quick results in some areas – in particular in opening up the market for domain name registration and developing a system for the resolution of domain name conflicts (Universal Dispute Resolution Policy/UDRP) – in other areas progress was slow.

The idea that Internet users should have half of the seats on the Board produced a lot of problems and confusion, particularly about how the nine ALM directors should be elected. A trial with a global online election of five regional ALM directors in summer 2000, in which nearly 150,000 Internet users participated, produced mixed results and called for further research and reconsideration.

Furthermore, the relationship between the ICANN Board and the managers of the ccTLD caused a lot of tension. The majority of ccTLD managers did not accept ICANN's leading role and operated rather independently under the national jurisdiction of the respective country. They were only interested in an informal technical service arrangement with regard to the root zone file management of their ccTLD.

The introduction of new gTLDs also produced more conflicts than expected. After a call for proposals, where nearly 100 projects were presented, in December 2000 ICANN adopted seven new TLDs for a test phase (.info, .name, .biz, .coop, .museum, .pro, .aero). Additional problems arose, in particular with regard to the WHOIS database and internationalized domain names, and this all led to an increase in ICANN's workload.

As the date for terminating the ICANN-DOC-MoU approached, it became clear that more "homework" was needed before ICANN could attain full independence. In October 2000, the Clinton administration extended the MoU for another year handing over the issue to the next US administration.

ICANN's Reform

Former Vice President Al Gore, who was directly involved in the making of ICANN, lost the 2000 presidential election and the new President George W.

Bush had a different agenda with regard to the Internet. While for the Clinton administration the Internet had high priority, for the Bush administration it was low priority. The Bush campaign was mainly financed by the old industrial giants, not by the Silicon Valley companies which showed more support for Al Gore. Furthermore the year 2000 witnessed the burst of the .com bubble and the collapse of the so-called new economy called for a more critical approach to the concepts of self-regulation and “governance without government”.

This was heightened after the terrorist attacks of 11 September 2001. The Bush administration redefined the Internet infrastructure as a “critical infrastructure” for US security and US economy and it called for a new more security-oriented approach to Internet Governance. ICANN, which had started partly as a project for “Cyberdemocracy” now became a project for “Cybersecurity”.

In December 2001, ICANN’s new CEO Stuart Lynn started a reform process. Within 12 months ICANN’s by-laws were rewritten. A new structure of the Board, of the main supporting organizations and of the advisory committees emerged. And the relationship between the ICANN Board and the Governmental Advisory Committee (GAC) was adjusted.

According to the new by-laws the ICANN Board is now obliged to give an explanation to the GAC if it rejects its advice. Furthermore in such a case the GAC can ask for “consultations”. If consultations fail, the ICANN Board is obliged to explain this failure to the global Internet community and governments reserve their right to act independently from ICANN’s decisions. Although such a procedure does not directly *de jure* introduce a governmental veto right, it can be interpreted de facto as such a right by substantially rebalancing the power in the relationship between the private sector in the ICANN Board and the governments in the GAC.

Another change affected the role of the At Large Membership. The new by-laws eliminated the nine At Large Directors and the option of direct elections and placed the Internet users in an "At Large Advisory Committee" (ALAC) which was given the right to send one non-voting director to the Board. A new Nominating Committee (NomCom) was created and given the mandate to select half of the Board members.

The Internet Governance Controversy during the Geneva Phase of WSIS

When ICANN's reform process was successfully ended by the adoption of the new ICANN by-laws in Amsterdam in December 2002, the issue moved one level higher and became more of a political controversy within the process of the UN sponsored World Summit on the Information Society (WSIS). During the preparation for the first WSIS Summit in Geneva in December 2003, more and more governments started to look deeper into the political implications of the management of the Internet in general and its core resources in particular.

A substantial number of governments criticized ICANN for being under the control of the US Government and called for a broader involvement in decision-making with regard to Internet development. The Chinese Government, supported by a majority from developing countries, proposed discussing an International Internet Treaty and the formation of an Intergovernmental Internet Organization. Private sector leadership was good in the early days of the Internet when there had been no more than one million users. Now with one billion Internet users, the Chinese argued, the time was ripe for governmental leadership in the management of Internet resources.

The Internet Governance conflict overshadowed the final preparations for the Geneva Summit in December 2003. The controversy was further fuelled by the unclear definition of Internet Governance. Some groups reduced Internet

Governance to the management of the technical Internet core resources; for others Internet Governance included all public policy issues related to the Internet, including eCommerce, cybercrime and freedom of expression.

The different definitions led to different conclusions. The supporters of the "narrow definition" argued in favour of a continuation of the role of ICANN and private sector leadership in the management of the technical core resources. The supporters of the "broad definition" argued in favour of an enhanced role of the ITU and the principle of governmental leadership.

The problem was – and still is – that when it comes to the Internet core resources it is not so easy to separate the political from the technical issues. Even purely technical questions like the allocation of IP numbers, the introduction of domain names or the management of root servers, have political, legal and economic implications and affect market developments and the security and stability of the Internet.

Until the end of the Geneva negotiations, the US Government, backed by the Europeans, continued to support the principle of private sector leadership based on a narrow definition. China and the Group of 77 called for governmental leadership based on the broad definition. While at the end of the day both groups agreed that all stakeholders – governments, private sector and civil society as well as intergovernmental and non-governmental organizations – have to play a certain role in Internet Governance, a consensus about these roles was not reachable.

The compromise was to ask the UN Secretary-General to establish a "Working Group on Internet Governance" (WGIG) and to give the group a mandate to elaborate a definition of Internet Governance, to identify the public policy issues related to Internet Governance and to specify the roles and responsibilities of the main stakeholder groups. Probably one of the most important agreements was the consensus over the composition of the WGIG. According to para. C6.13b of the Geneva Plan of Action the group should be set up "in an open and inclusive process that ensures a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries, involving relevant intergovernmental and international organisations and forums."[20]

The Working Group on Internet Governance

UN Secretary-General Kofi Annan established the WGIG in November 2004. The WGIG had forty members. More than half of them represented non-governmental stakeholders from the private sector, civil society, the technical and the academic community.

WGIG presented its final report in July 2005. It proposed a broad definition of Internet Governance which included much more than just names and numbers. The report defines Internet Governance as "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."[21] Furthermore it produced a list of 17 public policy issues related to Internet Governance and formulated specific roles and responsibilities for the different stakeholders.

WGIG concluded that the Internet should not be governed by a single entity but its management should be improved by better communication, co-ordination and co-operation among different organizations and stakeholder groups. WGIG recommended, *inter alia*, introducing a new high-level discussion space for Internet Governance issues by the creation of an "Internet Governance Forum" (IGF), which does not have any decision-

[20] WSIS Plan of Action, Geneva, 13 December 2006 at <www.wsis.org>.

[21] Final Report of the Working Group on Internet Governance, Geneva, July 2005, <http://www.wgig.org/docs/WGIGREPORT.doc>.

making capacity, instead of a new UN Internet governmental organization. WGIG could not agree about the oversight function and the specific role of the US Government in issues like the authorization of TLD root zone files and the oversight over ICANN based on the MoU. In 2003 the ICANN-DOC MoU was extended until October 2006.

The WGIG recommendations became the basis for the final negotiations during the third meeting of the WSIS Preparatory Committee (PrepCom3) in September 2005 in Geneva.

Before the restart of the WSIS negotiations, the US Department of Commerce published a statement reiterating four basic principles for Internet Governance. In the statement of 30 June 2005, the US Government made it clear that it was not considering relinquishing its special role and responsibility. “The United States Government intends to preserve the security and stability of the Internet’s Domain Name and Addressing System (DNS). Given the Internet’s importance to the world’s economy, it is essential that the underlying DNS of the Internet remains stable and secure. As such, the United States is committed to taking no action that would have the potential to adversely impact the effective and efficient operation of the DNS and will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file.”[22] In the same statement, the US Government also recognized sovereign governments’ interests with regard to their ccTLDs. Furthermore the DOC reconfirmed its full backing of ICANN’s role as the main technical organization for the management of the Internet core resources. And it supported a continuing dialogue on Internet Governance within and outside existing organizations.

[22] US Principles on the Internet’s Domain Name and Addressing System, US Department of Commerce, Washington, 30 June 2005, <http://www.ntia.doc.gov/ntiahome/domainname/USDNSprinciples_06302005.htm>.

While the main point in the US statement was certainly the reconfirmation of the oversight role, justified with the argument that such a role is needed to guarantee the stability and security of the Internet, the other principles had equal importance. The formal recognition of the national sovereignty of a government over the domain name space defined by its ccTLD was in particular of interest for the Government of the Peoples Republic of China and many governments in Third World countries. These governments feared that the present Internet management system would allow the US Government to interfere into their national Internet policies and harm Internet communication by blocking the publication of the ccTLD zone file in the Internet root. The assurance that the US Government does not intend to interfere with communication related to the ccTLD was an important message for developing countries and eased the negotiations when the diplomats came back to Geneva in September 2005.

During PrepCom3, the Chinese Government no longer insisted on the creation of an intergovernmental Internet oversight body. Brazil and India again argued in favour of an intergovernmental Internet Convention but they did not formally table a draft. The only concrete proposal for further development of the existing mechanism came from the European Union.

The European Union proposed at the end of PrepCom3 a “new co-operation model” based on the concept of a public-private partnership. The basic idea of the EU proposal was that the day-to-day operations – as executed by ICANN – should continue to be managed by the private sector. However, governments should play a more active role on the “level of principle”.

The US Government rejected the proposal with the argument that the Europeans did not explain in detail the borderline between the “level of principle” and the “day-to-day operations”. The US Government argued that a vague separation of responsibilities could lead to a silent mission creep by a new intergovernmental body which would end in the installation of a UN-type control mechanism over the Internet as a whole.

The US-EU controversy over the Internet moved to the highest level. US President George W. Bush raised the issue with the President of the European Commission, José Manuel Barroso when he visited Washington in October 2005. US Secretary Condoleezza Rice wrote a letter to the British Foreign Secretary Jack Straw, who had the rotating EU presidency in the second half of the year 2005, and argued against the establishment of a "new co-operation model" for Internet Governance. The debate became overheated when a number of Senators published warnings in the US Congress that they would reject any efforts towards a "UN take over of the Internet".

Neither WGIG nor the EU proposed such a take over. UN Secretary-General Kofi Annan himself rejected such an ambition in an article for the *Washington Post* and declared that the UN does not plan to take over the Internet. The Europeans also made clear that it is not their intention to introduce an intergovernmental control mechanism over the Internet. Such declarations helped to cool down the heated controversy and to prepare for a compromise in the final negotiations before the Summit in Tunis in November 2005.

The Tunis Compromise

The final compromise was reached just hours before the opening of the Tunis Summit. At the end all parties could agree on a number of basic principles for Internet Governance, on the establishment of an Internet Governance Forum (IGF) and on the launch of a process for enhanced co-operation.

The principles for Internet Governance include such important precepts like the recognition of national sovereignty over the ccTLD domain name space and the involvement of all stakeholders – private sector, civil society and governments in their specific roles and responsibilities – in all forms of Internet Governance. Of special importance is the principle "that all governments should have an equal role and responsibility for international Internet Governance and for ensuring the stability, security and continuity of the Internet."[23] This paragraph was seen as a political success for governments which had criticized the special role of the US Government, in particular in overseeing the Internet root and ICANN. On the other hand, it did not include any procedure for a gradual change of this historic role of the US Government.

Less controversial was the adoption of the resolution for the creation of the "Internet Governance Forum" (IGF). The IGF was seen as the substitute for the proposed new intergovernmental body. The important point of the IGF is that it is designed as a multi-stakeholder forum without any decision-making capacity. The expectation is that the high level discussion will produce important messages which will be taken into account when organizations with a decision-making mandate for specific issues prepare projects and treaties. Examples of these organizations are ICANN for domain names, IETF for standards, the ITU for infrastructure and UNESCO for multilingualism. The IGF was constituted for five years and will take place annually under the umbrella of the UN Secretary-General.

The agreement on the launch of a process towards "enhanced co-operation" disguised the fundamental dissent over the future of Internet oversight. The Tunis document does not offer any precise definition of what "enhanced co-operation" means. While the US Government interprets enhanced co-operation as nothing more than a more effective collaboration among existing organizations involved in Internet issues – from the ITU and WIPO to ICANN and IETF – other governments see this process as the beginning of a new organizational structure which will eventually lead to a "new

[23] See para. 68 of the Tunis Agenda for the Information Society.

co-operation model" as proposed by the European Union. However, the compromise formula allowed all parties to keep face and left the door open for future innovative developments.

Internet Governance in the Post Tunis Phase

In 2006 the Internet Governance debate continued in a less controversial climate. Some important steps had been taken to implement some of the Tunis decisions.

Most important was the substitution of the ICANN-DOC-MoU with a new "Joint Project Agreement" (JPA) between ICANN and the DOC. The JPA gives ICANN a little more independence from the US Government. ICANN is not obliged anymore to report periodically to the US Department of Commerce but has to report annually to the global community. Furthermore there is no more subordination, but ICANN is obliged to have "consultations" with the DOC on a regular basis. The JPA will terminate in October 2009 and it is expected that ICANN will be fully independent after this date. The EU Commissioner Viviane Reding welcomed the JPA, underlining the point that this new agreement is a step in the right direction of reduced governmental involvement in the day-to-day management of Internet resources.

ICANN itself has sped up its reform process in 2006 and 2007 by trying to position itself more as a global organization, *inter alia* by opening more regional offices and creating a network of 13 regional liaisons. Furthermore, ICANN improved its relationship with the ccTLDs by entering into formal or informal arrangements with key ccTLD managers. It enlarged the role of the At Large Membership via the conclusion of MoUs with emerging Regional At Large Organizations (RALOs) from Latin America, Africa, Asia and Europe. And it finalized policies for the introduction of new gTLDs, for internationalized domain names and the future management of the WHOIS database. Additionally the relationship between GAC and the ICANN Board was further improved and institutionalized via closer co-operation in working groups and task forces. However conflicts with the GAC, like the introduction of the .xxx TLD or the level of data protection in the WHOIS database, remain issues for further debate.

The first Internet Governance Forum (IGF) took place in November 2006 in Athens and was a great success. More than 1,500 experts – representing all stakeholder groups from developed and developing countries – discussed in six plenary sessions and more than 30 workshops on a high level key Internet issues like openness, diversity, access and security.

The IGF with its multi-stakeholder mechanism was seen as a real innovation in international politics. Although it was under the umbrella of the UN, the IGF did not follow UN procedures. There were no special name badges, reserved seats or special speaking rights for the individual stakeholder groups. Governmental and non-governmental experts discussed on equal footing. The decision not to draft a final document liberated such a discussion from the pressure to agree on certain issues at the end of the meeting. Such informality gave the IGF additional dynamics which also led to another political innovation: the creation of so-called “Dynamic Coalitions” on Internet issues like Spam, Cybersecurity, Privacy or Freedom of Expression by representatives from governments, the private sector and civil society on a voluntary basis.

The messages of the IGF were summarized in concluding remarks by the Chair and it remains to be seen how seriously these messages will be taken by the relevant organizations and institutions.

The IGF itself was prepared by a multi-stakeholder “IGF Advisory Group”, nominated by the UN Secretary-General. The IGF-AG worked under the chairmanship of Nitin Desai, a former Deputy Secretary-General of the United Nations who has already served as the Chairman of the Working Group on Internet Governance (WGIG).

Finally the process of enhanced co-operation has started in the form of informal consultations, mainly among governments themselves. It will be some time before the different parties are able to draft concrete ideas and proposals about how such co-operation could be implemented. The ITU Plenipotentiary Conference in Antalya/Turkey in November 2006, adopted, *inter alia*, a resolution which called the ITU Secretary-General to ask Member States and sector members about their approach to the process of enhanced co-operation. At the same time, the newly elected ITU Secretary-General Hamadoun Touré stated clearly that the ITU under his leadership has no intention "to govern the Internet". In 2009 the ITU will host its own "World Telecommunication Policy Forum" (WTPF) dealing with Internet issues.

Looking Towards Internet Governance in 2010

An important future milestone could be the year 2010. In 2010 the Joint Project Agreement (JPA) between ICANN and the US Government will have terminated. In 2010 the mandate of the Internet Governance Forum (IGF) comes to an end. And in 2010 the ITU has its next Plenipotentiary Conference in Mexico City.

It is too early to forecast what the environment of Internet Governance will be in the year 2010. Issues like internationalized domain names, alternative roots or net neutrality, cybercrime, eCommerce and individual human rights on the Internet will probably become more important than the authorization of the publication of root zone files. Yet whatever the future holds in store of a few things we can be certain. In the year 2010 there will be nearly two billion Internet users and there will never be an end to the debate on how the Internet should be globally managed.

Institutional Aspects of Internet Governance

Nico van Eijk and Katerina Maniadaki

Introduction

Internet Governance is a very broad concept. It is widely used (and abused) to deal with at least two matters. First of all, Internet Governance is a term that reflects institutional issues ("Who controls the Internet?"); second, the notion of Internet Governance is strongly linked to debates on the content that is transported over the Internet and the function of the Internet for society. This contribution is about the first type of Internet Governance, and in particular about the most central addressing/routing structure of the Internet, namely domain names. Domain names are the prime instrument to structure the Internet so that information can be found. They are also at the core of communication between users, as they provide an essential element for the use of e-mail addresses.

In this article we first describe in very general terms the international institutional context of domain names, with a focus on country code top-level domain names (ccTLDs), such as .nl, .de and .uk. In sections 3 and 4, we provide information on the national aspects of domain naming. In particular, we give a detailed description of the European framework for assigning .eu domain names. This description covers most of the relevant "national" governance issues and may therefore serve as an example or a checklist for the regulation of national domain names.

Global Issues Related to Domain Naming

The WSIS

Although the Internet Governance debate has been going on for some time, the UN World Summit on the Information Society (WSIS) represents a clear demarcation point. The WSIS – which held meetings in 2003 (Geneva) and 2005 (Tunis), and subsequently created the Internet Governance Forum (2006) – is the first more coherent attempt to structure the global debate on Internet Governance in its broadest sense. The Working Group on Internet Governance (WGIG), one of the supporting activities in this process, gave the following 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.[24]

As indicated, this article focuses on only some of the governance issues concerning the allocation of domain names.

What was discussed and concluded during these WSIS activities as far as domain names are concerned? When we look at the declaration of principles that resulted from the Geneva conference, it is important to notice that it strongly promotes the responsibility of all stakeholders involved.[25] This is an important element because sometimes the debate about who controls the Internet is dominated either by those who want the Internet to be in the hands of governments (or who support strong governmental control) or by those who see the Internet as a free environment without any regulatory

[24] World Summit on the Information Society (WSIS), Tunis Agenda for the Information Society, document WSIS-05/TUNIS/DOC/6(Rev.1)-E, Tunis, 18/11/2005 (WSIS 2005), p. 4.

[25] World Summit on the Information Society (WSIS), Declaration of Principles, document WSIS-03/GENEVA/DOC/4-E (12 December 2003). Geneva, 12/12/2003 (WSIS 2003), par. 20.

framework or relevant level of responsibility. An "all stakeholders approach" offers a better basis for finding compromises and a forward-looking approach to problems.

This underlying principle is also reflected in the paragraphs of the Geneva Declaration of Principles as far as the management of the Internet is concerned. The management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations (paragraph 48). It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism. The subsequent two paragraphs of the Declaration provide more details about the role of the various stakeholders and promote a co-ordinated approach to Internet Governance issues.

The Tunis Agenda for the Information Society, while reconfirming the Geneva Principles, further narrows down what is at stake when it comes to assigning domain names.[26] Paragraph 63 introduces the autonomy of countries concerning their own ccTLD:

> Countries should not be involved in decisions regarding another country's country code top-level domain (ccTLDs). Their legitimate interests, as expressed and defined by each country, in diverse ways, regarding decisions affecting their ccTLDs, need to be respected, upheld and addressed via a flexible and improved framework and mechanisms.

The subsequent paragraph addresses international domain name assignment: "We recognize the need for further development of, and strengthened cooperation among, stakeholders for public policies for generic

[26] WSIS 2005.

top-level domains (gTLDs, such as .com, .org, .net).” Both paragraphs seem to be inspired by the report of the WGIG.[27] This report points out in a more detailed way what the institutional governance issues are and includes alternative models for the restructuring of the present Internet Corporation for Assigned Names and Numbers (ICANN) model.

ICANN and the GAC

ICANN constitutes the epicentre of the institutional governance debate. It is the organization (to summarize it briefly without the intention of being complete) that, based on authority given to it by the US Commerce Department, a) controls the assignment of gTLDs, b) more or less authorizes the organizations responsible for the ccTLDs, and c) manages the necessary addressing system (the “DNS”, the Domain Name System with its root servers). In theory, ICANN acts as an independent organization, but it is the general assumption that there is a strong interdependence between ICANN and the US Government – not only because of some formal powers but also because various other factors are considered to be relevant, such as the fact that ICANN is based in the USA (as is the case with most of the root servers) and therefore is subject to US law. Recently, ICANN entered into a new agreement with the US Government that should result in more autonomy for ICANN by 2009.[28] Nevertheless, ICANN’s role remains highly debated.[29]

One of the instruments within the present structure to counterbalance these issues is the existence of the Governmental Advisory Committee (GAC), which represents countries that are interested in Internet Governance.[30] The GAC has adopted principles and guidelines for the delegation

[27] Working Group on Internet Governance (WGIG), *Report of the Working Group on Internet Governance*, Château de Bossey, June 2005 (WGIG 2005).

[28] Joint project agreement between the US Department of Commerce and ICANN, 29 September 2006.

[29] E.g. <http://www.icannwatch.org/>.

[30] More information on the GAC can be found at <http://gac.icann.org>.

and administration of ccTLDs.[31] The principles underline the national responsibilities for ccTLDs. Actually, according to the document

> … the main principle is the principle of subsidiarity. ccTLD policy should be set locally … Most of the ccTLD policy issues are local in nature and should therefore be addressed by the local Internet community according to national law.

Article 4.1 goes even further by claiming that ultimate public policy authority over the relevant ccTLD rests with the relevant government or public authority. And every country or distinct economy with a government or public authority should be able to ask for its appropriate country code to be represented as a ccTLD and to designate the registry. The GAC principles are not undisputed and, as such, are not a condition for the relationship between ICANN and the registries. It is interesting to notice that the new agreement between ICANN and the US Government contains a specific paragraph about the GAC: ICANN is to work with the GAC to review the role of the GAC within ICANN "so as to facilitate effective considerations of GAC advice on the public policy aspects of the technical coordination of the Internet". This seems to hint at a stronger involvement of the GAC and at a greater role for its principles on the delegation and administration of ccTLDs.

The European Dimension

The EU has constantly tried to increase its influence on ICANN and related governance issues.[32] It has sought to limit the control by the US Government over ICANN and has supported attempts to increase the role of national governments in ICANN's operations, for example through the GAC. In fact,

[31] Governmental Advisory Committee (GAC), GAC Principles and Guidelines for delegation & administration of ccTLDs <http://gac.icann.org> (GAC 2005). This is the current version of the principles; the original version was adopted in 2000.

[32] More information on the EU and Internet governance can be found at the website of the EU: <http://ec.europa.eu/information_society/policy/internet_gov/index_en.htm>.

the secretariat of the GAC has been run by the European Commission for quite some time. The GAC principles were influenced by the EU, and the EU strongly supported the various statements made during the WSIS conference on the ccTLDs.[33] Although its suggestions were not fully incorporated in the governance model of ICANN, the subsequent efforts of the Commission to influence ICANN's functioning through the GAC have been moving in the same direction.

National and European Assignment of Domain Names

In this section we look at the institutional design for the allocation of domain names at the national and European level. The various models are mentioned and a more in-depth analysis is made of the .eu model.

Institutional Aspects

The national institutional arrangements underlying the assignment of domain names are poised between the two extremes of private and public governance. In its pure version, private governance consists of self-regulation mechanisms, occurring "when those regulated design and enforce the rules themselves"[34], whereas its counterpart refers to the traditional "command and control" state-dominated governance. However, in the contemporary legal orders these two models of governance are not usually found in their genuine form. Accordingly, self-regulation is rarely detached from some kind of state participation and almost always amounts to what is

[33] Also see: European Commission, Communication from the Commission to the Council and the European Parliament, The Organisation and Management of the Internet International and European Policy Issues 1998 – 2000, COM(2000) 202 final, Brussels 11/4/2000 (EC 2000[3]); European Commission, International Policy Issues related to Internet Governance, 20/2/2001 (EC 2001); Volker Leib, "ICANN-EU can't: Internet Governance and Europe's role in the formation of the Internet Corporation of Assigned Names and Numbers (ICANN)", Telematics and Informatics 2002/19; and E. F. Halpin and S. Simpson, "Between Self-regulation and Intervention in the Networked Economy: the European Union and Internet Policy", *Journal of Information Science*, 28(4), 2002, pp. 285 et seq.

[34] Virginia Haufler, *A Public Role for the Private Sector. Industry Self-Regulation in a Global Economy* (Washington D.C.: Carnegie Endowment for International Peace, 2001) p. 8.

referred to as "co-regulation"[35] or "regulated self-regulation",[36] with different variations depending on the degree of public intervention. In addition, the traditional positive State is being increasingly replaced by the "regulatory State" characterized by privatization, liberalization and re-regulation, with the state intervening to address market failures in pursuance of the public interest. This in turn brings about different institutional structures, based on the delegation of the regulatory tasks to bodies that operate at arm's length from the government ("agencies").[37]

If one looks at the national registries, one can see that certain registries are acting on a very independent basis with hardly any regulatory framework. In other countries the registry is more or less a fully government controlled entity.

At the EU level, the shift towards the aforementioned regulatory-state architecture has induced several calls for the creation of Community-wide agencies charged with the implementation of European regulatory policies and functioning as the central nodes of transnational networks composed of the different levels of administration and stakeholders.[38] A variation of the regulatory State is the emergent "post-regulatory State" that relies to a significant extent on co-regulation mechanisms,[39] thereby approaching a mixed mode public-private governance. A categorization of the governance patterns of the different applications of the EU Internet policy according to the above distinctions is not straightforward. What can be safely said,

[35] See e.g. European Commission, Communication from the Commission-Action Plan "Simplifying and Improving the Regulatory Environment", COM (2002) 287 final, Brussels, 2002 (EC 2002).

[36] See Nicolinacos, "Nature and scope of Content Regulation for On-Line services", (2000) C.T.L.R. 6(5), pp. 126 et seq.

[37] See e.g. M. Moran, "Understanding the regulatory state", *British Journal of Political Science*, 2002/32, pp. 391 et seq.

[38] See e.g. G. Majone, "The credibility crisis of Community Regulation", *Journal of Common Market Studies*, 2002/38 (2), pp. 273 et seq.

[39] See Christou/Simpson, p. 48.

though, is that all the policies adopted at the EU level contain, at least to a certain extent, some private governance characteristics. This is partly a result of the decentralized and complex nature of the Internet and of the immense influence exerted by the strongly organized Internet community. More than that, in some parts of the EU Internet policy, recourse is made exclusively to private governance mechanisms, as it was the case, for instance, in the initial Safer Internet Action Plan, which incited the development and implementation of adequate systems of self-regulation in the fields of illegal and harmful Internet content.[40]

In the vast majority of cases, a mixture of the above defined models of governance is found within one and the same Internet policy field. This is the case, for example, with the e-commerce framework, where the encouragement of codes of conduct and alternative dispute resolution (ADR) procedures[41] coexists with legislative measures pursuing public policy objectives, such as the protection of consumers and of intellectual property rights (IPR) holders and the promotion of consumer confidence,[42] as well as economic policy objectives, namely the consolidation of the European "digital" internal market. Such legislative measures are enacted by the Community institutions and implemented by the national public administrations. The .eu governance model and its underlying institutional arrangements are a typical example of a mixed mode public-private governance model. It represents a public-private dispersed agentification model, with the public dimension shaped by the European Commission acting as an agent of the Member States. Seen from another angle, the .eu

[40] Decision No. 276/199/EC of the European Parliament and of the Council adopting a multi-annual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, OJ L 33/1 of 6.2.1999.

[41] Directive 2000/31 of the European Parliament and of the Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") OJ L 178/1 of 17.7200.

[42] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, OJ L 13/12 of 19.1.2000.

model has been held to combine elements of regulatory governance with a negotiated reading of self-regulation, partially resembling what was described above as a post-regulatory state model.[43]

National Assignment

Based on a relationship with ICANN, national registries are authorized to hand out domain names. The national registries use registrars as an intermediary between those who wish to use a domain name and the registration/activation of that domain name. In general, the role of registrar is exercised by Internet service providers (however, depending on the by-laws of the national registry, other parties may also have a similar role in the allocation process).

Most national registries "received" the right to manage the national domains in the early days of the Internet.[44] The authority, sometimes given to individuals, was then passed on to other organizations or to "natural" successors. Because of this organic process, the institutional design differs from country to country. This is the main reason why this contribution does not look into the various national structures for the allocation of domain names. Instead, the focus is on the recently developed .eu model, because it reflects in a much more structured way the various issues that are at stake.

The .eu Model

Towards the Adoption of the .eu TLD

The first steps towards the adoption of the .eu TLD were taken in 1997 when the Commission initiated consultations on this issue with users and representatives of the industry. In December 1999, the Commission undertook, as a part of the e-Europe initiative, to support the creation of a

[43] See G. Christou, and S. Simpson, "The Internet and Public-Private Governance in the European Union", *Journal of Public Policy* (2006), 26, pp. 43 et seq.

[44] There is still no full transparency about what type of right registries have with respect to their national domain name and on what legal basis control was given to them.

.eu TLD, with a view to encouraging cross-border e-commerce within the EU and to assisting those companies that wish to establish an EU-wide Internet presence.[45]

In February 2000, the Commission issued a Working Paper concerning the creation of a .eu TLD as a means of strengthening the image and infrastructure of the Internet in Europe for the purposes of European institutions and private users, and for commercial purposes including e-commerce.[46] In a statement that partly reflects the .eu governance structure, the Commission held that

> … in view of the highly decentralized structure of the Internet and the private statute of nearly all the organizations concerned (including ICANN itself) the European Institutions are only called upon to decide to fulfil the minimal responsibility of requesting the domain from ICANN and acting as the relevant public authority with ultimate oversight should the need arise.

Thereupon, the Commission considered several options regarding the bodies to which the operation of the .eu TLD could be delegated, the criteria and the entity responsible for the development and implementation of the registration policy, and the possibilities for trademarks and dispute policies. The replies submitted in the course of the subsequent consultation overwhelmingly supported the creation of .eu. Almost all respondents preferred the option of the .eu TLD being run by some form of non-profit organization in the private sector working in the public interest. As for alternative dispute resolution

[45] European Commission, Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon 23 and 24 March 2000 – e Europe – an information society for all, COM (1999) 687 final. (EC 1999).

[46] European Commission, Commission Working Paper of 2.2.2000, The creation of the .EU Internet Top Level Domain Name, Brussels, 2/2/2000 (EC 2000).

procedures, the responses were divided between the uniform alternative dispute resolution initiated by ICANN and that of a European forum. Lastly, there were many variations in the views on the different policy issues.

In July 2000, the Commission presented a Communication on how the creation of the .eu TLD was progressing, whereby it set out the principal results of the public consultation and its conclusions and drew the next steps to be taken.[47] The Communication made apparent the Commission's determination to promote a mixed governance in the regime to be applied to the .eu domain. On the one hand, the Commission endorsed the solution supported by the majority of the respondents, namely that the registry should be a not-for-profit private entity independent of the EU policy structure and that it should be assigned the .eu code for a limited period by means of a renewable contract. On the other hand, the Commission favoured the option of the EU assuming a role equivalent to the one assumed by national governments regarding ccTLDs as mentioned in the GAC Operating Principles (see par 2.2). By the same token, the EU would participate, through the Commission, in the overall policy formation process of the .eu domain, as a guarantee that the operation of the registry would be consistent with EU law and policy in the areas of, *inter alia*, competition law, intellectual property and data protection. The subsequent deliberations were mainly carried out under the auspices of the Interim Steering Group (ISG) set up within the European Community Panel of Participants (EC-POP) to report on options for the .eu registry. The general view was that the launch of .eu would have territorial and institutional implications for the EU that would necessitate a policy role of both the Commission and the Internet Community.[48]

[47] European Commission, Communication from the Commission to the European Parliament and the Council, Internet Domain Name System-Creating the .EU Top Level Domain, COM (2000) 421 final, Brussels, 5/7/2000 (EC 2000[2])

[48] Christou/Simpson 2006, p. 52.

At the international level, the proposal for .eu was negatively received by ICANN. The formal ground for this was that the EU is a regional entity. The Commission, however, managed to overcome the initial objections by focusing on arguments that could hardly be overlooked by ICANN. For instance, the Commission underlined the limited alternatives available for registration in the World Wide Web in the existing TLDs and the possible exhaustion of existing name space in the near future. Furthermore, a determinative factor was the general support that the Commission managed to recruit in favour of an EU domain name. This support was difficult to ignore, as the mission of ICANN is to act in the best interest of the Internet community. In 2000, the Commission formally requested ICANN to delegate the .eu. Due to the complex negotiations between the European Union and ICANN, but also because a registry had to be selected, it took about five years before .eu was put in the root as a ccTLD.

The Creation of the .eu TLD

In April 2002, the European Parliament and the Council of the EU adopted Regulation 733/2002, establishing the conditions of implementation of .eu TLD and providing for the designation of a registry as well as the general policy framework within which the latter would function.[49] The regulation stated that to the extent possible and without prejudice to Community law, the principles of non-interference, self-management and self-regulation should apply to the .eu ccTLD. Article 3.1 of the regulation states that the registry should be a non-profit organization designated by the European Commission on the basis of an open, transparent and non-discriminatory procedure. The delegation of the .eu code should take effect by virtue of a contract stipulating the conditions according to which the Commission supervises the organization, administration and management of the .eu

[49] Regulation (EC) 733/1002 of the European Parliament and of the Council of 22 April 2002, on the implementation of the .eu TLD, OJ L 113/1 of 30/4/2002.

TLD by the registry. A draft service concession contract was annexed to the Regulation.

According to the Regulation and the draft contract, the registry is charged with the organization, administration and management of the .eu TLD in the general interest and on the basis of principles of quality efficiency, reliability and accessibility. Its main tasks comprise the registration of domain names through registration agents, setting up extra-judicial procedures for the resolution of disputes related to .eu, and maintaining and ensuring the integrity of the databases of domain names. Moreover, the registry had to establish procedures for and carry out accreditation of .eu registrars and adopt its initial registration policy. Lastly, the registry, having obtained the prior consent of the Commission, should enter into the appropriate contract providing for the delegation of the .eu TLD code in accordance with the principles of the GAC.

The set of rules relating to the designation of the registry illustrate the private governance features of the .eu regime. Such features are reflected primarily in the fact that the management of the .eu TLD is contracted out to a private sector body. The same holds for the registrars that are to supply the domain name registration services. In addition, provision is made for setting up an alternative dispute resolution mechanism. Overall, a private transnational network is created by the regulation. The registry is the central node of this network (the registrars and alternative dispute resolution providers are its constitutive parts) and has the remit to organize, administer and manage the .eu TLD.[50] Moreover, private parties are afforded a significant role in the shaping and implementation of the .eu registration policy. In the first place, according to regulation 733/2002, interested parties (here, the term embraces undertakings, organizations and natural

[50] See Halpin/Simpson 2006.

persons) are to be consulted by the registry concerning the adoption of its registration policy. In the second place, the articles of association of the registry eventually appointed by the Commission (the European Registry for Internet Domains; EURID)[51] illustrate the great influence that interested parties can exert on its operation.[52] Those rules allow for any legal entity or natural person serving the interests of participants in the Internet or with an interest therein, to become a member of the association. The relevance of this provision is highlighted by the fact that each associated member has the right to nominate one director of EURID. Furthermore, the representatives of the various interest groups that together form the local European Internet community, set up the EURID Policy Council, which must be consulted on any decision that relates to the registration policy of the association.

Notwithstanding the pivotal role of the private actors, the Commission's role and, consequently, the public dimension of the .eu scheme is far from negligible. The Commission designates the registry and has the power to terminate, re-designate or abstain from renewing its contract with it. The registry is under the obligation to submit periodic reports to the Commission. In addition, the public dimension of the .eu governance becomes more apparent in the provisions on the public policy rules (PPRs). According to article 5 of Regulation 733/2002, after consulting the registry, the Commission shall adopt public policy rules concerning the implementation and functions of the .eu TLD and the public policy principles on registration. Such rules shall refer to the dispute resolution policy, the policy on speculative and abusive registration, and the policy on the possible revocation of domain names, issues of language and geographical concepts, the treatment of IP, and other rights. The public policy rules are to be implemented in the .eu registration policy adopted by the registry

[51] Commission Decision of 21 May 2003 on the designation of the .eu TLD registry, OJ L 128/29 of 24/5/2003. The service concession contract between EURID and the Commission was signed in October 2004.

[52] See European Registry for Internet Domains (EURID), Articles of Association <www.eurid.eu> (EURID 2006).

in consultation with the Commission. The failure to implement the public policy rules in the initial registration policy or the failure to manage, operate and control the .eu in accordance with those rules is stipulated as a valid reason for the Commission to terminate its contract with the registry. Lastly, another restriction of private governance relates to the codes of conduct. The Regulation stipulates that the implementation of the .eu TLD may take into consideration best practices in this regard and could be supported by voluntary guidelines or codes of conduct where appropriate. In accordance with the service contract between the Commission and EURID, a code of conduct is to be designed by EURID and proposed to the interested parties for consultation. However, the Commission has to be duly consulted on those matters for which it has competences and must ensure that the codes comply with public policy rules.[53]

All in all, a public-private partnership model of governance is established, whereby the registry (a private operator that is separate from but legally answerable to the Commission) adopts its registration policy in consultation with the stakeholders and the Commission, and in accordance with the public policy rules set out by the latter. In implementing the .eu TLD, the registry is called upon to play a role as the central node of a transnational network of other private operators, with the Internet community being in a position to substantially influence its policies. Such private governance mechanisms as self-regulation and alternative dispute resolution are designed to form part of this architecture, although under parameters drawn from public policy considerations and established by the Commission.

The Public Policy Rules

The rules that lay down the public policy parameters concerning the implementation and functions of the .eu TLD and the principles governing

[53] See Halpin/Simpson 2002, p. 56.

registration were introduced by Regulation 874/2004 of the Commission.[54] In general, the provisions of this Regulation further exhibit features of public-private partnership for the governance of the .eu TLD. On the one hand, those features are reflected in the institutional arrangements set out by the regulation; on the other hand, the substantive or procedural rules applying to the .eu TLD as such are an illustration of private or public governance elements. This is because, bearing in mind that they were set out by the Commission, the more or less intrusive nature of these rules is indicative of the degree of public interference in the shaping of the .eu policy. The following are the main issues of the Regulation.

1. The Regulation refers to Regulation 733/2002 to define the eligible parties that may request domain names under .eu and establishes the principle of "first come, first serve" to govern the procedure (article 2). The data to be submitted upon the request for a domain name registration are also provided for, which is a clear example of substantial involvement of the Commission to the registry's and registrars' operations (article 3).

2. The Regulation lays down the general principles for the procedure for the accreditation of registrars by the registry, which should take effect through a contract entailing the obligation of the registrars to observe the terms of accreditation and to comply with the public policy rules (articles 4 and 5). Such procedure shall be determined by the registry, it shall be reasonable, transparent and non-discriminatory, and shall ensure effective and fair conditions of competition. In that connection, the registry's responsibility to select and accredit the registrars according to the procedure and terms set out by it, readily implies

[54] Commission Regulation (EC) No 874/2004 of 28 April 2004, laying down public policy rules concerning the implementation and functions of the .eu TLD and the principles governing registration, OJ L 162/40 of 30/4/2004.

a certain degree of private governance, whereas the registrar's obligation to observe the public policy rules indicates the opposite. In addition, some specific procedural rules are set out stipulating the registrars' obligation to forward requests in the chronological order in which they received them, and to require applicants to submit accurate and reliable contact details of the person responsible for the technical operation of the domain name that is being applied for. Lastly, a private governance element is inserted by the provision empowering registrars to develop label, authentication and trust mark schemes to promote consumer confidence in the reliability of information that is available under a domain name, in accordance with applicable national and Community law.

3. The Regulation imposes on the registry the obligation to ensure the availability of the registration procedures in all Community languages (article 6). This obligation, which is an implication of sound political considerations of the Commission, entails a considerable administrative burden for the registry. Language-related considerations are also taken into account with regard to other issues (see the following points).

4. The public policy rules provides for a "sunrise period", during which the owners of intellectual property rights and related rights recognized or established by Community/national law and public bodies can pre-register a domain name (articles 10–14). Detailed rules are laid down regarding the names to be registered (e.g. concerning the characters to be included in such names), the duration and the carrying out of the procedure (e.g. blocking of the names concerned until the validation), which certainly diminish the possibilities of the registry to shape the registration policy. The prioritization of public bodies as well as the concern to safeguard the rights of IP and related rights holders are an indication of the public policy parameters

present in the governance of .eu. On the institutional ground, the phased registration procedure also contains mixed governance elements. On the one hand, the validation agents are considerable actors in the sunrise period, as they are responsible for validating the documentary evidence of prior rights claimed by applicants or rights to a name claimed by public bodies. Such validation agents are private entities designated by the registry. However, the validators should be bound by their contract to follow objective, transparent and non-discriminatory procedures. In addition, rules are set out concerning the form and time limits for the submission of information to the validation agents and the validation procedure (e.g. order of examination of the requests). On the other hand, the considerable involvement of the Commission is exemplified by the provision that an auditor shall be appointed by the registry in consultation of the Commission, with the purpose of confirming the fair, appropriate and sound operational and technical administration of the phased registration period by the registry.

5. Regulation 733/2002 already provided for the right of Member States to reserve country names and to limit the registration of geographical and geopolitical names only under second-level domain names (i.e. info@amsterdam.netherlands.eu). According to article 8 of Regulation 874/2004 (as amended by Regulation 1654/2005), a list of names set out in an annex to the Regulation shall be reserved or registered only as second-level domain names directly under the .eu TLD by the countries indicated in the list. In addition, geographical and geopolitical names that can be registered only under a second-level domain name have to be notified to the Commission, which is to carry out the relevant objection resolution procedure and further notify the names to the registry.

6. Provision is made in the Regulation for the creation of a WHOIS database to provide information about the technical and administrative contact administering the domain names under .eu (article 16). At the same time, specific rules are laid down that aim at ensuring the protection of the privacy of the holders of domain names, thereby inserting another public policy consideration into the .eu framework (article 5).

7. A denoting element of public policy parameters is found in article 18 of Regulation 874/2004, which provides that where a domain name is considered by a court of a Member State to be defamatory, racist or contrary to public policy, it shall be blocked by the registry upon notification of a court decision and shall be revoked upon notification of a final court decision. Such names shall be blocked from future registration.

8. The rules contain specific provisions on the revocation of domain names (articles 18–21). Besides traditional reasons for revocation (e.g. non-payment of the registration fee), particular attention is given to speculative and abusive registrations. Such registrations can be at stake in the case of issues related to property rights as well as when a domain name has been registered or is being used in bad faith. For example, the rules forbid the acquisition of domain names for the purpose of selling or renting, or in order to behave in an anti-competitive or abusive manner.

9. As mentioned above, the registry is responsible for implementing an extra-judicial settlement of conflicts policy that takes into consideration the recommendations of the World Intellectual Property Organization (WIPO). The regime for dispute resolution can be found in articles 22–23 of the policy rules). The registry is to select the alternative dispute resolution (ADR) providers (EURID has appointed

> the Prague-based arbitration court for this purpose). Although the availability of an ADR procedure amounts to a great degree of private governance, the power of the registry to shape an ADR policy has been considerably circumscribed by the provisions of the public policy rules. For example, the rules refer in detail to the cases in which an ADR procedure may be initiated by a party, namely when a registration is speculative or abusive, or when a decision taken by the registry conflicts with the policy rules. In addition, specific rules are stipulated to govern the procedure concerning, for instance, the language, means of communication with the parties, time limits for the different stages of the procedure, the majority required for an ADR decision, the number of members of the ADR panels, etc.

Thus, as the above review shows, the public policy rules introduce many private governance features. Apart from the registry and the registrars, other private actors were introduced in the .eu institutional network, namely the validation agents and, more importantly, the ADR providers. On the other hand, the provision for the adoption of public policy rules by the Commission and the latter's power to oversee their implementation already inserts a public dimension into the .eu governance.

Conclusion

The assignment of domain names represents an important aspect of Internet Governance. Assignment is part of the global discussion about Internet Governance and is strongly linked to the role of ICANN. Awareness of the importance of the institutional aspects of domain names is clearly increasing. Here, at least two trends can be identified, namely the growing focus on national involvement and, subsequently, the growing emphasis on national regulatory embedment. As far as the latter is concerned, the creation and structuring of the .eu TLD is used as an example in this article. The .eu regime deals with a broad range of topics in order to safeguard the fair allocation of domain names, data privacy, intellectual property and related rights, geographical names, etc. For this purpose, it is not possible to rely exclusively on the discretion of such a highly specialized entity as the registry, as it would likely prove to be ill-suited to take into full consideration and to weigh up the different interests affected by its policies. Therefore, the private entities entrusted with the task of implementing the .eu TLD needed to become bound to take into account those parameters in the exercise of their self-regulatory functions under the oversight of the European Commission. An indication of the impact of the chosen institutional design is the detail in which such rules are drawn. The public policy rules that have been adopted considerably influence the exercise of the self-regulatory remit of the private actors involved in the .eu scheme. This remit is further affected by the influential institutional position of the Commission in the .eu regime. Instead of the detailed level of regulation in the public policy rules, it might have been sufficient enough to indicate the relevant topics in a more general way and to leave it up to the registry to deal with the further implementation (i.e. in by-laws that then could be subject to approval by the European Commission). Such a process would also allow for more flexibility. Changing the public policy rules now requires an amended Commission Regulation which takes quite some time. Topics like the revocation of domain names, speculative/abusive registrations and a dispute resolution procedure might need quick adaptation in order to remain in line with the needs of the parties involved. Nevertheless, the .eu structure offers a broad scope of relevant aspects that are worth taking into account when addressing the issue of regulating the assignment of domain names.

II. Experiences from the OSCE Region

Governance of Hate Speech on the Internet in Europe*

Yaman Akdeniz

Speech that incites or promotes hatred towards individuals, on the basis of their race, gender, religion, sexual preference, and other forms of individual discrimination continues to be widely available on the Internet as in other kinds of traditional media. There is strong documented evidence to show that racist organizations and individuals are using the Internet to disseminate racist content. It was estimated by the Simon Wiesenthal Center in 2005 that there were more than 5,000 websites in a variety of languages which promote racial hatred and violence, anti-Semitism and xenophobia around the world.[55] Their study entitled *Digital Terrorism & Hate 2005* reported a 25 per cent increase in such websites compared to 2004 which indicated that the problem of racism and xenophobia was growing over the Internet. The estimated number of websites which promote racial hatred and violence reached over 6,000 in May 2006 according to the updated version of the *Digital Terrorism & Hate 2006* report.[56]

Leaving apart the statistics, which may be over- or underestimated, the problem of hate speech and racist content on the Internet is evident. These kinds of websites are largely used for propaganda, disseminating hatred,[57]

[*] This chapter is adapted from Y. Akdeniz, "Governing Racist Content on the Internet: National and International Responses", (2007) *University of New Brunswick Law Journal*, forthcoming.

[55] *Canada NewsWire*, "Digital Terrorism & Hate 2005 Report Shows 25 Per Cent Increase In Hate Sites", 7 October 2005.

[56] The Simon Wiesenthal Center, *Digital Terrorism & Hate 2006*, available through <http://www.wiesenthal.com/>.

[57] Note the study conducted by J. Glaser, J. Dixit, D.P. Green, "Studying Hate Crime with the Internet: What Makes Racists Advocate Racial Violence?" (2002) *Journal of Social Issues* 58(1) spring, pp. 177–193.

recruitment,[58] training,[59] fundraising,[60] and for communications[61] by racist as well as terrorist organizations. There are also several controversial publications of a racist nature, or publications which encourage violence disseminated through a number of websites. Obviously there is major concern about the availability of such content on the Internet and many governments and international organizations including the United Nations, OSCE, Council of Europe, and the European Union are in harmony that racism and manifestations of racism through the Internet should not and will not be tolerated. However, the major question that is being faced by international organizations and state level regulators is how to regulate the flow of such information over the Internet.

The question becomes even more complicated considering the fact that there exists different political, moral, cultural, historical and constitutional values between different States. This undoubtedly complicates efforts to find an "appropriate balance between the rights to freedom of opinion and expression and to receive and impart information and the prohibition on speech and/or activities promoting racist views and inciting violence."[62] That balance is yet to be reached and agreed at an international stage. It has become evident during the policy discussions of the last ten years or so that especially the United States of America oppose any regulatory effort to combat racist publications on the Internet on freedom of expression

[58] H. Hylton, "How Hizballah Hijacks the Internet", *Time Magazine*, 8 August 2006, at <http://www.time.com/time/world/article/0,8599,1224273,00.html>.

[59] Publications such as *Mujahideen Explosive Handbook* and the *Encyclopaedia of the Afghan Jihad* are some of the publications disseminated and distributed through the Internet. Note "Terror law vague, accused to argue", *The Globe and Mail (Canada),* 30 August 2006 and "Abu Hamza trial: Islamic cleric had terror handbook, court told", *The Guardian*, London, 12 January 2006.

[60] Note the Communication from the European Commission to the European Parliament and the Council concerning Terrorist recruitment: addressing the factors contributing to violent radicalisation, Brussels, 21.9.2005, COM(2005) 313 final.

[61] See "Foiled plots", *The Globe and Mail (Canada),* 11 August 2006.

[62] Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session (Chairperson-Rapporteur: Juan Martabit (Chile)), E/CN.4/2006/18, 20 March 2006, at <http://daccessdds.un.org/doc/UNDOC/GEN/G06/119/23/PDF/G0611923.pdf>, para. 8.

grounds based upon the values attached to the First Amendment of the US Constitution. At the same time there are other organizations or States which regard harmonized national legislation and international agreements as the way forward. For example, the European Commission against Racism and Intolerance (ECRI) believes, "national legislation against racism and racial discrimination is necessary to combat these phenomena effectively".[63] In fact this view supported by many Member States of the Council of Europe led into the development of an Additional Protocol to the Cyber-Crime Convention concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. However, while the US Government wholeheartedly supported the development of a Cyber-Crime Convention within the Council of Europe region and recently ratified the Convention as an external supporter, it decided not to support or get involved with the development of the Additional Protocol to the Cyber-Crime Convention. Hence, fundamental disagreements remain on the most appropriate and effective strategy "for preventing dissemination of racist messages on the Internet, including the need to adopt regulatory measures to that end".[64]

Despite these fundamental differences and difficulties encountered in terms of harmonization of laws, the growing problem of racist content on the Internet has naturally prompted vigorous responses from a variety of agents, including governments, supranational and international organizations as well as from the private sector. A detailed overview of these initiatives and regulations will be provided in this chapter.

[63] Note within this context the ECRI General Policy Recommendation No 7 on national legislation to combat racism and racial discrimination, CRI (2003) 8, adopted on 13 December 2002, at <http://www.coe.int/T/E/human_rights/Ecri/1-ECRI/3-General_themes/1-Policy_Recommendations/Recommendation_N%B07/3-Recommendation_7.asp>, para. 1 of the Explanatory Report.

[64] The meeting on the relationship between racist, xenophobic and anti-Semitic propaganda on the Internet and hate crimes held by the OSCE in Paris on 16–17 June 2004.

Effectiveness of State Laws

The effectiveness and application of state laws have been problematic in terms of encountering hate speech and racist content on the Internet. A number of court cases have targeted the creators of racist content as well as those hosting such content, or providing access to such content in a number of jurisdictions including in Australia, Canada, France, Germany, and other States in the OSCE region. Court cases involving the prosecution of individuals who disseminate and publish racist content reflect the complex nature of the Internet as well as the limitations of the application of existing laws to the Internet. Internet and new communications technologies challenge the notion of nation-state as the Internet does not respect territories, and has no boundaries to the effect that no single nation-state can effectively dominate or control the Internet by means of unilateral state regulation.[65] It should be noted that the "Zündel case" which involved Ernst Zündel's website which denies the existence of the Holocaust took nearly five years to be finalized in Canada.[66] Zündel has been charged in Germany in relation to his website after he was extradited from Canada and was sentenced to a five-year prison term in February 2007.[67] Despite a Canadian order to stop disseminating such views through his website, and despite the court ruling in Germany Zündel's website is still up and running from Texas, USA, and regularly updated with his "letters from prison". The Toben case[68] involving Holocaust denial was a similarly drawn out affair in Australia and Toben's carefully drafted website is still active and regularly updated. At the

[65] See for example J. Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence", *European Journal of International Law* 11 (2000), 135–148.

[66] *Sabina Citron Toronto Mayor's Committee on Community and Race Relations and Canadian Human Rights Commission v. Ernst Zündel*, Canadian Human Rights Tribunal, T.D. ½ 2002/01/18, at <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=252&lg=_e&isruling=0>.

[67] Associated Press, "5-year prison term urged for Holocaust denier", 26 January 2007.

[68] *Jones v. Toben*, Federal Court of Australia, [2002] FCA 1150. The decision can be accessed at <http://www.austlii.edu.au/au/cases/cth/federal_ct/2002/1150.html>; *Toben v. Jones* [2003] FCAFC 137 (27 June 2003). Toben was also prosecuted and imprisoned in Germany in relation to his website. In relation to the Toben's Germany prosecution see S. Gold, "German Landmark Nazi Ruling", Newsbytes, 12 December 2000. See further Agence France Presse, "Australian historian arrested in Germany for disputing Holocaust", 9 April 1999. For the German decision see Bundesgerichtshof, Urteil vom 12. December 2000 -- 1 StR 184/00.

same time the various cases related to the Yahoo! case[69] both in France and the US were initiated over five years ago and only came to a conclusion in May 2006.

The legal system which is more adapted to deal with one-off traditional publications (such as newspapers and magazines) has been extremely slow in dealing with Web-based publications. While the circulation of one-off publications such as books and magazines can be controlled by confiscation orders or by general bans which prohibit the delivery or entry in a particular State of such publications, the same results cannot be achieved with Web-based publications. Basically websites cannot be torched or confiscated or taken down, especially if the servers that contain them are based in another jurisdiction. Therefore, the above-mentioned cases illustrate that the emergence of Internet governance entails a more diverse and fragmented regulatory network with no presumption that these will be anchored primarily in nation-states. A shift from unilateral state regulation into various forms and models of governance will almost inevitably be witnessed in which alternatives to state regulation such as self-regulation, co-regulation, or a mixture of these are considered by States and international organizations. These alternative and additional forms of regulation will be addressed later in this chapter.

Harmonization Efforts

Harmonization efforts to combat illegal content, even for universally condemned content such as child pornography, have been protracted and are ongoing.[70] Efforts to harmonize laws to combat racist content on the

[69] *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v. Yahoo! Inc. (USA), Yahoo France*, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November 2000. Note also *Yahoo!, Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme*, Case Number C-00-21275 JF [Docket No. 17], United States District Court for the Northern District of California, San Jose Division, 169 F. Supp. 2d 1181; 2001 U.S. Dist. LEXIS 18378, 7 November 2001, Decided.

[70] Rights of the Child: Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the sale of children, child prostitution and child pornography, E/CN.4/2005/78, 23 December 2004. Note also the Addendum to this report: E/CN.4/2005/78/Add.3, 8 March 2005. Note further Y. Akdeniz, *Internet Child Pornography and the Law: National and International Responses*, Ashgate, forthcoming in 2007.

Internet have proved to be even more problematic. While child pornography is often regarded as a clear cut example of “illegal content”, racist content has been much more difficult to categorize due to constitutional, political, moral, and historical differences between States. While some forms of racist content or hate speech are regarded as illegal content in certain States, the same content may not be regarded as illegal in other States. The different approaches adopted to Holocaust denial within different OSCE States is a good example of evident contrasting policies in this field. Similarly, there exist specific laws in certain European countries such as France and Germany in which the simple act of displaying Nazi objects or memorabilia, including exhibition of uniforms, insignia or emblems resembling those worn or displayed by the Nazis, is prohibited by criminal provisions. At the same time, in other European States such as the United Kingdom, it is perfectly legal to deny the existence of the Holocaust or display or wear Nazi objects without facing prosecution.

Both the Council of Europe (CoE) and the European Union attempted to address these differences and the harmonization efforts within the European region starting with the CoE’s Additional Protocol to the 2001 Cyber-Crime Convention *concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*.[71] Currently, the CoE Additional Protocol is the only attempt at regional harmonization to encounter the dissemination and availability of racist content on the Internet.

[71] See CETS No: 189 at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=8/9/2006&CL=ENG>. Note also Y. Akdeniz, *An Advocacy Handbook for the Non Governmental Organisations: The Council of Europe’s Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems*, Cyber-Rights & Cyber-Liberties, December 2003 (revised and updated in February 2007), at <http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf>.

Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems

In 1997, a Council of Europe Recommendation on Hate Speech called upon Member States "to take appropriate steps to combat hate speech by ensuring that such steps form part of a comprehensive approach to the phenomenon which also targets its social, economic, political, cultural, and other root causes".[72] Parallel to this political call, the Committee drafting the Cyber-Crime Convention discussed the possibility of including content-related offences other than child pornography within the Convention such as the distribution of racist propaganda through computer systems. As there was no consensus on the inclusion of provisions involving the criminalization of acts of a racist and xenophobic nature committed through computer systems, these were left out of the Cyber-Crime Convention 2001. While European States such as France and Germany strongly supported inclusion, the United States of America, which has been influential in the development of the main Cyber-Crime Convention, opposed the inclusion of speech related provisions apart from child pornography.

Noting the complexity of the issue, the Committee drafting the Cyber-Crime Convention decided that the Committee would refer to the European Committee on Crime Problems the issue of drafting an additional protocol to the Convention.[73] The Parliamentary Assembly, in its Opinion 226(2001) concerning the Convention, recommended the immediate development of an additional protocol to the Convention under the title "Broadening the scope of the convention to include new forms of offence", with the purpose of defining and criminalizing, *inter alia*, the dissemination of racist

[72] Recommendation on Hate Speech, No. R (97)20, adopted by the Committee of Ministers of the CoE on 30 October 1997.

[73] Explanatory Report of the Additional Protocol to the Convention on Cyber-Crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, as adopted by the Committee of Ministers on 7 November 2002, at <http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>, para. 4.

propaganda.[74] In its Recommendation 1543 (2001)[75] on Racism and Xenophobia in Cyberspace the Parliamentary Assembly considered racism "not as an opinion but as a crime". The Parliamentary Assembly noted that such a protocol will "have no effect unless every state hosting racist sites or messages is a party to it."[76]

The Additional Protocol *concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* aims to harmonize substantive criminal law in the fight against racism and xenophobia on the Internet and to improve international co-operation in this area. The CoE believes that a harmonized approach in domestic laws may prevent misuse of computer systems for a racist purpose. The Explanatory Memorandum to the Additional Protocol states that "this kind of harmonisation alleviates the fight against such crimes on the national and on the international level",[77] and that "corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by Parties whose laws in this area are less well defined."[78] The Additional Protocol entails an extension of the Cyber-Crime Convention's scope, "including its substantive, procedural and international co-operation provisions, so as to cover also offences of racist and xenophobic propaganda".[79] Thus, apart from harmonizing the substantive law elements of such behaviour, the Protocol aims at "improving the ability of the Parties to make use of the procedural provisions of the Cyber-Crime Convention including international co-operation and mutual legal assistance".[80]

[74] Ibid., para. 5.
[75] Text adopted by the Standing Committee, acting on behalf of the Assembly, on 8 November 2001.
[76] Para. 4 of the Recommendation 1543 (2001).
[77] Ibid., para. 3.
[78] Ibid.
[79] Ibid., para. 7.
[80] Ibid.

The definition of "racist and xenophobic material" contained in article 2 of the Additional Protocol refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors in such a format that it can be stored, processed and transmitted by means of a computer system.[81]

Measures to be taken at national level are explained in chapter II of the Additional Protocol. Article 3 entitled "dissemination of racist and xenophobic material through computer systems" requires parties to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the distribution, or otherwise making available, of racist and xenophobic material to the public through a computer system. Such conduct needs to be committed intentionally and without right.[82] The "intention" requirement would limit the liability of Internet Service Providers as long as they act as a conduit. But this would not for example exclude "notice based liability" as introduced by the EU Directive on Electronic Commerce which will be discussed below.

Article 4 requires parties to criminalize racist and xenophobic motivated threats through computer systems and as in article 3 such conduct needs to be committed intentionally and without right. Article 5 requires parties to criminalize racist and xenophobic motivated insults made in public through

[81] Para. 12 of the Expl. Rep.

[82] But note that article 3(2) states that parties may reserve the right not to attach criminal liability to such conduct, where the material, as defined in article 2, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. Article 3(2) also states that notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.

computer systems.[83] Article 6 requires the criminalization of expressions which deny, grossly minimize, approve or justify acts constituting genocide or crimes against humanity, as defined by international law and recognized as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945.[84] This is supported by the European Court of Human Rights which made it clear in its judgment in *Lehideux and Isorni*[85] that the denial or revision of "clearly established historical facts – such as the Holocaust (whose negation or revision) would be removed from the protection of Article 10 by Article 17" of the European Convention on Human Rights. The Court stated that "there is no doubt that, like any other remark directed against the Convention's underlying values,[86] the justification of a pro-Nazi policy could not be allowed to enjoy the protection afforded by Article 10".[87]

The Additional Protocol was opened for signature in Strasbourg on 28 January 2003. Since then 31 Member States have signed the Additional Protocol (including the external supporters Canada, and Montenegro).

[83] Parties to the Additional Protocol however may under subsection 2 either (a) require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or (b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

[84] A party under article 6(2) may either (a) require that the denial or the gross minimization referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise, or (b) reserve the right not to apply, in whole or in part, paragraph 1 of this article.

[85] Judgment of 23 September 1998.

[86] See, *mutatis mutandis*, the *Jersild v. Denmark* judgment of 23 September 1994, Series A no. 298, p. 25, § 35.

[87] Note also that the United Nations Resolution rejected any denial of the Holocaust as an historical event, either in full or part in October 2005. See UN General Assembly Resolution on Holocaust Remembrance, A/60/L.12, 26 October 2005, at <http://www.hmd.org.uk/assets/docs/pdfs/misc/un_resolution.pdf>. Additionally, on 26 January 2007, the UN General Assembly adopted a resolution No: A/RES/61/255 (GA/10569) condemning any denial of the Holocaust (<http://www.un.org/News/Press/docs/2007/ga10569.doc.htm>).

Out of the 31 signing States, only ten CoE Member States (Albania, Armenia, Bosnia and Herzegovina, Cyprus, Denmark, France, Lithuania, Slovenia, Ukraine, and the former Yugoslav Republic of Macedonia) have ratified the Additional Protocol as of February 2007. The Protocol entered into force following the initial five ratifications on 1 March 2006.

Other Regional and International Harmonization Efforts

It is also worth mentioning that there have been other attempts at harmonization at both the European Union and United Nations levels to combat the publication and dissemination of racist content. These broader, and not medium specific initiatives include the International Convention on the Elimination of all Forms of Racial Discrimination (ICERD) at the United Nations level, and a European Commission proposed draft Framework Decision on combating racism and xenophobia designed to ensure that racism and xenophobia are punishable in all Member States by effective, proportionate and dissuasive criminal penalties at the European Union level.

The ICERD, through article 4, "condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form". Article 4 of ICERD clearly sets out the obligations of the signing and ratifying States by stating that state parties undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, *inter alia*:

> (a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons

> of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;
>
> (b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law;
>
> (c) Shall not permit public authorities or public institutions, national or local, to promote or incite racial discrimination.

Currently, with 170 ratifications by Member States as of August 2006,[88] the ICERD provisions remain the most important normative basis upon which international efforts to eliminate racial discrimination could be built.[89] The Committee on the Elimination of Racial Discrimination (CERD) in its General Recommendations VII[90] and XV[91] explained that the provisions of article 4 are of a mandatory character. According to CERD, to satisfy these obligations, state parties need to enact appropriate legislation as well as ensure that such legislation is effectively enforced. Nonetheless, harmonization has not been established and there remain different interpretations and applications of article 4. So far, 19 States have entered reservations and/or interpretative declarations in respect of article 4. Most notably, the US Government declared that the United States "does not accept any obligation under this Convention, in particular under articles 4 and 7, to restrict those rights,

[88] See Note by the Secretariat, Efforts by the Office of the United Nations High Commissioner for Human Rights for universal ratification of the International Convention on the Elimination of All Forms of Racial Discrimination, E/CN.4/2006/13, 15 February 2006, at <http://daccessdds.un.org/doc/UNDOC/GEN/G06/107/92/PDF/G0610792.pdf>.

[89] See Report of the Committee on the Elimination of Racial Discrimination, Sixty-fourth session (23 February – 12 March 2004) Sixty-fifth session (2–20 August 2004), No: A/59/18, 1 October 2004.

[90] General Recommendation No. 07: Legislation to eradicate racial discrimination (Art. 4), 23/08/85.

[91] General Recommendation No. 15: Organized violence based on ethnic origin (Art. 4), 23/03/93.

through the adoption of legislation or any other measures, to the extent that they are protected by the Constitution and laws of the United States". As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in his 1998 Report, "the ambivalence surrounding points related to the principle of the need to balance rights and protections is evident in the positions taken by Governments through the declarations and reservations they have entered to article 4".[92]

While there is an urgent need to review the functioning of ICERD and consider whether it should be updated, "great care must be taken to achieve an appropriate balance between the rights to freedom of opinion and expression and to receive and impart information and the prohibition on speech and/or activities promoting racist views and inciting violence"[93] as the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in his 1998 Report. That balance has yet to be reached and agreed.

In terms of the European Union developments, a draft Framework Decision on combating racism and xenophobia designed to ensure that racism and xenophobia are punishable in all Member States by effective, proportionate and dissuasive criminal penalties was proposed in November 2001. However, to date, no agreement has been reached on this initiative largely due to different approaches to limitations in the exercise of freedom of expression within the Member States of the EU. Similar drawbacks will be witnessed during the discussions involving the draft Television Without Frontiers Directive[94] which includes non-derogatory provisions to make

[92] Promotion and protection of the right to freedom of opinion and expression, Report of the Special Rapporteur, Mr. Abid Hussain, E/CN.4/1998/40, 28 January 1998, para. 7.

[93] Ibid., para. 8.

[94] Proposal for a Directive of the European Parliament and of the Council amending Council Directive 89/552/EEC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities (Television without frontiers), COM(2005) 646 final.

"non-linear media services" and "linear media services" subject to the same minimum requirements in relation to the prohibition of incitement to hatred. With the proposed Directive, the European Commission wants to ensure compliance with policy objectives relating to the protection of minors against harmful audiovisual content and the protection of human dignity including a ban on incitement to racial hatred. The recently announced European Union wide proposal to criminalize Holocaust denial, supported by Germany and based upon the above-mentioned similar but unsuccessful initiative in the form of a Framework Decision by the Luxembourg presidency,[95] faces similar obstacles based upon different approaches to limitations in the exercise of freedom of expression within the Member States.[96]

Despite all these significant policy initiatives, it remains problematic to develop common approaches in the face of cultural, moral and legal diversity at the European level, which has been shaped by historical, political and social experiences relating especially to wartime conflict. A fragmented approach is therefore unavoidable in terms of approaches to harmful Internet content. Ideally "states within Western Europe should especially avoid pandering to the lowest common denominator where the least tolerant [such as in respect of racist expression in France and in Germany] can set the pace".[97]

Effectiveness of Regional and International Regulatory Efforts

Substantial international efforts such as the CoE's Additional Protocol *concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* carry political significance but will such legislative initiative have an impact upon reducing the problem of racist

[95] See EU Annual Report on Human Rights – 2005, 12416/05, Brussels, 28 September 2005.

[96] German Presidency Press Release, "Outlawing racism and xenophobia throughout Europe", 29 January 2007, at <http://www.eu2007.de/en/News/Press_Releases/January/0129BMJantiracism.html>.

[97] Brackets added by the author. C. Walker & Y. Akdeniz, "The governance of the Internet in Europe with special reference to illegal and harmful content", [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, 5–19, at 14.

content on the Internet? Due to the global and decentralized nature of the Internet, government regulation and even prosecution of individuals who publish racist content on the Internet may have limited effect and application especially if the racist content is published and transmitted from outside the jurisdiction in which it is considered illegal.

The steps taken by a number of governments at the national level have shown their limitations, and a regional international regulatory initiative such as the CoE Additional Protocol aimed at punishing racism on the Internet will have no effect unless every State hosting racist sites or messages is a party to it, as rightly stated by a CoE Recommendation 1543(2001) on Racism and xenophobia in cyberspace.[98] The ratification process is a drawn out affair and it took over three years to bring the Protocol into force in March 2006 with only ten States ratifying it since January 2003. A considerable amount of time will be required to reach a substantial number of ratifications. This is not necessarily unusual as the ratification of such instruments is a very long process at the Member States level, and even one of the main supporters of the Additional Protocol, Germany has yet to ratify it, and France only ratified the Additional Protocol in early 2006.

However, States such as the United Kingdom, Spain, Russia, Norway, Italy, Ireland, and Hungary have not yet signed the Additional Protocol and the success of such a regional instrument depends upon the co-operation of all CoE Member States. Member States may be reluctant to sign and/or ratify it as becoming a party to the Additional Protocol may require substantial changes to national laws. Speech based restrictions may not be allowed by certain state constitutions, and the definition provided for “racist and xenophobic material” could conflict with state laws and constitutions. The offences included within the Additional Protocol – *inter alia*, dissemination of racist and xenophobic material, racist and xenophobic motivated

[98] CoE Recommendation 1543(2001) on Racism and xenophobia in cyberspace, 8 November 2001.

threats, racist and xenophobic motivated insults, and the criminalization of expressions which deny, grossly minimize, approve or justify acts constituting genocide or crimes against humanity – may not be all supported by the non-signing and non-ratifying Member States.

The reservations present in articles 3, 5, and 6 could also result in disparities between the parties to the Additional Protocol and harmonization may never take place in relation to “racist and xenophobic motivated insults” (article 5), and “denial, gross minimisation, approval or justification of genocide or crimes against humanity” (article 6) as these two articles allow the parties to the Protocol to reserve the right not to apply, in whole or in part, the offences provided within these articles. For example, within the Council of Europe region, only Austria, Belgium, the Czech Republic, France, Germany, Lithuania, the Netherlands, Poland, Romania, Slovakia, Spain, and Switzerland, have laws criminalizing the denial of genocide committed by the Nazis.[99] Yet, “the proliferation of Holocaust Denial websites dramatically underscores the limitations of any national laws, or even international conventions, to eliminate or punish any form of hate speech.”[100] A similar reservation is also provided in relation to the “dissemination of racist and xenophobic material through computer systems” (article 3) but only so far as the dissemination is related to material which advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. It is also provided that a party may reserve the right not to apply the dissemination offence provided in article 3 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies.

[99] See generally ECRI, *Legal Instruments to combat racism on the Internet*, report prepared by the Swiss Institute of Comparative Law (Lausanne), CRI (2000)27, Strasbourg, August 2000.

[100] A. Cooper and H. Brackman, “Punishing Religious Defamation and Holocaust Denial: Is There a Double Standard?” (2006) *Equal Voices*, Issues 18, EUMC, at <http://www.eumc.europa.eu/eumc/index.php?fuseaction=content.dsp_cat_content&catid=4498115372af1&contentid=44bb8bd0bd09f>.

It is difficult to speculate how effective a regional international effort such as the CoE Additional Protocol will be. The “one for all” rules advocated by the likes of the CoE Additional Protocol remain problematic and States with strong constitutional protection for freedom of expression such as the USA will not rush to sign and ratify such international agreements and conventions. In other words, there will always be safe havens to host and carry content deemed to be illegal by national laws or under the terms of international agreements, protocols, and conventions. Even if all Member States of the CoE sign and ratify the Additional Protocol, the problems associated with racist Internet content will not disappear. Certain websites will continue to be hosted in the United States and elsewhere in which the transmission of racist content is not criminalized. This, in a sense, reflects the true nature of the Internet which carries inherent risks. The key question is how to manage these risks.

It is not of course suggested that nothing should be done to tackle the problem of racist content on the Internet. But legal developments are lagging behind technological developments, and there are other options available to tackle such risks and problems in a global society. This should not be limited to developing international conventions, and adopting national laws. The development of international conventions and agreements and the implementation of such conventions, including the signing, ratification, and effective implementation by the States at a national level, is an incredibly slow and problematic process as witnessed by the implementation of the International Convention on the Elimination of All Forms of Racial Discrimination, the CoE’s Cyber-Crime Convention as well as that of the limited implementation of the Additional Protocol to the Cyber-Crime Convention.

Additional and Alternative Efforts to Combat Racist Content on the Internet

Regulation is often designed to reduce risk but alternative methods can be less costly, more flexible, and quicker to adopt than prescriptive government legislation. Hence, the other options include "doing nothing", social norms, self-regulation, co-regulation, and technical means, information, education and awareness campaigns.

Within the context of racism and xenophobia on the Internet, "doing nothing" is not a viable option given the extent and expanding nature of the problem. It was growing concerns over the availability of such content over the Internet that triggered the CoE to develop the Additional Protocol to the Cyber-Crime Convention. At the same time relying on social norms, customs and netiquette is also not a viable option as these will not be enforceable nor effective in a borderless and multinational, and multicultural environment.[101]

The Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003 encouraged self-regulation and co-regulatory initiatives regarding Internet content. Similar recommendations were also made in a CoE Recommendation (2001)8 on self-regulation concerning cyber-content.[102] The European Union's Action Plan on promoting safer use of the Internet[103] also supports and encourages self-regulatory solutions especially in terms of protecting children from harmful content. With self- and co-regulatory initiatives the States and international organizations can also co-operate with the NGOs and the private sector, and a "socially responsible private sector

[101] See E. Gelbstein and J. Kurbalija, *Internet Governance: Issues, Actors, and Divide*, DIPLO report, 2005, at <http://www.diplomacy.edu/isl/ig/>, p. 71.

[102] CoE Rec(2001)8, 5 September 2001.

[103] Decision No 854/2005/EC of the European Parliament and of the Council establishing a Multiannual Community Programme on promoting safer use of the internet and new online technologies, PE-CONS 3688/1/04 REV1, Strasbourg, 11 May 2005.

can help realize an Information Society that respects human rights".[104] This multi-actor approach is also supported by the UN's Durban Programme of Action[105] which encouraged the private sector to promote the development of voluntary ethical codes of conduct and self-regulatory measures, and policies and practices aimed at combating racism, racial discrimination, xenophobia and related intolerance.[106]

In terms of the role that can be played by Internet Service Providers (ISPs), they can contribute to the development of self-regulatory mechanisms such as industry wide codes of conduct as well as hotlines to report illegal content. In terms of liability, while a general monitoring obligation has not been imposed on ISPs in the Western world, this does not stop States issuing blocking orders. During 2002, North Rhine-Westphalia, Germany's most populous state, issued a blocking order to prevent German-based ISPs from providing access to websites based outside Germany (mainly in the US) if those sites host racist and neo-Nazi content.[107] The blocking order affected approximately 76 ISPs within that region.[108] Although there have been legal cases and appeals surrounding the blocking orders, a number of administrative courts have ruled that German authorities can continue to ask ISPs to block such pages.[109]

[104] Office of the High Commissioner for Human Rights, Background Note on the Information Society and Human Rights, WSIS/PC-3/CONTR/178-E, October 2003.

[105] See generally the Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance, Durban, 31 August – 8 September 2001, A/CONF.189/12, GE.02-10005 (E) 100102, 25 January 2002 at <http://www.un.org/WCAR/aconf189_12.pdf>.

[106] Ibid., para. 144.

[107] National Journal's Technology Daily, "Ban On Neo-nazi Web Content In German State; Upheld," 22 December 2004.

[108] Between 2002 and 2004 the Duesseldorf District Administration issued 90 ordinances against Internet providers in North Rhine-Westphalia, forcing them to block access to certain websites with rightwing extremist content. See US Bureau of Democracy, Human Rights, and Labor, Report on Global Anti-Semitism, January 2005, at <http://www.state.gov/g/drl/rls/40258.htm>. Note also Combating racism, racial discrimination, xenophobia and related intolerance and comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action Note by the Secretary-General, A/59/330, 4 October 2004.

[109] See generally E.T. Eberwine, "Note & Comment: Sound and Fury Signifying Nothing?: Jurgen Bussow's Battle Against Hate-speech on the Internet", (2004) 49 *N.Y.L. Sch. L. Rev.* 353; and C.D. Van Blarcum, "Internet Hate Speech: The European Framework and the Emerging American Haven", (2005) 62 *Wash & Lee L. Rev.* 781.

As racist websites and organizations seem to find refuge in the United States where they benefit from the protection offered by the First Amendment, the utility and effectiveness of such a “blocking and removal regime” remains to be seen. However, in addition to “blocking orders”, notice based takedown procedures have been developed in Europe. For example, the EU Directive on Electronic Commerce[110] provides a limited and notice based liability with takedown procedures for illegal content. The service providers need to act expeditiously “upon obtaining actual knowledge” of illegal activity or content “to remove or to disable access to the information concerned”.[111] Such removal or disabling of access “has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level”[112] according to the Directive.

Notice based liability mechanisms have been developed hand in hand with hotlines to report illegal Internet content. While most hotlines do have expertise in terms of content involving indecent photographs of children under the age of 18 (child pornography), the same may not be said for racist content on the Internet. This type of content is predominantly text based and in most cases assessing the racist nature of a Web-based publication may not be straightforward as in the case of content involving child pornography. However, expertise and specialized hotlines do exist in Europe, and it is worth mentioning the International Network Against Cyber Hate (INACH)[113], which acts as an umbrella organization for hotlines specialized in racist content. INACH was set up in 2002[114] by Magenta Foundation, the Dutch

[110] 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, *Official Journal of the European Communities*, vol. 43, OJ L 178 17 July 2000 p.1.

[111] Ibid, para. 46.

[112] Ibid.

[113] See <http://www.inach.net>. Note the INACH reports, *Antisemitism on the Internet*, April 2004, at <http://www.inach.net/content/INACH - Antisemitism on the Internet.pdf>, and *Hate on the Net – Virtual nursery for in Real Life crime*, June 2004, at <http://www.inach.net/content/inach-hateonthenet.pdf>.

[114] Note the INACH Annual Report for 2005 which was published during 2006 at <http://www.inach.net/content/INACH-annual-report-2005.pdf>.

Complaints Bureau for Discrimination on the Internet and by jugendschutz.net in Germany. The work of both the Dutch and the German hotlines is noteworthy in this field. For example, jugendschutz.net's activities resulted in action against 184 illegal extreme right-wing websites in 2003.[115] In 154 instances, websites were blocked by German ISPs or relevant parts removed from the Internet in cases where they were hosted within Germany. Of these, 107 were considered to be illegal websites based in Germany, while 47 were based in foreign servers.[116] During 2004, the hotline asked German hosting companies and service providers to block access or remove 131 further websites.[117]

However, although hotlines could play an important role in relation to illegal Internet content there remain significant question marks in terms of their operation. Hotlines are often criticized as there remain serious concerns for the policing role that can be played by such organizations. Many maintain that decisions involving illegality should remain a matter for courts of law rather than hotline operators. It has been argued that "these hotlines violate due process concepts that are also enshrined in international, regional, and national guarantees around the world".[118] While it may be tempting to identify and attempt to block content posted to particular newsgroups, websites, or other Internet forums that seem devoted to illegal material such measures could set dangerous precedents if hotlines assume the role of the courts. Such an approach could result in an act of privatized censorship that would come to be applied too broadly over time. As the Martabit report to the UN stated "while encouraging these initiatives, States should ensure that the

[115] jugendschutz.net, *Annual Report 2003: Right-Wing Extremism on the Internet*, at <http://www.inach.net/content/annual-report-jugendschutznet-2003.pdf>.

[116] See further jugendschutz.net, *Chart of illegal and blocked websites containing right-wing extremism 01.01.-31.12.2003*, 2003, at <http://www.inach.net/content/jugendschutz figures 2003.pdf>.

[117] jugendschutz.net, *"Right-wing Extremism on the Internet" - successful strategies against Online-Hate*, 2004 Annual Report, at <http://www.inach.net/content/jgs-annual-report2004.pdf>.

[118] Per Professor Nadine Strossen, from an ACLU Press Release, "ACLU Joins International Protest Against Global Internet Censorship Plans", 9 September 1999, at <http://www.aclu.org/news/1999/n090999a.html>.

due process of law is respected and effective remedies remain available in relation to measures enforced."[119]

In terms of avoiding access to racist content on the Internet, filtering tools have been developed to protect children deliberately or accidentally accessing such content. The market for filtering software is blooming, and there are currently around 50 filtering products (mainly US-based),[120] and approximately 40 of these block content that advocate or promote hatred and discrimination. For a long time, filtering software were seen as preferable alternatives to government legislation including at the US Supreme Court level,[121] and it has been stated that "promoting filter use does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished".[122] It was argued that filters might well be more effective than certain legislation and impose selective restrictions on speech at the receiving end, and would prevent universal restrictions at the source level. It was, however, acknowledged by the Supreme Court that "filtering software is not a perfect solution because it may block some materials not harmful to minors and fail to catch some that are".[123]

[119] Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session (Chairperson-Rapporteur: Juan Martabit [Chile]), E/CN.4/2006/18, 20 March 2006, at <http://daccessdds.un.org/doc/UNDOC/GEN/G06/119/23/PDF/G0611923.pdf>, at para. 47.

[120] See <http://kids.getnetwise.org/tools/index.php>.

[121] *Reno v. ACLU*, 117 S. Ct. 2329 (1997).

[122] *Ashcroft, Attorney General v. American Civil Liberties Union et al.*, certiorari to the United States Court of Appeals for the Third Circuit, No. 03–218. Argued March 2, 2004 –Decided 29 June 2004, at <http://supct.law.cornell.edu/supct/html/03-218.ZS.html>. See further *ACLU v. Reno II*, No. 99-1324. For the full decision see <http://pacer.ca3.uscourts.gov:8080/C:/InetPub/ftproot/Opinions/991324.TXT>.

[123] Ibid.

Limitations of such software has been detailed elsewhere[124] but it is worth noting briefly that filtering software could be defective[125] and such software are often criticized for over-blocking, leading to privatized censorship of a considerable number of websites for no particular reason.[126] Equally, filtering software are criticized for under-blocking by the users of such software, and according to many these kind of software do not block enough objectionable websites. Usually the criteria for blocking is decided by the software developing companies and there is no openness or transparency in terms of what is filtered out or why certain websites are filtered. Moreover, only a limited number of software developers offer appeal processes for removing websites from their databases. There are also freely available tools on the Internet which could be used to circumvent filtering. Therefore, although filters may play a role in terms of shielding children from harmful, or offensive Internet content, these tools should not be seen as an alternative to good parenting, and education. If their use is to be encouraged then their limitations or drawbacks should also be reported to the concerned user groups.

At the same time it should not be forgotten that the Internet itself can be an effective tool in the fight against racism.[127] The need to promote the use of new information and communication technologies, including the Internet, to contribute to the fight against racism, racial discrimination, xenophobia and related intolerance[128] is recognized by the above-mentioned UN Durban

[124] Y. Akdeniz, “Who Watches the Watchmen? The Role of Filtering Software in Internet Content Regulation”, in Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media (eds.), *The Media Freedom Internet Cookbook* (Vienna, 2004), pp. 101–125.

[125] Electronic Privacy Information Center, *Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet*, Washington, December 1997, at <http://www2.epic.org/reports/filter-report.html>.

[126] National Coalition Against Censorship, *Internet Filters: A Public Policy Research*, (written by Marjorie Heins & Christina Cho, Free Expression Policy Project), Fall 2001, at <http://www.ncac.org/issues/internetfilters.html>.

[127] Reports, studies and other documentation for the Preparatory committee and the World Conference: Consultation on the use of the Internet for the purpose of incitement to racial hatred, racial propaganda and xenophobia, A/CONF.189/PC.1/5, 5 April 2000.

[128] See Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance, Durban, 31 August – 8 September 2001, A/CONF.189/12, 25 January 2002, para. 92.

Declaration. According to the Declaration “new technologies can assist the promotion of tolerance and respect for human dignity, and the principles of equality and non-discrimination”.[129] As noted by an April 2000 UN report leading into the Durban World Conference “governments, intergovernmental organizations, national human rights institutions and non-governmental organizations are using the Internet to inform the public about their work and to spread positive messages of equality and non-discrimination”.[130] A number of initiatives aim to assist parents and teachers in preparing children for safer use of the Internet,[131] and within this context a recent Partners Against Hate initiative report highlights critical thinking skills as “one of the most effective tools to provide young people with protection against hate on the Internet”.[132] A similar approach has been taken at the OSCE level with recommendations that

> “Internet users should be educated about tolerance and that cooperation should be promoted among all actors, particularly non-governmental organizations and associations working to combat racist, anti-Semitic and xenophobic propaganda on the Internet”.[133]

Another good example of this line of argument is a pilot study of websites in English conducted by the European Monitoring Centre on Racism and Xenophobia (EUMC) to be used for intercultural training by children, young

[129] Ibid.

[130] Reports, studies and other documentation for the Preparatory committee and the World Conference: Consultation on the use of the Internet for the purpose of incitement to racial hatred, racial propaganda and xenophobia, A/CONF.189/PC.1/5, 5 April, 2000.

[131] Note particularly Partners Against Hate initiative report entitled *Hate on the Internet: A Response Guide for Educators and Parents*, ADL, December 2003, at <http://www.partnersagainsthate.org/publications/hoi_full.pdf>.

[132] Ibid., at page 30.

[133] The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/59/329, 7 September 2004. See further OSCE meeting on the relationship between racist, xenophobic, and anti-Semitic propaganda on the Internet and hate crimes, Consolidated Summary, PC.DEL/918/04/Corr.1, 27 September 2004, at <http://www.osce.org/documents/cio/2004/09/3642_en.pdf>.

adults, teachers and trainers.[134] A total of 273 good websites which deal with and promote cultural diversity were identified in the first half of 2002 by the pilot study.

In summary, there are currently only a limited number of specific self- and co-regulatory measures, including codes of conduct aimed at combating racist Internet content. However, there remain significant question marks[135] over the effectiveness and efficacy of the various mechanisms and tools currently offered by the private sector. Self- and co-regulatory measures may yet play an important role in the fight against racist Internet content. This will however be dependent upon substantial improvement of existing systems or the devising of less problematic alternatives.

Conclusion

As Farber rightly states, "hate on the Internet will not disappear overnight. But the intractability of the problem does not absolve us of the responsibility to engage in its resolution. The very size of the problem requires us to pursue multiple approaches for partnership with government, police services, schools, community groups and service providers".[136] Looking to the future, one can expect a trend towards "governance" rather than "government", where the role of the nation-state is not exclusive and where more varied forms of regulation, many in the private sector, come into play. The governance of the Internet will continue to evolve at the national, and

[134] A. Hieronymus, Using the Internet for Intercultural Training! A pilot study of web sites in English for children, young adults, teachers and trainers, EUMC, Vienna, September 2003, at <http://eumc.europa.eu/eumc/material/pub/intercult/Intercultural_training_Internet.pdf>.

[135] Note European Parliament Report A6-0244/2005 on the proposal for a recommendation of the European Parliament and of the Council on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry, 19 July 2005 (Rapporteur: Marielle De Sarnez)

[136] B. Farber, "The Internet and Hate Promotion: The 21st Century Dilemma", Canadian Human Rights Commission, *Hate on the Net*, spring 2006, Printemps, at <http://www.chrc-ccdp.ca/pdf/hateoninternet_bil.pdf>, pp 12–15.

international levels[137] "regardless of frontiers",[138] and policy initiatives need to reflect the decentralized nature of the Internet. Although legal regulation will doubtless continue to form an important part of future efforts to tackle the problem of online racism it will only ever form part of the solution. Ultimately, it will prove necessary to rely on additional measures in the form of self- and co-regulatory initiatives. The success of these measures will, in turn, depend upon substantial improvement of existing systems including the development of ISPs' codes of conduct, complaint and other mechanisms aimed at combating racist Internet content. If successful these measures would potentially be more flexible and could be more effective than prescriptive government legislation. However, consistent with recommendation 141 of the Durban Programme of Action, education about racist content on the Internet and how to foster tolerance, is arguably the single most effective way of combating racist content.[139]

The importance of education to promote respect and fight intolerance is highlighted in other broader forums especially following the events of 11 September 2001 with the rise of Islamophobia as well as anti-Semitism.[140] It is often argued that the development of good practice initiatives to reduce prejudice and "cultural, academic and educational initiatives, supplemented by a range of inter-religious and intercultural awareness events" is the best

[137] Note the World Summit on the Information Society, Tunis Commitment 2005, Doc. WSIS-05/TUNIS/DOC/7, 18 November 2005.

[138] Article 10(1) of the European Convention on Human Rights; article 19 of the Universal Declaration of Human Rights. See further Global Internet Liberty Campaign, *Regardless Of Frontiers: Protecting The Human Right to Freedom of Expression on the Global Internet* (Washington DC: CDT, 1998) at <http://www.cdt.org/gilc/report.html>.

[139] See Review of reports, studies and other documentation for the preparatory committee and the world conference: Report of the High Commissioner for Human Rights on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and on ways of promoting international co-operation in this area, A/CONF.189/PC.2/12, 27 April 2001.

[140] Note ODIHR (OSCE), *Education on the Holocaust and on Anti-Semitism: An Overview and Analysis of Educational Approaches*, April 2006, at <http://www.osce.org/publications/odihr/2006/04/18712_586_en.pdf>.

way to address such problems.[141] States, international, and specialized[142] organizations should continue to invest in education[143] and awareness-raising[144] campaigns to "provide users, particularly young people, with accurate information on the dangers of racism and anti-Semitism so as to counter the influence of racist organizations".[145] Information, education, and awareness campaigns should be a "crucial component in any initiative or programme to combat racism".[146] In January 2006, the UN Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action reaffirmed that States should promote the use of the Internet to create educational and awareness-raising networks against racism.[147] As stressed by the UN Intergovernmental Working Group, "States should increase awareness about the possibilities offered by new information technologies and continually develop tools to promote, among civil society, in particular parents, teachers and children on the use of the information networks".[148] The role the Internet can play as a powerful instrument to combat racism should not be underestimated.

[141] C. Allen and J.S. Nielsen, *Summary Report on Islamophobia in the EU after 11 September 2001*, European Monitoring Centre on Racism and Xenophobia (EUMC), Vienna, May 2002 at <http://eumc.europa.eu/eumc/material/pub/anti-islam/Synthesis-report_en.pdf>. Note further EUMC, *The fight against Anti-Semitism and Islamophobia - Bringing Communities together*, Vienna/Brussels, fall 2003, at <http://eumc.europa.eu/eumc/material/pub/RT3/Report-RT3-en.pdf>.

[142] ECRI, Specialised bodies to combat racism, xenophobia, antisemitism and intolerance, CRI(2006)5, January 2006, at <http://www.coe.int/t/e/human_rights/ecri/1-ECRI/3-General_themes/2-Examples_of_good_practices/1-Specialised_Bodies/ecri06- Good practices specialised bodies202005.pdf>.

[143] Note within this context Canada's Action Plan Against Racism, 2005, available through <http://www.pch.gc.ca/multi/index_e.cfm>.

[144] Note for example the Turn it Down initiative, a campaign against white power music and their Resource Kit at <http://turnitdown.newcomm.org/images/stories/tidresourcekit/turn_it_down_resource_kit.pdf>.

[145] Implementation of the Programme of Action for the Third Decade to Combat Racism and Racial Discrimination, Report of the United Nations seminar to assess the implementation of the International Convention on the Elimination of All Forms of Racial Discrimination with particular reference to articles 4 and 6 (Geneva, 9–13 September 1996), E/CN.4/1997/68/Add.1, 5 December 1996, para. 71.

[146] Reports, studies and other documentation for the Preparatory committee and the World Conference: Consultation on the use of the Internet for the purpose of incitement to racial hatred, racial propaganda and xenophobia, A/CONF.189/PC.1/5, 5 April 2000.

[147] Report of the Intergovernmental Working Group on the effective implementation of the Durban Declaration and Programme of Action on its fourth session (Chairperson-Rapporteur: Juan Martabit (Chile)), E/CN.4/2006/18, 20 March 2006, at <http://daccessdds.un.org/doc/UNDOC/GEN/G06/119/23/PDF/G0611923.pdf>, para. 103(b).

[148] Ibid., para. 103(c).

Internet Governance in Kazakhstan

Rachid Nougmanov

Internet Usage

Every year, the World Economic Forum (WEF) publishes *The Global Information Technology Report*, which has become a valuable and unique benchmarking tool to determine national ICT strengths and weaknesses, and to evaluate progress. The Report uses the Networked Readiness Index (NRI) to measure the degree of preparation of a nation or community to participate in and benefit from ICT developments. According to the latest Report, Kazakhstan's NRI has dropped from the 60th place in 2005 to 2006 to the 73rd in 2006 to 2007.[149]

In his September 2006 interview, Askar Zhumagaliev, head of the Information & Communications Agency, told Interfax that the number of Internet users in Kazakhstan had grown to 4 per cent of the population from 2.7 per cent on 1 January 2006. He tied this growth to a drop in Kazakhtelecom prices for connecting customers to the Internet. "The first serious drop in prices for Internet access was part of a company strategy to increase the number of users. 2.7 per cent of the population used the Internet at the beginning of the year, but now 4 per cent are active users," he said.[150]

Despite the growth in Internet penetration, the ICT developments in Kazakhstan are slowing down. The high cost of connection still remains the biggest obstacle. The largest national ISP is the State-owned monopolist

[149] See <http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm>.

[150] See <http://www.interfax.ru/e/B/finances/26.html?id_issue=11584058>.

Kazakhtelecom. As of 1 February 2007, they offer their customers the following options.[151]

Table 1. Dial-up Internet connection by Kazakhtelecom

Plans	*Rates in Kazakh tenge, excl. VAT*
Per minute	
Working days (Monday-Friday):	
from 08.00 to 18.00	1.66
from 18.00 to 23.00	2.05
Weekends (Saturday-Sunday) and national holidays:	
from 08.00 to 23.00	1.66
Monthly unlimited plan	12,791.00

The above per minute rates translate into 65 to 80 eurocents per hour. A customer would pay about 30 euros a month for basic email exchange without attachments, plus occasional web browsing, a few pages per session. No file downloads, no online chatting, let alone video conferencing. Should a customer opt for the unlimited dial-up plan, it would cost him or her about 82 euros per month. With the average monthly salary of 292 euros (as of January 2007)[152], coupled with the low bandwidth, this is not an attractive deal for most Internet users.

The next option is ADSL. It starts with various “Megaline” plans, that offer Internet connection limited by bandwidth and traffic in a highly complicated scheme (the quotes have been translated from tenge into euros at the OANDA Interbank rate since 1 February 2007).

[151] See <http://www.almatytelecom.kz/php1/tariffs/tariffs_PD.php>.

[152] See <http://www.stat.kz/index.php?lang=rus&uin=1171952750&chapter=1173855270>.

Table 2. "Megaline" ADSL by Kazakhtelecom

Plans	*Rates in euros, excl. VAT*		
Bandwidth, Kbps (download / upload)	Traffic included in the monthly fee, Gb	Monthly fee, €	10 Mb of additional incoming traffic, €
"Megaline Start"			
Active 128 / 128	0.4	11.11	0.83
Basic 128 / 128	0.8	17.77	0.75
"Megaline Plus"			
Active 256 / 128	0.6	20.80	0.78
Basic 256 / 128	1	27.72	0.70
"Megaline Optima"			
Active 384 / 128	0.8	28.89	0.72
Basic 384 / 128	1,2	34.66	0.65
"Megaline Turbo"			
Active 512 / 256	1.0	33.33	0.67
Basic 512 / 256	1,5	40.00	0.60
"Megaline Hit"			
128 / 128	-	24.27	*After reaching the allowed 7 Gb of monthly traffic, bandwidth drops to 32 Kbps*
128 / 128	-	22.99	*Same as above*

One-time activation fee: 40.24 euros

One-time installation fee: 11.70 euros

ADSL modem (to be purchased separately): from 69 to 600 euros

The allowed monthly traffic under the “Megaline” plans is very low, while the cost of every additional 10 Mb is very high, and the bandwidth is narrow by all modern standards. The initial one-time payments are also steep for an average user in Kazakhstan, ranging anywhere from the minimum 121 euros up to 650 euros. This option does not offer much advantage to the dial-up connection, considering the ratio of price per data, and does not add much to the ICT developments.

The today’s de facto standard in the world consumer market is unlimited ADSL connection. Kazakhtelecom offers that option, but the prices are very far from being competitive, as the following table demonstrates.

Table 3. Unlimited ADSL by Kazakhtelecom

Bandwidth, Kbps	*Monthly fee in euros, excl. VAT*
64	102.45
128	204.91
256	409.82
384	614.73
512	819.64
768	1,229.46
1024	1,639.29
1536	2,458.93
2048	3,278.57

One-time activation fee: 80.58 euros (modem not included)

The fee for unlimited traffic at 2048 Kbps with VAT included (14 per cent in February 2007) amounts to more than 3,700 euros a month. This is about

100 times more expensive than the price a customer in Western Europe would pay, while at the same time in Kazakhstan the average monthly salary is 10 times lower.

Currently, the bandwidth of 2048 Kbps is the limit for ADSL connection in Kazakhstan. Higher speeds are available only for cable connection, and here the price differences by comparison with the technically advanced countries are even more striking.

Table 4. Unlimited Cable Internet by Kazakhtelecom

Bandwidth, Mbps	*Monthly fee in euros, excl. VAT*
3	9,163.09
4	11,926.60
5	13,817.4
6	16,144.5
7	19,952
8	20,088
9	21,988
10	24,432

One-time activation fee: 302.12 euros

10 Mbps of unlimited traffic will cost a customer in Kazakhstan just under 30 thousand euros per month – about a thousand times higher than in Western Europe!

There is a small alternative to the state monopoly of Kazakhtelecom and their resellers. The highly advertised Satellite Internet (Kazlink) claims to be charging between 5 and 10 times less than the ADSL/Cable providers.

Their 1 Mbps Monthly Package is capped at 640 euros per month, and 2 Mbps cost 1,280 euros. The price is still prohibitively high for most users in Kazakhstan, and does not include the cost of equipment and installation (almost 300 euros), as well as the uplink connection (ADSL or dial-up) that has to be bought from a third party.

With all these numbers in mind, it is not surprising that Kazakhstan's NRI dropped dramatically in the WEF charts. The 4 per cent of Internet penetration in Kazakhstan is comprised partly of occasional dial-up home users who cannot afford regular daily Internet use. Others have limited free access at schools and universities and use Internet cafés from time to time. The majority of the rest of the users are corporate customers. With prohibitively high prices for individual customers, governmental and private offices remain by far the most popular places to go online in Kazakhstan. That explains the reason why only 4 per cent of the population are wired.

Internet Legislation

Under current legislation, all websites in Kazakhstan are considered mass media. The local Media Law is fully applicable to any website, be it a news service, blog, gaming community or personal page. As media outlets, websites are also subject to the Criminal and Civil Codes. Any user or professional journalist publishing their articles on the Internet can face a civil or criminal trial because of his or her publications.

In addition, there are two sets of regulations for governing the country top-level domain, .kz. The Public Association of IT Companies is responsible for the domain registration according to their own rules, which are in compliance with the ICANN standards.[153] At the same time, the State Committee on Informatization introduced their own regulations in April of 2005.[154] They

[153] See <http://nic.kz/rules/index.jsp>.

[154] See <http://www.zakon.kz/our/news/news.asp?id=40186>.

demand that every .kz domain must be hosted in Kazakhstan and also have two domain name servers in the country. However, not a single domain registration has yet been cancelled for being hosted abroad or using foreign DNS.

On 8 December 2005, the Association of IT Companies cancelled the registration of borat.kz, a domain owned by the British comic Sacha Baron Cohen portraying a false Kazakh journalist on his TV shows and in the film *Borat: Cultural Learnings of America for Make Benefit Glorious Nation of Kazakhstan*, which was in production at the time. The reason for that decision was not the foreign server located at the premises of 20th Century Fox in Los Angeles. Rather, the Association's President Nurlan Isin was straightforward in his interview to *Reuters*. "We've done this so he can't badmouth Kazakhstan under the .kz domain name," he said. "He can go and do whatever he wants at other domains."[155] For the first time, this precedent officially introduced control over content in Kazakhstan on the part of a registration service.

Another example is the case of navi.kz, one of the first online newspapers in Kazakhstan. In 2005, their domain was terminated without prior notice. Someone registered a trademark for its name, *Navi*, and claimed the domain ownership. The domain was promptly transferred by a court decision to the claimant who opened a new website, copied the design of the original site and posted their own materials, pretending to be the real *Navi*. *Navi* itself was forced to change the name to *Zonakz*, quit the .kz TLD for .net, and eventually moved the server abroad. They are now hosted in the US.

A recently introduced draft bill that requires publishing houses to get a licence from the Government will inevitably curb freedom of speech by

[155] See <http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20060907/borat_premiere_060907/20060908?s_name=tiff2006&no_ads=>.

narrowing the publishing market. Adil Jalilov, director of the MediaNet Centre for International Journalism, rightfully noted that if the bill becomes law, the opposition media will inevitably migrate over to the Internet.[156]

In summer 2006, shortly after the SCO meeting, Kazakh Minister of Information Yermukhamet Yertysbayev promised to develop a new policy on regulation of Internet media in Kazakhstan by the end of the year. In an interview published in Kazakhstan's *Vremya* newspaper, Information Minister Yermukhamet Yertysbayev said he now wanted to stamp out "dirt" and "lies" from Kazakh websites. "Those who think it's impossible to control the Internet can continue living in the world of illusions," he told the paper. Yertysbayev said Internet journalism and other loosely regulated media could harm Kazakhstan's national security but did not say in what way. He was referring to new Internet legislation, but no further details were revealed.[157]

As of 1 April 2007, there is still no new Internet legislation, but on 10 October 2006 President Nazarbayev approved Kazakhstan's Information Security Concept. As the decree states, "the Concept provides a basis for developing and implementing a single state policy for the Republic of Kazakhstan to provide for information security, and its provisions will be taken into account in creating and developing a single information space for Kazakhstan and further improving the Government's policy of information technology development."[158]

The guidelines provide for increased governmental control over the "single information space", but offer vague and broad definitions of the threats. Here are a few excerpts:

[156] See <http://iwpr.net/?p=bkz&s=b&o=326086&apc_state=henbbkzdate2006>.

[157] See <http://www.tiscali.co.uk/news/newswire.php/news/reuters/2006/07/07/technology/kazakhstan-plans-to-tighten-internet-control.html&template=/entertainment/feeds/story_template.html>.

[158] See <http://www.medialaw.kz/index.php?r=85&c=2268>.

- Threats to information security come from “destructive illegal political, religious, and economic organizations”;
- From “certain foreign political, economic, military, and information structures”;
- And even from “certain individuals and entities”.
- Among external threats are “unconstructive policies of foreign States in conducting global information monitoring and disseminating information and new IT systems”;
- “Operations of foreign political and economic organizations aimed against the interests of the Republic of Kazakhstan.”
- Domestic threats are “unlawful activities of political and economic organizations in creating, disseminating, and using information.”
- In the political field, information security work targets are “public consciousness and the political persuasions of various groups of the public, as shaped by domestic and foreign media;”
- “The system whereby political parties and civic organizations popularize their views in the media”.
- Threats to information security in the political field are posed by “negative propaganda or psychological impact on society exerted by domestic and/or foreign media that excite social, ethnic, inter-confessional, and tribal discord and set various population groups against the nation’s leadership in the interests of certain political forces;”
- “politicization of the system that shapes the public opinion, use of sociological survey findings to falsify or make a biased interpretation of the information obtained;”

Expressed in such all-encompassing terms, the Concept allows for any interpretation of its guidelines, easily triggering the Soviet-style “spy mania”, when any dissident individual, organization, or an entire country could be named an “enemy of the nation”.

Criminal Prosecution

The first case of criminal prosecution for online journalism was reported in July 2002. The KNB (Committee of National Security) opened a criminal case against independent journalist Sergey Duvanov for publishing his article “Silence of the Lambs” on KUB.kz, an independent blog service.[159] The article allegedly hurt the dignity of the President of Kazakhstan. Soon, however, the charges were dropped.

In 2006, the KNB filed a suit against Kazis Toguzbayev for publishing two articles on the same blog service, with the same charges as the Duvanov case. On 22 January 2007, an Almaty district court handed down to the journalist a two-year suspended prison sentence for “Infringement on the honour and dignity of the President” under article 318 of the Criminal Code. The sentence was followed by a plea from OSCE Representative on Freedom of the Media, Miklós Haraszti, who called for the removal of special insult laws in Kazakhstan which give elevated protection to state officials from verbal offence.[160]

Another case was reported by the independent journalist Andrey Sviridov. In 2003, the year when Internet filtering was at its peak in Kazakhstan, Sergey Musorin filed a complaint with the local prosecutor’s office, accusing his ISP of blocking access to his favourite website, eurasia.org.ru. In response, the prosecutor opened a criminal case against him for compromising the security system of Kazakhtelecom. He was beaten, sentenced and sent behind bars. Later he was amnestied and quit Kazakhstan.[161]

[159] See <http://www.kub.kz/article.php?sid=1140>.

[160] See <http://osce.org/item/23098.html>.

[161] See <http://www.club.kz/index.php?lang=ru&mod=discuss&submod=large&article=217>.

Blocking and Filtering

Legislation is not the only way to limit the free flow of information. There is a long history of content filtering by the local ISPs in Kazakhstan. The authorities maintained a list of independent websites that were marked "destructive" for their criticism of the Government. Among them were kub.kz, navigator.kz, respublika.kz, zhakiyanov.info, club.kz, eurasia.org.ru and freeas.org.

For instance, KUB.kz was blocked for more than three years by Kazakhtelecom and Nursat, from January 2002 to April 2005. The site was inaccessible for local customers, as if it did not exist. As it was blocked by the IP address and not its domain name, by simply changing the IP address it could be accessed again for a week or two before the ISPs blocked the new number. The server did the change several times, and the pattern persisted. At the end of March 2005, after another IP change, the local ISPs finally stopped blocking. Approximately at the same time, the filtering of other websites ceased, too.

However, Yuri Mizinov, the chief editor of the online newspaper Zonakz.net (formerly known as *Navigator*), reports that two websites, freeas.ord and eurasia.org.ru remain blocked for dial-up users in Kazakhstan. Furthermore, Mizinov describes a new method of restricting access to "destructive sites". This method consists of increasing the connection latency. Users click on a link and wait for several minutes for the page to open. Finally, they give up and go elsewhere.[162] Coupled with the unrealistically high price of the Internet connection, this is a sure way to detour people from the unwanted information.

[162] See <http://www.club.kz/index.php?lang=ru&mod=discuss&submod=large&article=217>.

Recommendations

In spite of the low level of penetration in Kazakhstan, the growing importance of the Internet is gaining close attention from the State. State regulation will inevitably find its way into this field, which just a few years ago seemed to be out of the Government's control.

What can be done by the OSCE and press freedom organizations to facilitate the free flow of information in Kazakhstan? It is important to support the view of the World Press Freedom Committee that "governance" must not be allowed to become a code word for government regulation of Internet content.[163] Governments, which already censor their own Internet traffic, seek content controls internationally and/or legitimization of such controls nationally. The system must not be reorganized to permit this on an international level or encourage it at the national level.

The Declaration adopted by the World Summit on the Information Society in Geneva on 12 December 2003 could provide important guidelines and principles for any changes in the Internet governance system:

1. There should be no controls over content or modifications of the Internet's technical "architecture" that facilitate or permit censorship of news or editorial opinion. Nor should "self-regulation" be allowed to become a surrogate for governmental regulation of content on the Internet.

2. The system should explicitly commit itself to respect and to implement Article 19 of the Universal Declaration of Human Rights, and to the fundamental principle of press freedom. National or international security concerns must not be allowed to limit freedom of expression, including news and editorial comment, in cyberspace.

[163] See <http://www.wpfc.org/>.

3. Considerations of “ethics” should not be allowed to become a veiled approach to introducing or allowing censorship.

4. There are many forms of communication over the Internet, and it is important not to confuse them. News, for example, is different from such things as pornography, pedophilia, fraud, conspiracy for terrorism, incitement to violence, hate speech, etc., although there may be news stories about such problems. Such matters are normally covered in existing national general legislation and should, if appropriate and necessary, be prosecuted on the national level in the country of origin.

Concerning Internet Governance in Kazakhstan, it is recommendable to analyse the Information Security Concept and see if it complies with OSCE standards. The OSCE could work out possible measures of de-monopolizing Internet services and reducing prices to the internationally acceptable level, allowing for competitiveness among local and foreign ISPs, especially in view of Kazakhstan’s ascension to the WTO. I would also recommend that it should be considered that networks in Kazakhstan and other Central Asian republics should be monitored for content filtering, using the method developed by Ben Edelman and successfully tested in China and Saudi Arabia.[164]

And finally, the Government should be urged to recall the State Committee on Informatization Regulations of April 2005, to support affordable and safe hosting of websites with the national ISPs, and to guarantee that no content control in any form is exercised by the registration or hosting services in Kazakhstan.

[164] See <http://www.benedelman.org/>.

Internet Governance in Georgia

Ana Dolidze

Introduction

This article aims to present the main legal instruments for regulating the Internet in Georgia as well as analyse the quality of Georgian legislation related to Internet regulation. Being one of the first attempts of this kind, the article does not envisage in-depth and detailed analysis of each and every legal act pertaining to Internet use. On the contrary, it attempts to provide the reader with an overview of Georgia's major legislative acts on the subject and brief discussion on relevant protection mechanisms as well as deficiencies.

As many readers might not be fully aware of the Georgian legal system, the article starts with background information on Georgia's legal system. What follows is a description of legislation concentrating on three fields: the regulation of ISPs' activity, Internet content regulation in Georgian legislation, a discussion of criminal legislation to fight cybercrime and an overview of the most recent draft legislative initiatives on the topic.

Background

Since independence, Georgia's legal system has undergone significant reform. This has included fundamental reform of criminal, civil and administrative law and has involved the incorporation of many principles from continental jurisprudence and common law systems. It has also involved bringing the law into line with international human rights standards, notably the European Convention of Human Rights. Importantly, the General Administrative Code of Georgia includes a chapter on Freedom of Information, which provides regulations concerning the provision of public information by state agencies and is framed so as to incorporate many relevant principles from similar legislation in Europe and in the USA.

It should be noted that procedural legislation is currently in the process of reform, and the focus here is to balance continental European and common law principles, bringing in traditional common law notions such as jury trials, stage and procedure of confirmation of charges etc.

The Constitution of Georgia

The Constitution of Georgia, adopted in 1995, is the supreme law of the State. Article 6 of the Constitution provides for the hierarchy of legislation and also mandates that all other laws should correspond to the provisions of the Constitution.[165] The following is the hierarchy of normative acts enforced in Georgia, as articulated within Article 19 of the Law on Normative Acts:

a) Constitution of Georgia
b) Constitutional agreement
c) International agreement of contract of Georgia
d) Organic Law of Georgia
e) Law of Georgia, *reglement* of the Parliament of Georgia, Presidential Ordinance
f) Presidential Decree
g) Decision of the Parliament, Decision of the Government of Georgia
h) All other sub legal acts, such as Order of the Minister, decision of the Chamber of Control, etc.[166]

Moreover, the Constitution requires that Georgian legislation conform to internationally recognized norms and principles. Of particular interest in the context of the protection of human rights is the provision within

[165] Article 6, Constitution of Georgia.
[166] Article 19; Law of Normative Acts of Georgia.

the constitution which requires that the State “recognizes and protects universally recognized human rights, as eternal and supreme human values”.[167] This provision establishes Georgia as a monistic legal system, i.e. a system whereby international principles enshrined in international treaties have direct application and can be directly invoked before courts and administrative bodies, without the need for their translation into domestic legislation.

Legislation Regarding Internet Regulation

Up until recently, Georgia could be regarded as one of the most liberal countries in terms of regulation of the Internet. Before analysing recent legislative proposals that in the author’s view attempt to curb freedom of expression on the Internet, it is worth taking a look at legislation related to regulation of Internet use. Legislation can be roughly divided into three categories: legislation concerning the activity of Internet service providers (ISPs), laws and regulations regarding Internet content and criminal legislation related to the definition of cybercrimes and related punishment.

Legislation Related to the Activity of ISPs

The Law of Georgia on Electronic Communications adopted by Parliament on 2 June 2005 regulates the issue of Internet service provision in Georgia. The law provides for the legal basis for provision of services related to electronic communication on the territory of Georgia.[168] It also governs the rights and responsibilities of the Georgian National Communications Commission related to the authorization and licensing of electronic communications services.

The law provides that activity in the sphere of electronic communication is possible only after receipt of due authorization.[169] This is provided by

[167] Article 7, Constitution of Georgia.
[168] Article 1; Law of Georgia on Electronic Communications.
[169] Article 14; Law of Georgia on Electronic Communications.

the Commission which also maintains a registry.[170] In order to receive authorization, an entity applies to the Commission with a declaration, which the Commission then approves.[171] Applicants should also provide information on their legal status and a brief description of services that they propose to offer. Information regarding the legal status should be certified with certificates from the official registry of entrepreneurs.[172] It is worth noting that the law does not discriminate between commercial and non-profit entities, allowing both to apply for the provision of electronic communications services.[173] The Commission maintains the database of all entities authorized to provide services and the records are accessible to the public.[174] Within ten days of receiving the application, the Commission provides authorization by entering the data about the applicant into the public registry. Within seven days after authorization was granted, a certificate of authorization is issued to the applicant.[175]

The law lists a series of obligations that are incumbent upon the provider, including non-discrimination between users, financial accountability and transparency as well as prohibition of monopoly. It is worth emphasizing the terms upon which the Commission is entitled to sanction the provider. The law underlines that the Commission continuously monitors the terms of the law as well as that the regulations are being complied with. It is noteworthy that the Commission is only entitled to fine the providers, with varying amounts depending on the nature and continuity of the offence. It is not endowed with the power to revoke the authorization or otherwise hinder the operations of the provider.[176] This limit is indeed laudable from the perspective of the accessibility of Internet services, as the law does not

[170] Article 15; Law of Georgia on Electronic Communications.
[171] Article 16(1); Law of Georgia on Electronic Communications.
[172] Article 16(3); Law of Georgia on Electronic Communications.
[173] Article 2(f); Law of Georgia on Electronic Communications.
[174] Article 17; Law of Georgia on Electronic Communications.
[175] Article 18; Law of Georgia on Electronic Communications.
[176] Article 45; Law of Georgia on Electronic Communications.

endow the Commission with mechanisms to stop or otherwise hinder the activity of the ISP.

Regulation Regarding Internet Content

There are several pieces of legislation that deal with the regulation of Internet content in Georgia: the Law of Georgia on Protection of Minors from Negative Influence adopted by Parliament on 28 September 2001; the Law on Freedom of Press and Speech, adopted by Parliament on 24 June 2004, and the Law on Intellectual Property and Related Rights, adopted by Parliament on 22 June 1999.

The Law on Protection of Minors aims to protect juveniles from negative influence as a result of viewing video and printed productions, consumption of alcohol and tobacco products and gambling activities.[177] With the current deluge of video and graphic materials on the Internet, it is important to study relevant provisions in Georgian legislation. Although it prohibits exposure of minors to video productions that can adversely impact their health, intelligence or emotional development, the law mainly elaborates on proper identification of such material while it is being transmitted on regular broadcast media and provides for specific requirements concerning the airing time of films containing certain material.

First of all, the law disregards modern methods of information transmission, including the Internet. And therefore, the issue of broadcasting harmful content through the Internet completely falls out of its ambit. The same concerns the quite widespread practice of Internet gambling, which seems to have been similarly omitted from regulation. To a certain extent this is understandable as at the time of its adoption (2001) the Internet was not a widespread instrument of communication. Yet with the gradual increase of

[177] Article 2; Law on Protection of Minors.

Internet users in Georgia there is a continuing need to regulate these aspects in conformity with widely accepted international standards.

Article 24 of the Constitution of Georgia relates to freedom of expression. It provides that "every individual has the right to freely receive and disseminate information, to express and disseminate her or his opinion orally, in writing or in any other form […]." Moreover, it lists the basis for restrictions of freedom of expression. "[…] Clauses under 1 and 2 can be restricted by law when conditions make it necessary to do so in order to guarantee and by the conditions necessary in a democratic society for the guarantee of state and public security, territorial integrity, prevention of crime, and the defence of rights and dignity of others, to avoid revelation of confidentially received information or to guarantee the independence and impartiality of justice in a democratic society." Furthermore, article 17(1) states that "A person's honour and dignity are inviolable" and article 23 protects "intellectual creativity and intellectual property rights."

The Law of Georgia on Freedom of Press and Speech complements the Constitutional provisions listed above. It is interesting that the law specifically mentions that it is applicable to the Internet as it defines "media as print or electronic means of mass communication, including the Internet."[178]

The law devotes extensive attention to defamation and yet the provisions are not sufficiently defined to function as a full defamation regime.[179] *Article 19* expressed its reservations concerning draft article 8, nowadays article 9 of the law, sanctioning content regulation in nine specific areas based on several arguments, including vagueness of definitions.[180] *Article 19*

[178] Article 1; Law of Georgia on Freedom of Press and Speech.

[179] *Article 19*, memorandum analysing the Draft Law of Georgia on Freedom of Press and Speech, prepared by the Liberty Institute at <www.article19.org> at p. 12, it is noteworthy that the draft was passed by Parliament only with minor changes, so the views of *Article 19* expressed on the draft remain pertinent as well to the law.

[180] Ibid. p.13.

recommended that the draft article 8 be removed.[181] However, despite this recommendation, the article was adopted in the initial form, permitting content regulation.[182] The law provides that content regulation can only be exercised in a manner of non-discriminatory, neutral limitation.[183] Therefore, although the Law of Georgia on Freedom of Press and Speech affords a high level of protection to freedom of expression against attempts of pressure through defamation proceedings, vague provisions related to content regulation pose considerable risk of interference with freedom of expression, including via the Internet.

The use of intellectual property over the Internet is an equally important issue. The Law of Georgia on Intellectual Property and Related Rights protects works of science, literature and art, performance, audio and video material and databases, which are owned by the citizen of Georgia, Georgian permanent resident, and legal person registered in Georgia. Moreover, it affords its protection to those works that were published or made in Georgia for the first time.[184] It has to be stressed that initially intellectual property related provisions were part of the Georgian Civil Code, which came into effect in 25 November 1997, yet at a later stage were removed from the Code and adopted as a separate piece of legislation. The provisions of the law were adopted from the model legislation provided by WIPO and seem to be in conformity with the standards of Trade-Related Intellectual Property Provisions of the World Trade Agreement.[185]

Unfortunately, neither of these laws specifically mentions the Internet. However, it provides for an expansive definition of "publicizing" protected material, which includes publication of material through any "other means",

[181] Ibid. p.14.

[182] Article 9; Law of Georgia on Freedom of Press and Speech.

[183] Ibid.

[184] Article 3; Law of Georgia on Intellectual Property and Related Rights.

[185] Bruce McDonald, *Intellectual Property Protection in the Republic of Georgia* <http://ourworld.compuserve.com/homepages/usazerb/414.htm>.

in addition to publication on the air or via cable.[186] Therefore, although the law does not regulate use of intellectual property over the Internet, it gives full possibility for protection by not limiting itself to other specific media.

Georgia's Criminal Legislation Regarding Internet Use

Chapter 35 of the Georgian Criminal Code deals with computer crimes. Article 284 criminalizes illegitimate access to computer information. It concerns information stored in the computer, system or network protected by law, and declares the action punishable if it resulted in the destruction, blocking, modification or acquisition of information or damage of the computer system or network. The action is punishable with up to two years of imprisonment.

Article 285 of the Code relates to the creation, use and dissemination of a program damaging computer technologies. The necessary element of the crime is the intentional character of the action.

Article 286 declares the violation of the rules of using computer technologies punishable. However, it requires the person to have authorized access to a computer, computer system or network. As a result of the crime, information protected by law must have been destroyed, blocked, modified or multiplied or any other grave consequences incurred.

The crime of cyber terrorism is placed separately together with other terrorism crimes, and is defined as “illegal acquisition of computer information protected by law, its use or threat of use, which poses the threat of grave results, and violates public security, state strategic, political or economic interest, committed with the purpose of coercing the population and/or influencing the state agency.” Article 324(1), defining cyber terrorism was added recently to the Criminal Code of Georgia.[187] The crime is

[186] Article 4(d); Law of Georgia on Intellectual Property and Related Rights.
[187] Amendment of #3530 of 25 July 2006.

punishable with imprisonment for 10 to 15 years. The same activity which resulted in the death or other grave consequences is punishable with imprisonment from 10 to 20 years or a life sentence.

It should be noted that this indicated legislation has been subject to little change since its adoption.[188] It was only sanctions of several articles that were changed to be brought in line with the overall reform of sanctions in the Criminal Code. Moreover, the instances when these articles are applied are so rare and unknown that it is hard to discuss the quality of their formulations or need for their streamlining.

Pending Initiatives, Curbing Freedom of Expression over the Internet

This article would have already been concluded were it not for the current debate among Georgian media professionals on the Broadcasters' Code of Conduct to be adopted by the Communication Regulation Commission. The Law of Georgia on Broadcasting, adopted on 23 December 2004 by Parliament gave the Communications Commission the right to adopt the Code of Conduct for Broadcasters "a normative act, passed by the Commission … determining the rules of conduct for licence holders."[189] It should be adopted on the basis of consultations with the broadcasters as well as the public.[190] The initial deadline of 31 December 2006 for adopting the Code was postponed until 1 June 2007 by the Parliament of Georgia on 28 March. The deadline had already been postponed once until 1 April 2007 as broadcasters demanded more time for discussing the Code and suggesting their own proposals.

After its adoption, citizens will be able to complain to the Commission about any breach of the Code.[191] If a violation is found, the broadcaster in question

[188] Criminal Code of Georgia was adopted on 22 July 1999 by the Parliament of Georgia.
[189] Article 2(h); Law of Georgia on Broadcasting.
[190] Article 50; Law of Georgia on Broadcasting.
[191] Article 14(2); ibid.

is required to broadcast the Commission's findings within five days.[192] The Commission will also be able to initiate its own investigations, which can lead to the imposition of fines or the suspension or revocation of a licence.[193] Finally, broadcasters will be required to produce an annual report outlining their compliance with the Code.[194]

It would seem at first glance that the Code of Conduct for Broadcasters has little in common with the subject under discussion in this article. However, several provisions included in the draft presented by the Commission require attention and in the author's view attempt to interfere with freedom of expression on the Internet. The draft attempts to regulate the content of websites owned by the broadcasters. For example, it requires that the "contents of those websites that attract many children should correspond to the relevant audience and its expectations."[195]

Article 37 of the draft concerns Internet forums and message boards. Initially, the draft provides for the right of broadcasters to organize and maintain public Internet forums and message boards. However, the need for such thorough regulation of the area is rather questionable, especially considering that Georgian legislation in general contains protection against defamation and libel as well as other kinds of criminal conduct, whatever the medium. There is not enough space in this article for a detailed analysis of the provision, but a few quotes are enough to illustrate that the regulation is a threat to freedom of expression on the Internet and should not be supported. For example article 37(5) "on politically or otherwise intense questions, moderation should take place within the hour of displaying the post. Open message boards and forums on politically or otherwise intense topics should be avoided," or "topics for message boards and forums should be selected

[192] Article 14(5), ibid.

[193] Article 71, ibid.

[194] Article 70(3), ibid.

[195] Article 70(11), Draft Code of Conduct of Broadcasters, prepared by the Communications Regulatory Commission, <http://www.media.ge/files/qcevis_kodeqsi.pdf>.

on the basis of objective and transparent editorial criteria. Principles of justice and honesty should be abided to and the balance in publishing these viewpoints should not be violated."[196]

Thus, the article is precarious in two respects: on the one hand, over-regulation of the activity hardly leaves any room for action for those interested in maintaining the forums and message boards and gives a frequent reason for interference on the part of the Commission. On the other hand, it contains referral to vaguely defined and general principles, which cannot be evaluated objectively and might serve as the basis for unfair interference with the activity of the broadcaster through sanctioning.

The attempt to regulate the content of the websites operated by licence holders was criticized by *Article 19* as well, drawing a distinction between the regulation of broadcasting and regulation of the Internet.[197] The organization therefore recommended removal of all articles from the Code related to regulation of operating websites by licence holders.[198] Unfortunately, at the time of writing this recommendation has not been followed.

In conclusion, it can be said that the level of regulation of the Internet in Georgia is satisfactory. It is in general in conformity with international standards. However, as was pointed out above, Georgian legislation still contains provisions and mechanisms, sometimes contradictory and ill-defined, which on certain occasions might give leverage for illegitimate limitation of freedom of expression on the Internet. Therefore, it should be kept in mind that improving legislation is a continuous and arduous task, especially in relation to such a rapidly developing instrument as the Internet.

[196] Article 37(7) Draft Code of Conduct of Broadcasters, prepared by the Communications Regulatory Commission, <http://www.media.ge/files/qcevis_kodeqsi.pdf>.

[197] *Article 19*, Comment on the Draft Georgian Broadcasting Code of Conduct, August 2006, p. 6, available at <http://www.article19.org/pdfs/analysis/georgia-broadcasting-coc.pdf>.

[198] Ibid, p. 7.

III. The Multi-stakeholder Approach to Internet Governance

Protecting Minors on the Internet: An Example from Germany

Jennifer Siebert

The Current Situation in Germany

Computers are becoming more and more popular and dominant with young people and the number of households with children with Internet access is steadily increasing. According to the JIM and KIM studies[199], almost all young people in Germany have access to computers (98%) or the Internet (92%). 60 per cent of persons aged from 12 to 19 have their own computer, 38 per cent have Internet access in their room. More than two-thirds of all interviewed young people go online several times a week or even more. They mainly use the Internet for communication, mostly via instant messenger and e-mail and more than a quarter visit chatrooms on a regular basis. When assessing how they use the Internet, young people estimated that they spend 60 per cent of the time on communication, 23 per cent looking for information and 17 per cent for online games.

No medium has developed faster than the Internet. Children and young people often cannot cope with all the contingencies and require special attention.

What does Protection of Minors Mean?

Protection of minors means safeguarding the well-being of children and young people. The level of protection they need depends on their age and

[199] <http://www.mpfs.de/fileadmin/JIM-pdf06/JIM-Studie_2006.pdf>, <http://www.mpfs.de/fileadmin/Studien/KIM06.pdf>.

maturity. The aim is to nurture the personality development of children and young people and to shut out influences from the adult world which are not suitable to the development status of minors. On the Internet this is a challenge as media content can pose a threat.

It must be remembered that the Internet was actually designed for adults. It was originally dominated by academic content and the community regulated itself. This changed in the mid-nineties when children started to use the Internet. At the same time an Internet business evolved and the Internet became a commercialized mass media.

As a medium, the Internet poses new problems for the protection of minors. This is due to the rapidity of the Internet infrastructure and the ever-changing content and services, the sheer volume of content and providers, the cross-border accessibility and the "aggressiveness" of adult content. Standards for the protection of minors are set in youth protection laws.

Current Laws in Germany: The Youth Media Protection State Treaty

In Germany the protection of minors on the Internet was legally reformed in 2003. German lawmakers implemented the Youth Media Protection State Treaty (JMStV)[200] on 1 April 2003, presenting the model of a regulated self-regulation. The JMStV makes allowance for the convergence of the media. The legal framework for broadcasting and the Internet have been harmonized and share the same provisions.

The current situation concerning illegal and harmful content on the Internet in Germany is mainly dominated by the JMStV. Other acts and treaties regulate the responsibility of providers for content. And of course the German Penal Code criminalizes illegal actions. The principle regarding content in the media is: What is illegal off-line is also illegal online.

[200] <http://www.lfk.de/gesetzeundrichtlinien/jugendmedienschutzstaatsvertrag/main.html>.

The JMStV regulates youth protection in broadcasting and on the Internet, the tasks of the state media authorities and jugendschutz.net. It is the responsibility of jugendschutz.net and the appropriate state media authorities to observe and evaluate Internet content relevant to the protection of minors.

jugendschutz.net is the cross-national bureau for youth protection on the Internet in Germany.[201] The Youth Ministries of the federal states founded jugendschutz.net in 1997 and since 2003 it has been assigned to the Commission for Youth Protection in the Media (KJM). The latter was founded in order to achieve a consistent control of broadcasting and the Internet and to eliminate the fragmented supervisory structure. This avoids the same content in various media being subject to different laws.

The JMStV follows the principle of a regulated self-regulation. An essential aspect of this new youth protection model is to place a lot of responsibility and initiative in the hands of the industry. The self-regulatory bodies have a legally defined authority to make decisions which the state media authorities as the supervisory bodies can only control to a certain extent. The self-regulatory bodies have to be certified by the KJM according to the provisions in the JMStV.

With the supervision of the Internet the KJM entered new territory. This is why the new youth protection model counts on close interaction with other youth protection organizations. The KJM collaborates closely with jugendschutz.net, which has a lot of experience in youth protection on the Internet and supports the KJM. The tasks of jugendschutz.net in terms of the protection of minors on the Internet are specifically stated in the JMStV. The JMStV will be evaluated at the end of 2008.

[201] <http://www.jugendschutz.net>.

The JMStV basically defines three levels of youth protection:

- “Absolutely illegal content”, i.e. content which is illegal without any exceptions in Germany, e.g. child pornography, so-called posing photos of minors, bestiality, violent pornography, incitement to racial hatred, denial of the Holocaust, glorification of war, violation of human dignity
- “Other illegal content”, i.e. content which is illegal to be made accessible for minors, e.g. adult pornography, or content harmful to minors
- “Content endangering the development of children and young people”, e.g. explicit violent or sexual depictions which can have a negative impact on the development of minors

Both “absolutely illegal content” and “other illegal content” is generally not allowed in broadcasting or on the Internet. However, in the case of “other illegal content” there are some exceptions when it comes to the Internet. For example adult pornography or content included in the index of media harmful to minors (“indexed content”) are allowed under specific circumstances. They have to be presented in a so-called “closed user group”. The content provider has to ensure that only adults can have access. “Content endangering the development of children and young people” has to be protected by technical means, for example the so-called “youth protection programs”.

Closed User Groups

Closed user groups are the most important and the most effective technical measure in terms of the protection of minors. According to the JMStV, content providers have to make sure that only adults have access to pornographic, indexed and harmful content on the Internet. The age check has to be carried out through age verification systems.

Over the past years there have been disputes about the question of the protection level necessary for this age check. As it was not possible to come to an agreement with content and service providers, closed user groups were regulated by law. Based on these legal provisions the KJM defined the key points for the requirements of closed user groups. Basically two steps have to be taken. At least once there has to be an *identification*, an age check via a personal contact to make sure the person is of full age (which in Germany is 18).

In order to have a reliable age check it is a precondition to have at least one personal identification, e.g. through a "Post Ident procedure" by the German post or a reliable age check at an appropriate point of sale. The KJM also evaluated other suitable identification modules which can be based on a recent face-to-face control.[202] With these partial solutions which can be integrated in age check systems, the development of systems that meet the requirements of the JMStV is easier to accomplish.

Secondly there has to be an *authentication* at every usage in order to reduce the risk of passing the access data to minors. The authentication makes sure that only identified and age checked persons have access to closed user groups and it should also impede the circulation of access data to unauthorized persons. In order to ensure that harmful content can only be accessed by pre-identified persons of full age, various authentication methods can be applied. Generally a hardware component which cannot be easily reproduced is applied (e.g. ID chip, bank card). The risk of passing on access data to unauthorized persons can also be reduced by combining this with an integrated payment function.

According to the JMStV, it is the duty of content providers to develop and implement safe protection systems. However, companies can have their

[202] For more information see <http://www.kjm-online.de>.

concepts for closed user groups examined by the KJM in order to see if they comply with the legal standards.[203] Unlike for youth protection programs (see below), which the legislator demands as a protection measure against content endangering the development of children and young people, the JMStV does not contain an acceptance procedure for age verification systems. They have to be efficient and content providers can submit their system to the KJM for evaluation, i.e. they then have the statement that their systems meet the legal requirements.

In recent years courts of law also decided on the requirements for closed user groups and affirmed the standards set up by the KJM and specifically stated that plain identity card checks are not sufficient. The reason for this is that ID card numbers can easily be reproduced, either by just using an existing ID card number or by generating a valid ID card number, for instance using programs which can be downloaded from the Internet.

Youth Protection Programs

Content with a negative effect on the development of children and young people has to be protected from access by technical measures. This kind of content could pose a certain risk for minors, but it is not classified as harmful. As a result it is not subject to age verification systems so instead there have to be technical control mechanisms such as youth protection programs.

Youth protection programs can be applied by content providers to protect minors from unsuitable content. This is an alternative to the restricted broadcasting times on the radio and TV. The legal requirements for youth protection programs are set down in the JMStV. They differ substantially from age verification systems for closed user groups. Youth protection programs have to offer differentiated access to content with a negative effect on the

[203] The KJM has evaluated various age verification systems.

development of children and young people, whereas closed user groups have to ensure that minors cannot access adult pornographic, indexed or harmful content.

Content providers can either program a youth protection program or upstream it and they have to submit it to the KJM for approval. As yet no youth protection program has fulfilled the legal requirements and could be approved by the KJM. Pilot projects, however, are already receiving support. The KJM can allow pilot projects as test models with certain time limits in order to try out procedures or technical measures.

In these pilot projects, programs are tested for their efficiency, filtration performance, manageability, and acceptance. Every pilot project is concluded by an evaluation conducted by the KJM and the applicant. At the end, the KJM can accept the youth protection program if this meets all the criteria. However, according to the results of the EU's 2006 benchmark study of the Safer Internet Plan (SIP), filters are not effective yet.[204]

Other Methods

According to the JMStV, content providers have to provide ways of blocking access to content that has a negative effect on the development of minors using technical or other means. Unlike youth protection programs, "other technical means" do not have to be acknowledged by the KJM. The KJM has also decided that content providers comply with the requirements of "other technical means" if they use a positively rated age verification system. Though it cannot be deemed a "youth protection program" because ages are not differentiated, it is a way of controlling access to content that could have a negative effect on the development of minors. Other methods could be, for instance, time restricted accessibility to adult content and separating adult and children's content.[205]

[204] <http://www.sip-bench.eu/SIPBench%202006%20Detailed%20Report.pdf>.

[205] For more details see § 5 JMStV.

Implementing the JMStV

Considering the rapidity of the medium and the vast amount of content potentially harmful to minors, a comprehensive control of the Internet is not possible. The Internet is an accumulative medium combining various services and media under one “umbrella”. There is no obvious solution for the control and elimination of offences. jugendschutz.net tries to effectively make use of existing resources through co-operation and communication with relevant stakeholders, targeted actions, and concentration on content relevant to the protection of minors. Whenever there is a violation of the JMStV it is the task of jugendschutz.net to advise the content provider and to inform the self-regulatory bodies and the KJM so they can take further action.

The processing of content relevant to the protection of minors is subdivided into three basic steps:

- First, monitoring and determining which content on the Internet is relevant to the protection of minors is the task of jugendschutz.net and the appropriate state media authority.
- Second, the KJM then examines and evaluates potential offences and also decides on further measures to be taken.
- Third, the enforcement of these measures is again the responsibility of the relevant state media authority.

If the KJM identifies a breach of youth protection laws, it also decides on the sanctions. These sanctions depend on the seriousness of the offence which can range from content with a negative effect on the development of minors to absolutely illegal content.

The following sanctions for the breach of youth protection legislation are possible:

- Objections voiced in official letters to the content provider

- Interdictions issued to the content provider
- Blocking orders against the host or service provider
- Administrative offence procedures; institution of summary proceedings; referral to state attorney's office for criminal offences

The decisions of the KJM or the other relevant supervisory bodies are of course subject to general opposition legal proceedings.

The situation of youth protection on the Internet has improved over the last few years. Larger German content providers in particular now meet the new legal requirements outlined in the guidelines of the KJM. Now that pilot youth protection programs are being supported, jugendschutz.net can take up the operators of big portals on their obligation to deal with content which could have a negative effect on young persons. This is an important step towards the protection of minors on the Internet, because minors often access the Internet through the big portals, e.g. popular TV portals.

In order to meet the special challenges the Internet poses, jugendschutz.net developed a multidimensional strategy over the last years to protect minors. The aims are to take action against illegal content and at the same time to promote content that appeals to children and young people, to demand protection measures from content providers and to educate young Internet users to surf and communicate safely in the Net.

jugendschutz.net does extensive research on the Internet in order to identify new phenomena relevant to the protection of minors, to assess these and to take effective action against illegal content. Apart from the traditional "hot topics" such as sex, violence and right-wing extremism, jugendschutz.net systematically examines other hazardous Internet services, e.g. fora, chatrooms, instant messaging and mobile Internet, and technical protection solutions, e.g. age verification systems and filter systems.

When it comes to violations of youth protection laws it is often difficult to allocate liability on the Internet. In the Internet's most important service, the WWW, the content is relatively traceable. When it comes to interactive services e.g. communities, guest books, fora, which are attractive to children and young people it is more difficult. An unlimited number of users can post comments. The content is not long-lasting, because it is only relevant until it is replaced by more up-to-date contributions. Here, you cannot get hold of the author, but only of the operators of the platform. In the case of communication services like chatrooms, instant messaging, file-sharing systems and peer-to-peer networks, these can only be controlled in real time. Here too, the author is hard to identify and you can only track down the host provider. The more short-lived the content is, the harder it is to supervise it from the "outside" using the classic methods. This is the reason for the multidimensional approach of jugendschutz.net, as it is trying to make all parties aware of the issues involved in the protection of minors.

Multidimensional Approach

jugendschutz.net takes a multidimensional approach to protect minors. It takes action against illegal and harmful content by trying to withdraw the platform or to make it more difficult to find that kind of content. The actions range from official objections, supervisory action, and indexing proposals for host and service providers. When content hosted abroad is in question, jugendschutz.net has been able to achieve remarkable success by communicating with the host providers or through contacts abroad. jugendschutz.net is very much involved in projects at international level in order to further the development and implementation of cross-border protection standards.

Since Internet content needs no prior approval and many services on the Internet defy control, content providers have the obligation to provide for the protection of minors. jugendschutz.net not only insists that content providers meet the legal requirements, but also tries to sensitize them and to have them take safety measures which are possible and reasonable.

In spite of all these efforts, we will not be able to make the Internet itself safe for children. This is why communicating skills for a safe use of the Internet is an important task. jugendschutz.net has developed various handouts and brochures for parents, children and teachers.

In this field jugendschutz.net is working on various projects:

"A Net for Children – Surfing without Risk" – here jugendschutz.net presents recommended websites for children, informs about dangers for children on the Internet and gives concrete tips for safe surfing and for a competent use of the Internet.

"Chatting without Risk? Between a Big Grin and Cybersex" – here jugendschutz.net created a brochure providing a list of safe chatrooms and guidelines for children, young people and parents for chatting without danger.

"Klick-Tipps" for children and parents – here jugendschutz.net presents a regularly updated selection and review of recommended web content for children. jugendschutz.net offers this service to interested providers to present these "Klick-Tipps" for free on their websites in order to make their content more attractive to children and young people.[206]

Culture of Joint Responsibility

The worldwide nature of the Internet means that it is crucial for youth protection on the Internet to find successful international procedures and a common basis regarding illegal and harmful content.

[206] For more information see <http://www.jugendschutz.net>.

The Internet is increasingly being used by children and young people. The Internet has to be further developed into a medium which also offers attractive, communicative, creative content for children and young people tailored to their age and which allows them to surf and communicate without risk. Part of this responsibility is to take into consideration the inexperience and need for protection of underaged Internet users and to show reasonable diligence and sensitivity when selecting and designing Internet content. This notably applies to websites which are specifically directed at children.

Access to new information and communication techniques is not only exciting for children and young people because it allows them to communicate worldwide, it is also important for their professional future. jugendschutz.net works on handouts and manuals for parents and teachers in order to promote the media literacy of adults and children.

The work of jugendschutz.net not only concentrates on making sure laws are observed, but also tries to raise awareness of the needs of children and young people on the Internet. In a type of “culture of joint responsibility” industry, government and society are asked not to put anything on the Internet without prior thought to its consequences and also to provide content attractive to children. We can only ensure that our young people have a positive experience of online media if they do not stumble across unsuitable content. They still need protection from pictures, texts or movies that could scare or confuse them.

Conclusion

Freedom of speech and information is one of the most important basic rights in our society. Adults can and should decide for themselves how to use the media. However, there can be hurdles for adult access, if this is necessary in order to protect minors. Every fundamental right reaches its limits when it infringes on the fundamental right of others. And children have the right to live in a safe environment, the right to be protected from harm.

In terms of content that endangers children and young people or content that has a negative effect on their development, the providers have to take the necessary steps in order to prevent access by minors or to make it more difficult for them to gain access. The speed of the medium and the large amount of content requiring youth protection mean that a complete control of the Internet is no longer possible. The Internet is a collective medium combining various services and media under one "umbrella". There is no one right way to control it and to remove every possible offence. jugendschutz.net tries to use resources most effectively through targeted exemplary actions, co-operation with various partners and a concentration on content relevant to youth protection.

The Internet is an international medium without any borders. A global approach is necessary in the battle against illegal and harmful content. Working together on an international level, developing joint approaches to illegal and harmful content, and sharing expertise is an effective way to achieve a safer Internet.

Of course, the German model is not the "magic bullet", but it is a possible strategy towards a safer Internet for children and young people. The German model of youth protection on the Internet will be evaluated at the end of 2008 in order to assess the achievements so far and to adjust or improve the provisions accordingly.

The multidimensional and unbureaucratic approach of jugendschutz.net has proved itself. jugendschutz.net researches phenomena relevant to the protection of minors, takes action against offences, helps develop evaluation criteria, communicates with providers about the requirements of youth protection laws, assesses technical protection measures and develops handouts for parents and children.

In the past jugendschutz.net took numerous actions against illegal content on the Internet and achieved remarkable results. Most of the offences could be dealt with before supervisory measures were necessary, even when it came to offences hosted abroad. While it is often denied that protecting minors on the Net is feasible and parents are called upon to take care of the online safety of their children, jugendschutz.net insists on the responsibility of the providers and demonstrates that it is possible for them to make their services on the Internet safer.

In Germany, after the JMStV was enacted, jugendschutz.net concentrated on taking actions against illegal content. However, jugendschutz.net also started with the next step and focused on Internet content which is hazardous for children and young people and which can have a negative effect on their development. Here the enforcement of the JMStV is more difficult than in cases of illegal content. Perceptible improvements can be expected when technical protection measures such as youth protection programs are better defined, when content providers know exactly what is expected from them and when offences are sanctioned effectively.

On the Internet, technical protection measures are of more significance than in traditional media. This specifically applies to the mobile Internet, which is defying parental control more and more. Apart from filter solutions, self-regulation based on codes of conduct plays an important role. The collaboration of all relevant stakeholders is the first step towards effectively improving the protection of minors. At the same time safe surfing surroundings for children and young people have to be created and their needs and right to information must be taken into consideration.

Forum des droits sur l’internet: An Example from France

Isabelle Falque-Pierrotin, Laurent Baup

In the last years, the Internet world has played with two words: Internet and governance, combining the two in different understandings. The “governance of the Internet”: this expression has been flourishing in international caucuses and traditionally covers the crucial subject of domain names and the technical management system of ICANN. “Internet Governance”, another expression that has emerged in working groups, refers to all the Internet-related subjects, from infrastructure to content, which need decisions from public or private actors. In that case, the scope of international discussions is very extensive.

The World Summit on the Information Society (WSIS) in Tunis started to make a choice between these two paths when it stated that 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.”

Following the WSIS, the Internet Governance Forum (IGF) and dynamic coalitions have kept up the momentum. They try to organize international co-operations between public and private stakeholders on various Internet issues: security, privacy, and freedom of expression. Underlying these initiatives, we have started to realize that “Internet Governance” is a kind of new paradigm that is generated by digital networks.

In France we have been thinking along those lines for a long time. For the Forum des droits sur l'internet (Internet Rights Forum), Internet Governance is not a question of technology. It means the new ways of thinking and decision-making related to the complex digital world and their consequences in terms of roles and status for public and private actors. For us, Internet Governance means democratic challenge and modernization. The Internet Rights Forum has worked since its creation in 2001 to implement such ideas in practice.

The Creation of the Internet Rights Forum

The Irrelevance of a Top-Down Approach

In September 1997, the French Prime Minister, Lionel Jospin, asked the Council of State to analyse legal issues related to the development of the Internet and to highlight any necessary adaptations for the French legal system. From October 1997 to June 1998, the Council of State had to deal with the idea of a significant change in the way regulation is implemented by government authorities. France has always tended to follow a "top-down" approach which means that the State never really consented to give back some of its powers to different actors. That is the reason why the general philosophy of the report elaborated by the Council of State was so "modern"... and disturbing.

This report begins with a strong assertion: "Regulations introduced by the State must now combine with players' self-regulation, i.e. the intervention of Internet players to develop the principles of rule of law in environments where there is no such provision and to act in a preventive manner to curb infringements."[207] This recognition of interdependence between public and private-sector players has been the key element of the multi-stakeholder approach chosen by France on all Internet issues (protection of minors,

[207] Internet er les Reseauz Numerique <http://lesrapports.ladocumentationfrancaise.fr/BRP/984001519/0000.htm>

respect for human dignity, freedom of expression, privacy and personal data, respect for intellectual property, advertising etc.).

It has become obvious that the traditional approach of state regulation is not entirely suitable for the networked world. Its global nature makes it impossible to regulate this sector on a top-down and purely national basis. The very first regulatory initiatives, like the Communication Decency Act in 1996 in the United States, very quickly proved their inadequacy in the digital environment.

The private stakeholders, mainly businesses, then developed an approach based on self-regulation. In various sectors, companies agreed on codes of conduct defining common values and practices in order to outline the professional uses and respect fundamental rights. Although there have been some successful initiatives, such as the PEGI system for video games, these actions experienced ups and downs. And criticisms emerged straight away. Moreover these initiatives mainly concerned the trading sector of the Web. As a result a large amount of activities were not taken into account and the commercial approach to ethical codes of conduct often raises the issue of their impartiality. Nevertheless, self-regulation seemed to be one possible answer, provided it had limited and professional objectives. It shows, within the regulatory framework, how Internet actors can cope and implement the law.

Facing these two solutions, state and business regulations, the Council of State proposed the creation of a third way: a joint regulatory body. The idea was to set up a “co-regulation infrastructure”, allowing public and private players to meet, discuss subjects of common interest and combine their own regulatory tools.

Recognition of the Co-regulation Method Proposed by the Council of State

In 2000, MP Christian Paul was asked by the Prime Minister to audit the idea of co-regulation. He compiled a report called "Law and freedom on the Internet: Co-regulation, French contribution to a worldwide regulation".

"If democratic institutions want to fulfil their mission without being bypassed by reality, they must be able to treat the questions at stake with the necessary speediness and pertinence. They must do it by listening more and with better collaboration with all the actors and participating bodies. (...) This is not about defining a new source of law, a new regulation model, but about finding a methodology suitable for these new times. That is this method called "co-regulation". It is based on the idea that, given the novelty of these subjects and the diversity of actors involved, it is necessary to ensure that people with different opinions can meet and, when possible, make a consensus emerge."[208]

The main recommendation of the Christian Paul report was the creation of a new instrument: the Internet Rights Forum, a private law body of "general interest" covering all legal issues surrounding the Internet. Its role is to work out recommendations to the public and private actors on Internet-related issues (e-commerce, e-government, privacy, freedom of expression, protection of minors, intellectual property etc.). It provides a permanent dialogue spot and collaborative process between public and private actors, helping them to draft public policies and make decisions.

Apart from the publication of recommendations, the report insisted that the Forum should have an educational and information role for the general public, by producing users' guides or by answering Internet users' questions on its website.

[208] <http://lesrapports.ladocumentationfrancaise.fr/BRP/004001056/0000.pdf>.

The Forum also participates in international initiatives and has helped to create the European Internet Coregulation Network (EICN) in December 2003. Through EICN, members from seven different European countries can share experiences, good practices and knowledge; they can also give proposals to European institutions.

Finally, the Forum is responsible for the "mediateur du net", an Ombudsman service which helps to create trustworthiness on the Internet by allowing Internet users to find an alternative dispute resolution mechanism. To guarantee the independence of this collegial body, the Christian Paul report insisted that it should have funding. An annual subsidy is granted by the Government and the private members of the newly created association pay an annual contribution which is adjusted according to their respective turnovers. The report conclusions were analysed and discussed in-depth. Eventually, the Government decided to launch the Internet Rights Forum as an experimental structure with a first mandate of three years.

Functions and Challenges of the Internet Rights Forum

The Forum system is based on the idea of all the stakeholders sharing responsibilities to regulate digital networks. This is primarily because the protagonists have a legitimate right to collaborate in defining the rules they will have to implement. But also, and above all, because the Forum must efficiently address a great deal of issues which can only be solved by active participation of all categories of partners. Here we face the timeless problem of theory versus practice. What makes a legislative provision successful is its ability to be implemented in real life, its capacity to meet real needs at ground level. Therefore it is only logical to federate private interests, organizations of Web users and public authorities, since they are all interdependent. In other words they all play a part in the responsibility and tools of regulation and they all have the ability to evade the rule if they want.

The approach of the Forum is not to stress the differences between stakeholders but to understand what needs to be done in order to achieve consensus. It will then gradually become possible to enlarge the scope of agreement. This is the only process that is coherent with the issues we have to deal with in the Internet field. After all, when we talk about freedom of expression, we are not only referring to the Web but also the way the Internet is to be ruled.

An independent body

The Forum is a private law association with great autonomy. This status allows flexibility and openness. Its funding is shared between public grants and private contributions. The French Government is involved thanks to the Forum's mission of "general interest". The Forum must hold on to both its autonomy and its proximity to the State and the Administration, so as on the one hand to guarantee the impartiality of its decisions or recommendations, and on the other to allow its proposals to be taken into account by public authorities. Therefore the State is not a member of the Forum but its representatives are invited to participate in the Forum's working groups. With three partners – users, industry, public authorities – its composition is pluralistic in order to guarantee the impartiality of the Forum's recommendations and the balance of interests.

A legitimate body

Any Internet actor can be part of the Internet Rights Forum provided it pays its contributions. Industry representatives, consumer organizations, research centres, individual rights organizations – over 70 actors have already agreed to work in this neutral area in order to help shape the Internet environment.

The legitimacy of the Forum arises from the diversity of these partners which guarantee that the Forum's "voice" is not solely from the economic sector. Thus, thanks to users and associations participating in the working groups, the Forum can never be seen as a new lobby model.

So although the Internet Rights Forum is not a representative body in terms of constitutional laws, it is clearly a legitimate body because it is open to all interested actors and because there is an official and organized balance between their different interests. Moreover, individuals also take part in the discussions. Through online forums linked to working groups and through public consultations Internet users can contribute and express their views.

A democratic body

By permitting different actors to exchange contradictory views and allowing a consensus to emerge, the Forum is in keeping with the move towards participative democracy.

In absolutely no way whatsoever does the Forum claim to substitute the National Assembly of Deputies or the Senate in the legislative process. As mentioned before, the Internet Rights Forum is not a representative body; its goal is to enable the representatives in parliament to make a decision by helping the consensus to mature. On complex subjects, this can take quite a while and the Forum is a good neutral space for that. If consensus is reached, the result is brought to the official representatives for decision; if not, it is up to the Government to make a political choice between the different proposed solutions.

Helping democracy to function by drafting consensual rules, the Forum submits itself to democratic principles. It must not be seen as a totally free body with nothing to counterbalance and control it. It has to be fully transparent to the Government and the general public and to report back about its actions and the way it functions.

All the institutional information is available on websites; the representatives in boards are elected each year and the annual report provides the general public with information in order to monitor the Forum’s work during this process of elaboration. In addition, the status of the Forum means that it has the opportunity to introduce a minority view in a recommendation.

An explanatory body

The educational dimension of the Forum needs to be stressed: as the Internet becomes more and more popular, Internet users are becoming less aware of the characteristics of digital networks. Internet literacy is thus a key aspect of the Forum and it is the first layer of regulation. Informed and well prepared for the risks and opportunities of the Internet, individuals can play an active part in Internet regulation if needed.

The French approach is original, but it has required a real effort. This type of initiative does not belong to our cultural habits, as our tradition is to stay entrenched behind our "top-down" methods. The usual excuse is that debates in France are so emotional and passionate that our country can't be reformed.

Co-regulation is the new working method we want to offer our politicians in order to manage reform better. This collaboration and harmonization pacifies the debate because it is not a vertical top-down process. Instead it is a horizontal way of thinking and it takes into account the needs of all the partners. It belongs to the move towards participative democracy, which is very relevant in the French context nowadays. Six years on, the Forum is no longer experimental. The third convention with the public authorities has been signed. It has become a real asset in the French Internet policy with some remarkable initiatives.

The Outcomes of the Internet Rights Forum

Within six years, the Forum has become the point of reference for Internet rules. Its legal expertise is now well established on a national and international level and its consultation methods have proved to be an efficient way of building consensus on complex issues. This tool shows how new technologies can drive methodological innovation and help in creating adapted answers to the complex world.

Co-regulation as a Way to Gather Public Opinions

The Forum organizes debates on various themes so a large number of citizens can participate in the collective effort and their opinions and ideas can be transmitted upwards. Web users are welcome to react to our proposals for recommended rules or to any relevant questions. These reactions are then integrated within the framework of debates and working groups.

A particularly striking example is the project of the French electronic identity card. On this sensitive issue, the Forum suggested organizing a public debate to the Minister of the Interior so public opinions could be voiced before the law was examined by Parliament. The Minister officially accepted this proposal in January 2005.

The Forum then organized a public online discussion for four months and gathered more than 3,000 contributions. Public debates were also set up in six large cities in France so as to meet people and collect their opinions and visions of the stakes involved with the ID card. Finally, a survey was carried out.

The conclusions of the whole process were quite interesting. As a whole the survey showed that French people were in favour of the plan to create a mandatory electronic ID card and to set up a national databank of fingerprints to fight against fraud. Yet many very reluctant views were also expressed. To quote just a few opinions, people said they needed more guarantees that privacy would be respected and information on how biometric data would be used. They saw no real benefit in using the ID card to access administrative or sales services.

Based on this consultation process, the Forum was able to issue recommendations to the Minister of the Interior, Nicolas Sarkozy, so that he might adapt the project and take into account the misgivings and expectations that were expressed. Thus, this project will be carried out with a really wide consensus. This example illustrates the fact that bodies that consult many partners meet a real need and allow public authorities to define their project more precisely, bearing public opinion in mind.

Some may question the need for consensus. Is it utopian to seek a consensus? Do we need it to make a public choice? Of course not, and governments are still able to decide against the people. But it is becoming more and more difficult. People want to discuss, express their views and, this is the real change, have the chance to be heard. Therefore, as evidence of the maturity of our institutions, the State is asked to redefine its role in public policy-making. By organizing these consultations and taking a stand about their results, the State does not reduce its power. It only explains what is at stake and makes sure it will reach a legislative provision by taking every partner's views into consideration.

Co-regulation as a Facilitator of Negotiations

Co-regulation does not restrict itself to mere discussions before making a decision. It is a transferable method which can also be used to master negotiation techniques and practices. For instance, on the issue of teleworking, a framework agreement was signed with European trade union partners on 16 July 2002. It was the first time that the social partners from each Member State of the EU had reached such an agreement.

It was then necessary to adapt the agreement at a national level and rephrase it in internal law terms thanks to a deal between national unions and corporate representatives. This is never simple, particularly in France, where social negotiations are often tough and entwined in wider political issues. At the end of July 2003, the Minister of Social Affairs, Labour and Solidarity asked the Internet Rights Forum to analyse the impact of teleworking and make suggestions which could help and inform all social partners before the start of negotiations. The Forum had to invite the social partners around a table and the process started in a climate of real suspicion. Every partner was keen to protect its negotiation powers and did not want the Forum consultation to replace the “real negotiation”. A whole range of methods had been used for consulting and opinion gathering. One of the key elements was to ensure absolute respect for the balance of forces, and the recommendation formulated by the Internet Rights Forum managed to have nearly 95 per cent of its proposals accepted during the negotiation. Eventually, the national inter-professional agreement on telework was signed in 2005.

Co-regulation as a Contribution to Decision-Making

Since it was created, the Forum has published 24 recommendations on various themes as diverse as the fight against child pornography, electoral communication on the Internet or e-commerce. They have all been implemented, either by government, or by parliament or private actors, which goes to show that French style co-regulation is not merely a research process; it is indeed a contribution to decision-making.

One significant example can be cited in the field of online sales and specifically sales at auction. After criticism from the European Commission, the legal system of sales at auction in France changed with a law of 10 July 2000. This text put an end to the monopoly of auctioneers and set up a strict perimeter for this kind of activity. During the legislative debates, the representatives widened the scope of these provisions to all online sales by auction and to online commissions of “cultural goods” which are characterized by the fact that there is no adjudication or intervention by a third party in the signing of the contract.

The absence of a clear definition of a "cultural good" made it necessary for the Council of Voluntary Sales to create an autonomous definition based on two criteria: its age and whether there is a signature of an author, artist or trademark.

This definition and, more generally, the legal framework were heavily criticized by those involved in online auctions because of the specific nature of their activities. As a result, the Internet Rights Forum decided to launch a working group about these issues. As diverse actors were represented within this working group (online commission firms, users and public authorities), several propositions were made. The Forum first sensed that the definition of "cultural goods" should take into account the need to preserve the national cultural and historical heritage, security of transactions and the protection of contracting parties. The Forum also made several recommendations concerning the legal system of online commissions in order to ensure that the objectives of the law of 10 July 2000 are consistent with EU rules[209] in this matter. All this work helped to clarify the objectives and set up a balanced framework for online activities, separating the issues of consumer concerns from heritage protection.

These results reflect that the co-regulation approach can be the right answer in dealing with legal issues concerning the Internet. But can we widen the scope of this method? Is it possible to think of co-regulation as a new political model? The opportunities offered by this governance process are unanimously recognized, whereas the reluctant attitudes are mainly due to ideological or political reasons. But this method has also been placed at the basis of the IGF process. And this choice – at an international level – is probably proof that we can imagine a transfer of the co-regulation model to other issues or other countries.

[209] Such as the identification of both buyers and sellers; pre-emption system for the Ministry of Culture, better co-operation between online commission websites, Ministry of Culture and Ministry of the Interior in order to prevent illegal traffic.

Forecast

The co-regulation approach chosen by France has proven to be efficient in organizing regulatory answers for digital networks. It has helped France in the last years to implement balanced public policies on Internet issues and to build a common vision of the Internet society.

The question that now needs considering is: can this method go beyond drafting legislation and be applied for other purposes, like for instance designing purely functional tools for a whole profession? Can a multi-stakeholder process be used for the elaboration of professional tools like labels, certification and ethical charts? It would seem natural to give a positive answer to this question, because the development of common ethics only seems possible by gathering ideas from different partners who are likely to implement the ethical principles of their profession.

The Forum itself has recently started to enter into this new field. On 10 January 2006, mobile operators and the Ministry of Family signed a charter on multimedia mobile contents. Following this signing, operators asked the Internet Rights Forum to help them define a classification scheme for this kind of content. The scheme applied to multimedia content accessed only through operator portals (as they are the only ones for which a contract between operators and editors have been signed). Its objectives were to:

- Define contents classification levels on a common and transparent basis;
- Define the self-classification system and control of editors' commitments;
- Outline the different contents with parental control systems.

After months of discussions between the industry, consumers' associations and public authorities representatives, the classification scheme has been finalized.

This co-operation between industry, users and public authorities has undoubtedly been at the root of European thought leading to the signing on the “Safer Internet Day” last February of an agreement between the European Commission and European mobile operators on how to protect minors using mobile phones. This example is interesting since it parts with the traditional vision implying that the EU decides, States transpose the directives within their local legislation and actors apply the law. In this case, the trend has been reversed and the work of operators has reached the European institutions in a bottom-up process.

Some might say that this methodology is obviously reducing, if not denying, the role of the State. We do not believe this to be true. States remain at the centre of the decision-making process: they are part of the discussions and the only ones that can give the official stamp to the outcomes of the negotiations so that the results become operational. On the contrary, we believe that the co-regulation approach means that governments have the opportunity to adapt to the complexity of modern times. We have witnessed too many instances in our recent history when political decisions taken without a minimum of consultation have caused various degrees of conflict. The passing of some resolutions or laws is then systematically criticized by some protagonists who were not consulted and resent this. Digital networks, however, offer ways to resist this.

A different approach is therefore needed when tackling issues with such diverse interests; an approach based on the values of freedom of expression and sharing. The Internet has urged us to widen the scope of consultation and even to initiate negotiations on the processes behind the development of standards. It is legitimate to think that the same may be true for numerous issues in political life.

Co-regulation is a way for the State to understand complex debates, to make decisions enlightened by a practical vision and to build on its expertise.

This is a modern and democratic understanding of the roles of the State and there is no reason to be afraid of that. By replacing our French old-fashioned "top-down" habit with a horizontal approach, a new political model is clearly emerging which is more democratic and participative.

There is one point that illustrates this turning point: the setting of the agenda. Traditionally, it was the role of States to put a subject on the public agenda for legislative discussions. Now, with the help of the Internet, the public is emerging as an alternative authority to place subjects on the public agenda. The discussions in France on the DADVSI law[210] (the law on copyright and related rights in the information society) are a good example of such a phenomenon. The interoperability issue appeared in the forums and online discussions and there came a point when the deputies had to integrate it in the official discussions in the Chambers.

It is very difficult to resist public pressure because digital networks function as a viral system; once a subject starts to emerge in a specific community, it can easily reach others and spread to the whole Internet. In fact, Internet governance introduces a new political paradigm and the co-regulation approach tries to propose a way forward. Will it be strong enough to cope with ethical international divisions on freedom of expression and help consensus building? Or will we go back to State, block to block, oppositions. It is difficult to answer.

Obviously, Europe has a card to play. European institutions have been able to federate a certain number of countries around common ethical rules. Nevertheless, the small number of countries that have signed a text as

[210] French acronym for *Loi sur le droit d'auteur et les droits voisins dans la société de l'information*. The DADVSI law aimed at reforming French copyright law, mostly in order to implement the 2001 European directive on copyright. It generated considerable controversy when it was examined by the French Parliament between December 2005 and 30 June 2006, when it was finally voted through by both houses. The law mainly focuses on the fight against exchange of copyrighted works over peer-to-peer networks and the criminalization of the circumvention of digital rights management (DRM) protection measures.

consensual as the Additional Protocol to the Convention on Cybercrime of 2001 is a relevant indication on the practical efficiency and swiftness of this decision scheme.

By comparison, the Pan-European Game Information (PEGI) age-rating system of video games has been very revealing of the industry's ability to devise a system that is likely to be implemented in most of the Community territory while respecting the sensibilities of each State. European institutions have understood that it is relevant in some fields to consult prior to any decisions or adoption of directives. In these cases the slowness of local processes begs for something different than the law to deal efficiently with making sure that the great principles of our European countries are respected.

At a time when ethical differences between countries will increase, the new co-regulation governance model gives Europe a chance to elaborate legitimate and efficient rules and therefore to defend our values in the world.

The Role of Industry in Internet Development in Latvia

Viesturs Pless and Ina Gudele

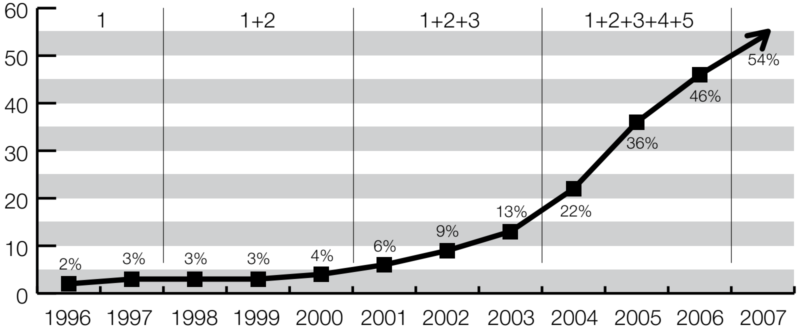
Introduction

The Internet in Latvia has enjoyed rapid development, setting an example for countries undergoing market liberalization and growth processes, and showing how a single telecommunications service can impact the economic development of the whole country. Undergoing various phases of development and affected by different factors, the Internet has changed from a system to transmit data allowing for academic communication into a catalyst of economic growth, and a crucial factor contributing to the development of the Information Society. With the access technologies developing from a 36.6 kb/s to broadband connections of 100 Mb/s and more, the Internet has been playing a major role in the country's growth. Internet communication now benefits all areas of life, from business processes to school and university studies and public administration, allowing for data exchange between the various groups of society, and optimizing the associated processes.

Internet access for all companies and households is not just part of a long-term national development plan, but a "must" to be achieved in the forthcoming years, making the most of the environment, which is so favourable to Internet growth in Latvia. The Internet is variously referred to as a means of communication, mass media and a service. In my opinion it possesses all of these features and these three factors all have an impact on each other as well as on the Internet as a whole, facilitating an irreversible change in Latvia's society. The factors which have so far influenced

Internet development will have to be retained at the present level to meet the ambitious plans regarding the development of the Information and Knowledge Society, where the Internet plays a crucial role in all its functions – as a means of communication, mass media and a service channel. During a five-year period, the Internet has changed from a 6 per cent "nerd" environment into an everyday necessity for 54 per cent of Latvia's population, a role which it will retain for good. The Internet is now being used widely by all generations, from senior citizens to young people, and it is now hard to imagine a time with no Internet. The following diagram traces this development.

Organizations input into the increase in regular Internet users



1. ISP 2. Content providers 3. Other companies 4. Non government institutions 5. Government institutions

Birth of the Internet

August of 1991, the time of the Communist putsch, was the first time the Internet was used in Latvia not just for academic needs (which used to be the primary reason for Internet usage). There was a real need to tell the world what was going on in Latvia at that time so it also served the country's political needs. The University of Latvia's Internet connection, supported by the Nordic countries and connecting the Baltic and Scandinavian States was used to brief Western news agencies of the attempted coup in Latvia. This was important as access had been blocked to voice and data transmission channels, linking the country with Russia and representing the only official international access to information from overseas. At this time the country not only regained its political independence, but also started using the Internet for information purposes. At this time the advantages of the new technologies were revealed in full to society, also marking the beginning of the Internet era, which since then has enjoyed rapid and irreversible growth, covering all areas of life – from public administration to economy and information. We could even go as far as to say that the Internet has contributed greatly to retaining Latvia's independence and brave spirit. For a couple of days this University of Latvia's Internet connection stood for the only information link with the world. Those days mark the real birth of the Internet in Latvia. The Internet had a great impact on the development of the whole country and its return to Europe.

The Internet in Latvia has developed in several phases and progress was driven by various technical, economic, political and public factors. In this respect various groups in society had an impact in a direct and indirect way on Internet development. Latvia is an outstanding example of Internet development not only in Europe, but also in other parts of the world, especially countries enjoying rapid development.

By late 1999, there were several local and international ISPs that provided their services, either using the fixed network of the telecommunications operator Lattelekom (in 2006 renamed Lattelecom), or launching wireless solutions as alternative means of data transmission. Until 2000, monopoly of the telecommunications network in Latvia was held by the company Lattelecom. Given the fact that the monopoly rights only related to the fixed telecommunications and voice transmission network services, at least seven ISPs in Latvia had emerged by 1996 that provided dial-up and permanent Internet access, covering the capital city Riga and other major cities in the country. There were also a few international connections to the global network, the largest of which was the Lattelecom-owned submarine fibre optic cable. The other ISPs rented the network infrastructure from Lattelecom, which greatly increased the price of Internet services, both dial-up and permanent connections.

By 1996, the telecommunications network infrastructure had undergone rapid development, with the analogue network upgraded to a digital network. The fibre optic connections provided Internet access for nearly all regional centres, thereby ensuring quality permanent connections tailored to corporate needs. By contrast rural areas were only provided access to dial-up services, most of which were of low quality as the distribution networks had only been digitalized by 50 per cent. The Internet was used by companies dealing with information technologies or exports as well as companies co-operating with international partners or investors. In the majority of cases, the Internet represented a mandatory prerequisite imposed upon local companies by investors and international partners rather than a business need. The Internet was also used by banks that saw the benefits they could reap in terms of high potential customer care and service. The Internet was not popular and was very rarely used by companies with local capital, small and medium companies, and residents.

As late as 1996, the Internet was used by about two per cent of the country's population. Though the telecommunications market in Latvia was regulated by a public body – the Public Utilities Commission (hereafter: the Regulator) – the charge for telecommunications services was still very high and Internet services, both dial-up and permanent connections, were not accessible to all. This market situation made existing ISPs look for alternative ways of providing lower priced Internet connections to companies. Some of the ISPs launched wireless services, thereby providing an alternative to the existing high quality permanent connections. This undoubtedly added to the number of Internet users, yet the low quality of connections did not convince company management that the Internet could benefit business. For this reason, the Internet was primarily used for e-mail rather than to facilitate the development of customer-tailored services.

The Internet was mostly regarded as something exclusive both by businesses, especially small and medium enterprises, and residents. This was enhanced by the fact that there were not many PCs in use as the price of computers was very high compared with the average person's income. Despite this, the number of Internet users kept on increasing by 10 to 15 per cent a year, and the development of services was primarily driven by customer demand. It was not the ISPs developing the market and launching new customer services and service connections, but customers demanding that specific services meet their needs, as they were not yet fully aware of the Internet's benefits.

Apollo Phenomenon

Early in 1997, the telecommunications network operator Lattelecom, following the upgrade of the analogue network to a digital network and the increase in the number of international connections, launched a variety of data services. These soon became a real necessity in view of the rapid growth of entrepreneurship and high number of international business transactions. At that time Latvia could already boast a well-developed fibre optic network infrastructure, interlinking the regional cities, as well as two international connections. As a result Lattelecom could launch both dial-up and permanent access Internet services. 1997 is now referred to as the beginning of the Internet boom in Latvia. The boom was facilitated by bundling the Internet with telecommunications services, where such service packages were available at a lower price than the existing services. It was also encouraged by laying the main focus on Internet benefits and content development rather than on connections. For the general public the Lattelecom dial-up connection provided access to e-mail and content services, the latter being something new and still unknown at that time.

One of the main hindrances to content development in Latvia is the low number of Latvian speakers, both at home and overseas, where only half of the population (currently 2.3 million) speak Latvian on a daily basis. The other half of the country's population speaks Russian and has access to a whole variety of content services in Russian language, originating in Russia and other Russian-speaking countries. Being aware of the situation, the ISPs worked hard to develop various portals, which, in turn, facilitated the activities of Internet users in developing their homepages, portals, blogs, etc. Despite this, the low number of customers makes the development of commercial content economically unviable, which is also one of the main reasons why content development is regarded as a sideline by existing ISPs.

New Internet services promoted the use of marketing elements in the local service market, which until then was regarded as something technical and "customer unfriendly". To enhance the existing image of a company holding a monopoly on voice transmission and fixed network services, Lattelecom drew up a new service development strategy, and introduced a completely new brand name for Internet services – Apollo. The new ISP Apollo commenced its business in an area where there was a high level of competition among the existing ISPs that used both the Lattelecom infrastructure and alternative service solutions allowing for global access. International capacity represented the biggest issue for all ISPs, where connections to global ISP networks were very expensive in terms of providing both network connections and international data billing. With commencing wholesale Internet capacity, Lattelecom introduced a new customer service targeted at the other ISPs. This allowed them to provide low price quality connections for their customers to the global network. The Internet boom in Latvia coincided with rapid technology development throughout the world, which resulted in the introduction of a new dial-up modem (data transfer of up to 56.6 kb/s), which was a big achievement in 1997.

Viewing the market situation in Latvia, many experts in 1997 did not believe that the new ISPs had major potential for growth, regardless of the fact that the Internet could be bundled with other telecommunications services. Despite these rather gloomy forecasts, the entry of *Apollo* on the market promoted the development of its competitors. Inspired by the *Apollo* example, other ISPs started using various marketing elements to advise customers about Internet benefits, to help them acquire basic Internet skills through training and launching free-of-charge customer helpline services. Being part of a large company, *Apollo* was thereby placed in a position to offer a completely new approach to customer services. *Apollo* was the first ISP in Latvia to give up international traffic billing by introducing permanent customer connections available for a fixed monthly subscription, which was especially beneficial to large companies. Many of the services introduced by *Apollo*, such as combined billing for calls and Internet, customer helpline services and various marketing and promotional activities, had a big impact on competitors. For the first time ever, the Internet was popularized, covering a large audience, and, secondly, the new customer care methods inspired existing ISPs to re-evaluate their business and make it more efficient, active and customer-oriented.

International capacity increase and the installation of fibre optic connections, interlinking regional cities, facilitated the development of regional ISPs. These regional ISPs covered a single city, or the whole region, and contributed greatly to regional Internet competency. They introduced a new business of residential Internet access and PC maintenance service, which until then had not been very popular, especially in small regional cities and towns.

At the same time, issues concerning installation of international connections and telecommunications service tariffs were dealt with separately by ISPs.

There was still one major obstacle to a countrywide Internet development – the low PC usage by small and medium enterprises (SME), which constituted the vast majority of companies in Latvia, and the residents. Internet development at that time was also greatly facilitated by banks and other financial institutions that were fully aware of the country's economic situation, and knew that residents' credit worthiness was not sufficient to buy PCs. For this reason, the banks and ISPs introduced several credit lines and leasing services, focused on the target audience, also including solutions targeted at teachers, thereby allowing for hire purchase of PCs and Internet connections. In just one year, service packages such as "Apollo PC", or the competitor's service "Navigators", meant that over 2,000 users could obtain a PC and Internet connection on leasing terms. In view of the country's total population of 2.3 million this was a very high percentage. Leasing services were especially popular among SMEs and residents. In addition, various types of accounting, CRM and software solutions were introduced, primarily targeting the SME sector, and allowed the Internet to be used to enhance co-operation between customers and suppliers.

This was also the time when Internet content developed rapidly with several companies, especially those representing the IT sector, launching a variety of Internet services. The banks, in turn, focused on developing various Internet banking solutions and in this way contributed greatly to the number of Internet users in the SME segment. These new banking services provided great savings in time and money, while banks could also enhance their productivity and lower labour costs. Banks have also facilitated large investments to install public Internet terminals throughout their branches. Such action ensured higher PC availability, allowing customers to access Internet banking services and e-mail. Several of the portals provided access to public e-mail services, where the users were allocated unique Internet logging names and passwords. TV, radio and printed media displayed various promotional materials and ads with information about the Internet and associated services, and the benefits offered by new technologies. The development also affected schools and a new subject Information Science was introduced, which included acquiring Internet literacy skills with Web pages being designed by both children and (indirectly) by their parents. Internet literacy was regarded as one of the main criteria when recruiting staff, too.

With the ISPs, telecommunications operators, banks and financial institutions joining forces and attracting various marketing elements and promoting content development, the annual increase of Internet sales reached between 30 and 50 per cent. The ages of Internet users became more varied, covering ages 15 to 60 and more.

The Involvement of Non-governmental Organizations

Starting in 1998, ISPs discussed the idea of setting up a non-governmental organization that would represent their interests when dealing with public bodies and be a central body to tackle industry issues like popularizing the Internet, increasing public awareness of Internet usage, Internet ethics and data security. These issues featured on the "to do" list of nearly all ISPs and called for a combined solution, which ISPs could not possibly tackle alone, as such action required significant labour and financial resources. Likewise, ISPs were still having major problems with international Internet traffic and how it was used within the boundaries of a single country, as well as the interconnect agreements concluded between the various ISPs to allow for quality exchange of local traffic. It was not an easy job to reach an agreement in this regard, especially in view of the high competition where the existing ISPs were practically fighting for each customer. In many cases this competition hindered co-operation between the ISPs, as they treated each other as competitors rather than potential business partners. They fought for the customer with all possible means, without giving a thought about possible market segmentation, and trying to cover as many Internet market niches as possible.

The number of market stakeholders in Latvia has been rather high since the very start. Where it was not viable to interlink existing ISPs to allow for exchange of traffic between them, a single point for local traffic exchange was set up within the premises of one of the leading ISPs. This point, however, was not a good enough solution to meet the growing needs of Internet users, which was why another local traffic exchange point was set up by seven leading ISPs, linking it with the first point and thereby preparing the ground for setting up a public body. It was only early in 2000 that an agreement concerning setting up a non-governmental body – the Latvian Internet Association (LIA) – was finally reached by 25 leading ISPs, Internet content providers and consulting companies engaged in Internet business. By then, there were about 43 ISPs, operating at national and regional levels. Work on liberalization of the telecommunications market had already started. This led to the need to set up a body that would represent the ISPs' interests when communicating with public bodies, developing a self-regulatory system embracing all ISPs, and participating in the law-making processes to resolve issues like spam, data security, user training, and child pornography.

The Latvian Internet Association incorporated various ISPs, content providers, portal providers, consulting companies and Internet software developers. At the same time as the LIA, the Information and Communications Technology Association (LIKTA) was also set up in Latvia. In general, LIKTA operations were quite successful, yet it failed in tackling specific issues concerning Internet development. The LIA liaised between the various ISPs, resolving the technical issues they faced and developing a common infrastructure. In this way it contributed considerably to the overall quality of Internet services and connections in Latvia and mediated among the ISPs and their customers (both existing and potential). In addition, the LIA also facilitated a dialogue with public bodies to allow for an environment most favourable to entrepreneurship and to resolve the various legal issues.

Until 2000, the Internet was generally believed to be a virtual environment, operating according to specific self-regulated rules and not needing any other administration whatsoever. With the development of e-commerce and the Internet's downsides, such as pornography, copyright infringement, and all kinds of intolerance, there were more and more public discussions about imposing some Internet regulations. The LIA started to tackle these issues and liaise between the various ISPs, public bodies and society. The rapid growth in user numbers led to a need for more active public discussions concerning Internet user ethics, and to advise society about these issues, focusing especially on children. The LIA, together with the mass media, advised the public on various issues, and publications on Internet services, Internet threats, user education, seminars and round-table talks focusing on various groups in society became a routine task for the LIA. With international activities gaining momentum and becoming more active, the LIA also joined various international projects (with European, or CIS countries participating), focusing on copyright protection, child and data security and a secure Internet environment.

Measures to upgrade the quality of the Internet and provide higher service availability (following the DSL "success story", the service is now available to 90 per cent of households in Latvia) contributed to a situation where the Internet was regarded as a basic necessity in business, education and the work of state and local government bodies rather than the domain of the chosen few. LIA activities inspired the other non-governmental associations to make the most of the Internet, treating it as a highly efficient tool allowing for e-democracy development and fast information exchange, as well as popularizing it and educating the public in this regard. There are a range of public portals in Latvia dealing with democracy and social issues, as well as various discussion forums concerning state administration and other issues of vital importance to society. This enhances communication between government bodies and various groups in society. To allow for higher public participation in these processes society needed adequate PC literacy training. It should also be noted that the vast majority of the population, aged 45 and over, had no PC literacy skills. This applies especially to the retired, who, more often than not, were more involved than working people.

One of the most successful projects initiated and supported by a non-governmental body, is the “Latvija@world” project, which provided training in basic PC literacy skills for various groups of society. The project was primarily aimed at senior citizens, who had never had the chance to obtain these skills. By training regional coaches, and using the Internet access infrastructure available at public libraries and various PC training facilities, PC literacy training was made available close to home to many people. The greatest interest in the project was shown by senior citizens, with some students aged between 81 and 87 attending the course. At the same time as implementing the project, the infrastructure of public Internet access points was also developed, supported by both the State and local governments, which allowed people to practise their newly acquired skills by using Internet banking and various e-services launched by public or commercial bodies. This has also led to the spread of various Internet blogs, which are most popular among senior citizens.

Non-governmental bodies play an important role in drawing up laws to regulate and monitor the Internet and the representatives of these bodies are very often involved in the work of various working groups preparing regulations. Currently, LIA specialists, in association with the relevant public bodies, are working on a number of legislative issues focused on Internet development, such as data reuse, protection of children’s rights and copyright protection, combating computer piracy and the development of electronic services. There is not one regulation in Latvia that has not been publicly discussed and agreed with by various non-governmental bodies. The Internet is used as a means of communication allowing for such discussion and to follow up on the daily work and agenda of the Cabinet of Ministers and the Latvian Parliament (the Saeima) and discuss these processes publicly. The non-governmental bodies have greatly contributed to the development of e-processes in Latvia, where the State has provided both the infrastructure and access to information allowing for public participation in these processes.

Co-participation of Public Bodies

From the middle of 2003 – when the Information Society Bureau (ISB) was set up reporting directly to the Prime Minister – state participation in Internet development processes became even more active. The first signs of such participation were recorded much earlier and coincided with the launch of the first state and local government IT projects and the e-Government programme. The Information Society Bureau drew up a strategy for developing the Information Society in Latvia, laying the main focus on the Internet and content development. The first state administration IT projects were launched back in 1998 when the first electronic registers and state central register system were set up. To allow for centralized IT use in state administration, a group of local scientists and IT specialists drew up an “Information Science” programme that was based on the EU programme “e-Europe”, and recorded the main objectives and tasks with respect to Information Society development in Latvia. At the same time, a school IT project “LIIS” was also launched in 1997. This provided for combined use of IT and the Internet at schools and set up special PC classes and centralized information systems to train teachers and provide permanent Internet access throughout the country. In addition to these projects, a uniform local government information system was also introduced to facilitate the development of local government services and availability of these services to the public, and allow for exchange of data between the various local governments and central data registers. And last but not least, the State Unified Library Information Network (SULIN) *Network of Light* was launched, which installed permanent public Internet access points, interlinking public libraries throughout the country (state, local government and school libraries). The project is due to be completed shortly. Public Internet access points have already been set up in 870 libraries, thus allowing people to access all kinds of information, e-mail and various state and local government e-services.

Facilitated by the above programmes and projects, the Internet was made available all over the country, be it a school, library, local government or public body. By late 2006, broadband Internet was made available to all schools in Latvia; public Internet access points had been installed in all of the country's public libraries and all local governments had provided permanent Internet access. In 2005 the "e-Government Development Programme" was drawn up and approved by the Cabinet of Minister's decision. The programme aimed to optimize communication between the public and local government bodies and society, providing for a favourable environment for entrepreneurship and eliminating existing administrative obstacles. The "e-Government Development Programme" set several objectives, such as interlinking all central registers to a uniform system, thereby allowing for e-service delivery. For this, various channels are used like portals, one-stop agencies, operator centres, digital TV and others. Furthering infrastructure development, the "Broadband Internet Development Programme" was also introduced. Yet all this action has not resolved the last mile problem. This still exists in the country in spite of the wide availability of fibre optic connections, which in 2000 were laid throughout the country, interlinking all cities. The main cause of the last mile problem is a situation where many people still live in farms, especially in rural areas, which is why broadband Internet access will remain an issue for the next few years.

In 2004, the position of Special Assignments Minister for Electronic Government Affairs was established. This role was to contribute to making quality state and local government services available, and to use the benefits of new technologies to their best advantage to meet the targets and objectives of the above-mentioned programmes and projects. This minister was made accountable for the Information Society development processes and launch of e-Government, excluding the telecommunications infrastructure (including broadband Internet), which was the responsibility of the Ministry of Transport. Co-ordination of the relevant activities meant that a more sustainable and efficient development of e-processes, such as e-Health, e-Education, e-Welfare and e-Government could be furthered, using existing administrative and financial resources to their best advantage.

In 2006, the e-Signature was launched which holds legal power according to the laws of Latvia and this promoted the use of the Internet in everyday life. Many of the companies introduced new Internet services, significantly increasing the number of their customers, while the customers could save time and money. The e-Signature gave the green light to the development of many state and local government services, which called for user ID data to be verified. In a situation where there was no clarity as to whether to proceed with e-Signature development, or to stop using e-Signature in view of the limited number of such e-services, the State came forward with a suggestion. It proposed using the e-Signature for state and local government officials which would allow for the development of the most crucial public e-services. If the e-Signature is used by state officials this will reduce and later eliminate public concern, which is inevitable in a situation when something new and unknown is introduced.

Through introducing various programmes, the State is successfully tackling infrastructure development and public education issues. The programmes are either financed by the State or local governments, or supported by various European structural funds or private investors (public-private partnership). This is all contributing a great deal to Internet development and availability of stakeholder services for the whole of society. I would say that at this stage Internet connection alone does not mean a lot – it is the services that are made available using this connection that matter.

With the public and non-governmental bodies participating in Internet development processes, the number of Internet users kept on increasing by on average 70 per cent a year, reaching 52 per cent of the total population in 2006. It is also interesting to note that the age distribution of Internet users kept on increasing, too, from age 6 up to 75. Based on the survey, conducted jointly by the LIA and public bodies, 90 per cent of children aged up to 12 use the Internet regularly, and claim that it is their main means of communication.

Partnership between existing ISPs and other companies, also including participation of public and non-governmental bodies, has created a situation where during a ten-year period from 1997 to 2007, Latvia has transformed from a country with rather low Internet literacy into enjoying one of the fastest service growth numbers in the world. Growth at 70 per cent a year sets an example of how to achieve industry boom through combining the efforts, skills and know-how of various stakeholders.

Future Prospects

In the world of the Internet, like anywhere else, much attention is focused on future prospects. Are there any limits to Internet development, and will it go on forever? How can we tell if we are in a situation where the speed of Internet development is no longer crucial, and how can we measure Internet saturation? The situation is similar to mobile telecommunications, the only difference being that the mobile communication field underwent a worldwide revolution earlier than the Internet and was less costly. This difference can be eliminated by substantially lowering the price of computers, in which case Internet development would be analogous with that of mobile communications. Based on the latest statistics, mobile saturation in the leading European countries is higher than the population number, meaning that the same person can have several phones for various needs (at home, in the office etc.). The situation is slightly different regarding the Internet –

broadband and wireless Internet technologies mean that a single connection can meet the various needs of the whole household.

The analysis of Internet development in Latvia, which has gone through several stages and was facilitated by various stakeholders and groups in society, allows us to draw certain conclusions, such as:

Internet growth in Latvia has been largely impacted by the development of the telecommunications infrastructure. A country where the development of the telecommunications infrastructure is hindered by the geographic or economic situation cannot possibly enjoy a sudden Internet boost. Several attempts have been made so far to develop highly efficient satellite connections for both the Internet and communication services, but they all failed due to the high cost. This issue can be resolved by minimizing the cost of such satellite solutions. People's solvency is yet another factor impacting the process and calls for a separate analysis. The general tendency is that the larger the number of people that are solvent, the faster the growth of Internet user numbers.

The educational level and digital literacy of people also have a significant impact on the growth of Internet user numbers, but this issue is easier to deal with than upgrading the telecommunications infrastructure or enhancing the country's economy. Latvia is a good example of how the number of Internet users and ISP development can be influenced directly by implementing appropriate state policies, contributing to a higher level of education, more efficient work by companies and non-governmental bodies, a higher demand for Internet services and development of new services.

The level of education can and does have an effect on the capability of people to use new technologies. It indicates whether people are aware of the various benefits offered by the new technologies and are ready, willing and able to use these to their advantage. The world's experience has shown that some Internet development projects where this factor was not taken into account have fallen flat. In Latvia, where senior citizens are rather unwilling to use PCs, we have to focus efforts on showing how easy it is and that these skills can be obtained by anyone. For this reason, much attention needs to be focused on increasing public awareness and digital literacy, where all stakeholders – the State, commercial companies and ISPs – should combine their efforts in achieving a common goal.

Internet development is also facilitated by various commercial enterprises which use the Internet in daily communication with their customers, such as finance institutions, mass media, sales and manufacturing companies. By using the Internet to provide various customer-tailored services, these companies also contribute to the higher demand for new services and play a part in the overall Internet growth. This is a self-perpetuating process – business is driven by service development and this in turn contributes to high customer interest and demand. The State should provide for two things – an environment that is favourable to business and overall infrastructure development. The rest will be done by companies appropriate to market needs, and in this respect the launch of the e-Signature will be a great contribution.

The role of non-governmental and professional organizations in facilitating the country's growth keeps increasing. The same applies to the impact of the Internet on society, where the Internet is regarded as an environment allowing for public action and opinion. For this reason, special rules of conduct and operation need to be drawn up, regulating this area and providing for security and maximum comfort to all its users. The Internet should not be treated as something where everything is possible and allowed. It also shouldn't condone actions that encourage anarchy or chaos, and this message should be made very clear and conveyed to all. The various groups of society should join forces to provide an Internet environment that is free of all those things we are combating in real life, such as racism, hostility, terrorism, child abuse, etc.

In order to avoid a situation where public bodies interfere too much in regulating the Internet environment, there should be well-developed and close co-operation between the stakeholders and high trust in public and non-governmental bodies. By facilitating co-operation between the various groups of society, we will achieve better and more efficient results in developing the Internet. The Latvian Internet Association has initiated the most efficient way of co-operation between the various ISPs, harmonizing their operation, enhancing partnership and eliminating unhealthy competition, as well as facilitating the use of promotional tools allowing for overall growth. The LIA has also managed to find the best way of co-operating with public bodies, which is no less important than co-operation between the various ISPs, as the State can both promote and hinder business. This includes LIA participation in law-making processes, which avoids the risk of specific companies lobbying their own interests and abides by general principles of sustainable development.

A User Perspective on Spam and Phishing

Jon Thorhallsson

Introduction

In this paper, Internet Governance is examined from the user perspective. The analysis is based on the Internet Governance definition by the United Nations Working Group on Internet Governance from 2006. The word user is used synonymously with civil society and consumer.

The paper analyses user needs and concludes that there are two key issues in Internet Governance as far as the user is concerned: ease of use and safe to use. The user market is heterogeneous and can roughly be divided into one market for technology-confident people and another market for technology-challenged people. The industry has focused on the technology-confident market and neglected the technology-challenged one. The latter is a huge virgin market of over 200 million people in the EU's 25 countries alone. These people look at the Internet as a tool for communication among themselves and their families and increasingly for online services like online banking and shopping. For this they need a safe, maintenance free, turnkey "Internet machine". The paper concludes that the present offering is far from being such a machine. It is neither easy to use nor safe to use the Internet. Besides technical issues many legal issues need to be addressed.

The article also highlights the role of the media reporting security incidents to raise awareness among users and also politicians and the industry. In addition it analyses the two most prominent user threats of spam and phishing from various points of view. These constitute a serious threat to the future of the Internet. Without users the Internet is nothing and users who get burned leave and their friends hold back. The legal situation regarding compensation is very confused and can only cause fear and uncertainty among the users. There are also technical questions about software and service providers. Are they doing everything they can to provide a safe Internet?

Some comparison is made between the USA and EU situations, both in legislation and law enforcement, with the USA being the forerunner in legislation and also tougher on enforcement. It is assumed that the situation in other countries in the OSCE region is similar or soon will be. The transitional countries will in a few years face the same situation as the technically advanced countries are facing today.

The industry, ICT hardware and software companies and IT service providers are urged to enter this market with innovative solutions. The report also calls on the stakeholders, governments, industry and civil society to work together to solve those issues and indicates respective roles and responsibilities, also of the OSCE.

What is Internet Governance?

Governance means "act, fact, manner of governing".[211] Therefore, Internet Governance means the act, fact, manner of governing the Internet. This is a very broad definition and after much deliberation and reflection the United Nations Working Group on Internet Governance 2006 came up with the following definition:

> "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."[212]

[211] *Oxford Advanced Learner's Dictionary of Current English* (Oxford University Press, 1974).

[212] Working Group on Internet Governance <www.wgig.org>.

This is still a very broad definition and allows many interpretations depending on the position and priorities of the person looking at it. But it identifies three main stakeholders: governments, civil society and private sector. Let us see the relationship between the stakeholders as a triangle where the stakeholders have their own corner. Each corner has a relationship with the two other corners and together they make up the sides of the triangle. The area of the triangle is the scope and content of Internet Governance.

None of the stakeholders can do it on their own. It is only if civil society, the private sector and governments work together and support each other that effective Internet Governance can emerge. But what exactly does working together mean? Who gets what? Who gives what? In this paper we are going to focus on civil society or the user and look at Internet Governance from the user perspective.

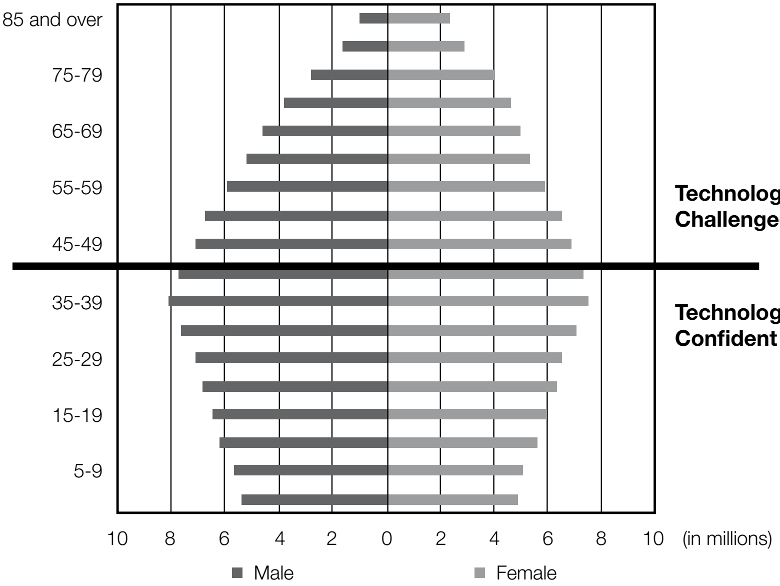
Unfortunately, the body of research on user needs is very limited. All too often this is seen purely as a marketing issue. It is only recently that people have started to question the motto that “the market knows best”. But before we proceed, let us consider who we mean by civil society or “the users”.

Who are the Users?

For the moment we will limit our discussion to the European Union of 25 States. According to EUROSTAT in 2006 there were 463 million people in the EU.[213]

[213] <http://epp.eurostat.ec.europa.eu>.

EU-25 population



There are approximately the same number of males and females. What is most interesting for our discussion is the age distribution: approximately half is under 40 and the other half is over 40. This is a very important issue because user needs are age dependent.

Those who are 40 years and younger had the advantage of growing up in the information society with computers in schools and homes. They feel confident about technology. The situation is different for those over 40. They did not have the privilege of growing up in the information society and had to join it the hard way and under their own steam. Many or even most of them feel technology-challenged, although this is of course a generalization. Somehow the "over 40s" have been forgotten. The industry has focused its marketing efforts on the "young", technology-confident group under 40 years of age. The industry does not seem to understand that the market is not homogeneous but heterogeneous. It is interesting to consider why the needs of “older people” have been neglected.

Technology-challenged?

The “over 40s” make up a total of 230 million people in the EU 25 alone. 115 million males and 115 million females is a huge market. This could amount to a half to one billion people in the OSCE region. And many of these people are well off. So why is the industry neglecting these people? There has been virtually no research on this subject, something which needs to be remedied. The following discussion is based on the limited research done by the Confederation of European Computer User Associations (CECUA) and the CECUA Academy. They take a practical approach because to most users the Internet is not an abstract space with its own language, law and jurisdiction. In this research, two key issues have emerged: ease of use and safe to use.

What do we mean by ease of use?

When we talk about ease of use we think of something like a TV remote control, toaster or automatic transmission for a car. You push a button and get your favourite TV station, you put the bread in and the toast pops up when it is ready, and in the car you no longer have to shift the gears.

The users see the Internet as a tool for communication with friends and family and for getting information. Many also use it for e-banking and e-shopping. Ideally they envisage an “Internet machine”, which is as easy to switch on as the TV, pops up when ready like the toaster and has no clutch and gears. Are they getting this today?

Let us go through a scenario involving a technology-challenged person buying an “Internet machine”. The person goes to a computer store and buys a personal computer. The vast majority of PCs run the Windows operating system and Internet Explorer browser. For the sake of simplicity we will assume the person uses Webmail. Let us also assume that the software was preinstalled. At the store they will have been informed of the dangers of “attacks” from viruses or worms and they will also have preinstalled firewall and anti-virus/malware software.

Let us assume that by now the person has secured an Internet hook-up from some supplier. The person comes home and plugs the “Internet machine” into the power and Internet sockets. He or she expects this to be like the TV remote and pop-up toaster with a screen popping up saying “ready and what do you want?” In all likelihood something is wrong and after tearing their hair out and finally calling the store for help the person is ready to send the first e-mail or search the Web. Finally everything works and the person starts enjoying the wonders of the Internet.

But paradise may soon be over. Soon our technology-challenged person starts to get e-mails with information that there are updates for the software ready to be downloaded. Does the person want to download or not? If the person says “yes” he or she has to go through some “acrobatics” to install the update. Many people think: “I just bought the ‘Internet machine’, why should I need an update?” And they say “no”. Sooner or later they will start to get messages that their protection is out of date and they have left themselves open to attacks. If they suddenly change their mind they have go through installation “acrobatics” more complicated than the updating one. This is too much for a technology-challenged person.

But this is not all. Soon they will start to get invoices by e-mail advising them that the software subscription is just about to expire and asking them for money for updates and new and improved products. And they say: “I bought the ‘Internet machine’ and now they want more money from me?” This is going too far and they say “no”. And they are indeed open to attacks. To do all of this they are expected to become some sort of system administrator.

And that is definitely too much to expect from a technology-challenged person.

This is not what the user expected. The TV remote control and the toaster do not need updates. Why should it be different with the “Internet machine”? The Internet industry owes us an answer to this and this should be a reply understandable to those who see no difference between the “Internet machine” and the TV remote control and the pop-up toaster.

In summary here is a tremendous business opportunity for the industry and service providers, an opportunity where they have failed. Although I have used the EU of 25 as a background, I am sure the conclusions also apply to the other countries in the OSCE region.

What users need is a maintenance free, turnkey “Internet machine”. Industry and users must co-operate. Here is a huge virgin market for hardware and software makers and service providers. A comparable example is the famous French “Minitel machine” which had 6 million users in France alone and was a tremendous success. We need a successor. The ball is in the industry and service provider court.

Safe Use

The other thing that users need is safe use. Even if they update their software regularly, either themselves or by bought assistance, they are by no means safe. All kinds of threats lie in wait for them like spam, phishing or identity thefts. Almost every day the media report on people being swindled out of their savings by Internet bandits. It goes without saying that this hardly encourages people to do their business on the Web. While governments and industry seem to play down this issue, the media are playing an important role by informing the public about the real situation even if it is very bad for the image of the Internet.

In the absence of research results I am making extensive use of the CECUA media database. We will look at some examples and experiences that have been reported in the media.

Spam

Spam means that users get all kinds of unwanted e-mails. There is a certain analogy between spam and the paper advertising materials most households receive in their mailbox. The constant stream of offerings for “Viagra” and other drugs, replica watches and the like is tiresome. The CECUA database is full of stories about it. Some spammers seem to do it for fun, others to make money out of innocent people. They are playing the numbers game: just send a large enough amount of spam mail and you will find enough victims to make money out of. They send millions of spam mails and only a small percentage of responses is needed to make it “good” business.

Here is an example where the perpetrator was actually caught and brought to justice. A Dutch spammer was fined 75,000 euros for sending at least 9 billion spam e-mails. The man used spam e-mails to advertise pornography, erection pills, sex articles and similar things and made at least 40,000 euros profit.[214] This is the biggest fine a spammer has ever received in the Netherlands. Sending spam e-mails has been forbidden in the EU for two years. Whoever sends advertising materials by mail, fax or SMS first has to ask recipients if they want to receive these materials and they are not allowed to hide their own identities.

This is the so-called “opt in” approach as adopted by the EU. The USA has adopted the opposite, or “opt out”, approach. These various approaches regarding spam adopted by different countries in the OSCE region are causing a lot of confusion, including questions about implementation in practice.

[214] “Dutch spammer is fined 75,000 Euro”, *Focus online*, 2 February 2007.

The industry is trying to help by offering so-called spam filters, computer programs that go through e-mails and “identify” spam mails. These filters are good but not fail-safe. Some important e-mails may get lost because the filter identified them as spam mails and deleted them.

But spam can turn nasty. The spammers are continuously thinking of new ways to “squeeze” their victims. Their latest is the so-called Killer Spam: A new spam wave is scaring US citizens. E-mails threaten the receiver that he or she will be killed unless they pay a large amount of money and the sender gives the name of “professional killer”.[215] It is one thing to receive an offer for Viagra or something like that and quite another to be sent a death threat. This would be a violation of the EU spam directive, firstly in sending it without approval by the receiver and secondly by hiding the sender’s identity. And the content is pure blackmail.

Where does all this spam come from? Most spam mails still come from the USA, but the security firm Sophos has reported that the USA portion is rapidly decreasing. In 2005, 26 per cent of spam came from the USA.[216] Countries with widespread broadband like South Korea and China are catching up with the USA, taking advantage of outdated Windows software.

Statistics are one thing, catching the perpetrators is another. Most reports on enforcement and punishment come from the USA. EU country cases are an exception. Although an isolated example, there is a report that the South Korean police arrested a man known on the Internet as “the Queen of Spam”.

The South Korean digital magazine *Chosun Ilbo* reports that from September to December 2006 alone the accused, a 21-year-old student, sent 1.6 billion

[215] “KILLER-SPAM – Pay or die!”, *Spiegel online*, 17 January 2007.

[216] “Broadband countries like South Korea and China catch up on spam-USA”, *Computerworld DK*, 14 October 2005.

spam e-mails and obtained personal information from 12,000 people. He sold this information for 82,000 euros. Although his success rate was only 12,000 out of 1.6 billion, he still made good money out of it. Playing the numbers game paid off for him.[217]

What about legal issues and punishment? Is the legal environment adequately prepared to deal with this kind of crime? While the USA claims successes, the EU is in trouble. The anti-spam law in the USA is showing a deterrent effect. Providers exchanging information in the fight against spam and the passing of the CAN-SPAM law in the USA have helped to reduce spamming there.[218] The tough prosecution of caught spammers in the USA seems to be showing effect. This is happening while the EU is having a hard time implementing the Spam Directive.

The EU Commission is urging Member States to take stronger action against spam, spy- and malware. It concluded that Europe still suffers from illegal online activities from EU Member States and third countries, in spite of spam being forbidden by EU Directive. This issue has been on the political agenda for a long time and governments should do more to get these activities under control.[219] The main stakeholders in this case are governments and industry.

Spam law needs to be harmonized, issues like "opt in" or "opt out" resolved, and generally adopted. But spam is not restricted to the USA or EU but is a global issue and has to be dealt with on a global scale. Until then the spammers will hide out in a place with lax spam law and ply their trade from there. This is an issue for the OSCE region and the OSCE could play an important role in this process. The industry can help by providing technology to filter out spam mails. But spam will not be solved by technology alone.

[217] "South Korean police arrested the 'the Queen of Spam'", *heise online*, 31 January 2007.

[218] "Anti spam law in the USA is showing effect", *heise online*, 12 October 2005.

[219] "The EU Commission urges the member states to take stronger action against spam", *heise online*, 27 November 2006.

Phishing or Identity Thefts

Phishing or identity stealing is another thing. The CECUA media database is full of stories about it. And these stories can be serious. While spam is mostly annoying, phishing can cause serious damage. Phishing is to trick users to reveal their passwords and other identification. Bank accounts and online shopping accounts are very popular phishing objects. Phishing is like tricking somebody into giving away the key to his or her home.

A MessageLabs analysis showed that in January 2007 attempt was made to solicit personal data in 1 of 93.3 e-mails (1.07%). The number of viruses was lower according to the Intelligence Report from the message security specialist firm. In January 0.87 per cent or 1 in 119.9 electronic mails was infested with malware.[220]

These numbers are astonishing. Out of every 100 e-mails, one e-mail is a phishing mail. Phishing has become "big" business and organized crime is probably involved. They focus on financial institutions like banks, targeting the bank's customers. This raises a lot of questions including bank liability. Who is responsible? Do customers sit on their losses or is the bank liable?

The Nordea Bank is reported to have shut down its online banking after a phishing attack. It has closed down its netbank and all its Internet services in Sweden after major attempt was made to trick information from customers by e-mail.[221] This all happened in late 2005. But the Nordea Bank was not out of the woods. They suffered another attack recently, this one from Russia. Russian hackers have stolen 800,000 euros from Nordea after a sophisticated phishing attack tricked some of its Internet customers into downloading a Trojan horse that recorded their account login details.

[220] "More phishing than Virus and Trojan attacks", *Computerwoche.de*, 31 January 2007.

[221] "Nordea Bank panics and shuts down Internet banking after phishing attack", *Computerworld DK*, 4 October 2005.

The first attack took place in August 2006 and was detected a month later. Around 250 of Nordea's customers have been hit by the attack to date. Hackers targeted the bank's customers with e-mails purporting to be from Nordea that told them to download an anti-spam tool. But those who downloaded the attachment were infected by the Trojan "haxdoor.ki". The malicious software activates itself when the customer tries to log on to Nordea's Internet banking service and displays an error message asking the customer to re-enter their login information, which is then recorded and sent to servers belonging to the hackers. Swedish police have traced the attacks to Russia, via servers in the US, and have arrested more than 100 middlemen in Sweden, the bank said. The bank compensated all the customers in full.[222]

This phishing attack is interesting in many ways. Firstly the size of it: one million US dollars. Secondly it was a multinational attack, from Russia via the USA with local help. This strongly suggests international organized crime. It is probable that only the middlemen will be punished and the others will go free.

Swedish authorities have at last reacted and started an investigation into net banking security. A survey showed that security is a key issue for more than half the people selecting a net bank. Seventy-five per cent of participants agreed to a more complicated security system, if it raises the security level.[223] These results show the paramount importance of safe Internet use as stated earlier.

But banks are not the only targets. Online auction houses are also a favourite target. For example, using a hacked password from the Internet auction house eBay an unknown person made more than one thousand

[222] "Hackers Nab $1 Million from Nordea Bank", *Business Week online*, 19 January 2007.
[223] "Nordea under pressure after phishing", *Computerworld DK*, 5 February 2007.

purchases in just one night. The hacker ordered merchandise valued at more than 400,000 euros using the name of a 67-year-old man from Iserlohn in Sauerland.[224]

German bank customers have also been targets. For example, a user of online banking one day discovered that 4,800 euros were missing from his account. Without his knowledge the money had been transferred to a woman. The bank informed the man that everything looked alright. The money had been transferred using his access codes. Realizing that this was a case of Internet fraud he immediately pressed charges. The police checked the customer's computer and found out that somebody had infested his computer with a program to pick up his bank access codes and transfer the money to their own account.[225]

In these incidents the perpetrators focused on the customer or the client side. There are also cases where they focused on the server side. A hacker was potentially able to access 40 million credit card numbers by infiltrating the network of a company that processed payment data for MasterCard International Inc. and other companies.[226] Small wonder then that users are afraid of losing their money. Maybe they thought that Internet banking was a bit risky but credit cards have been well established for a long time and are considered pretty safe. Can nothing be trusted any more?

I have reported on typical spam and phishing cases based on media reports. I have used reports from serious media only known for their professional journalism. This raises the question of whether these examples are isolated incidents?

[224] "eBay hacker makes purchases for 400,000 Euro", *Computerwoche.de*, 28 September 2005.
[225] "Online banking robbery", *FAZ.NET*, 4 December 2006.
[226] "Security breach may have exposed 40M credit cards", *Computerworld USA*, 17 June 2005.

The IT security company Integralis warns of serious security gaps in online shops. The company estimates that more than half of all e-business platforms are open to attacks. According to Integralis about 20 per cent have security gaps which mean that customer data can be read or manipulated. The most common reason for this is cost cutting pressure and lack of resources and knowledge according to the security specialist. Most web shop operators underestimate the threats they face, claims the e-commerce expert from Integralis.[227]

Therefore, the examples we reported here are not isolated incidents but reflect the situation as it is. And examples like this appear in the media almost every day. What effect is this having on the readers? The reports in the media are certainly not reassuring but are seriously damaging the image and potential of the Internet. There are reports on users' dwindling trust in the security of the Internet. These are the findings of two respected research companies in the USA, Gartner and Forrested. Gartner market researchers surveyed 5,000 adult US citizens and found that their confidence in online transactions is going down. They blame reports on credit card theft and more and more phishing.[228] This tallies with the results of the recent survey from Sweden. Security is a paramount issue for users.[229]

After having established that security is a paramount issue for users and also that the Internet faces massive security problems let us look at who is liable. This is a very complex issue and can be looked at from several points of view. We will start with the security experts' opinions. Security experts are discussing who is responsible for inadequate security. Some expressed the view that software producers and Internet providers should be made liable. Private persons must also look after their own PC security. Governments

[227] "Integralis warns of security gaps in Online shops", *Computerworld.de*, 27 September 2005.

[228] "USA citizens confidence in e-commerce is going down", *heise online*, 23 June 2005.

[229] "Factors that Would Persuade Internet Users in Europe to Start Using or Use More Online Banking, 2005", *BDM News*, Forrester Research, provided to Paul DiModica by eMarketer.com under contract, 3 October 2005.

should shoulder the responsibility of training users to make them competent to work with common user friendly and secure software. It is difficult to understand why software companies do not use the many available technical solutions to improve security. According to experts, the time has arrived to make the software companies responsible by law, for example by taking them to court. The same should be done with Internet service providers.[230]

That the industry is failing to provide the best available security is a very serious allegation. Why could they be doing that? Our research has not found any cases where users have taken software companies or service providers to court for offering products or services with inadequate security.

Legally it is unclear under what circumstances phishing victims are responsible for their own losses. The legal situation is continuously changing and the first court decisions are awaited. Accordingly there is a grey area where self-responsibility ends and bank and shop responsibility begins. This is an unacceptable situation for the users. Waiting for the courts could take a long time and while waiting, the users sit on their losses.

How are the banks and shops reacting? Are they compensating their customers or not? There are reports that in the past banks were co-operative and compensated their customers for their losses. However, in view of the growing volume of Internet criminality their attitude seems to be changing.[231] While the Nordea Bank very recently compensated its customers for their losses, German banks seem to be reluctant to do so. Of course we cannot make generalizations but a trend seems to be emerging. Again this is a totally unacceptable situation for the users.

Another issue is how the police have reacted to the growing volume of criminality on the Internet. The police in Germany have recorded growing

[230] “Discussion about who is liable for inadequate security?”, *Doppelklicker.de*, 24 October 2005.
[231] “The banks are not always co-operative”, *Focus online*, 23 October 2005.

criminality through e-commerce and in 2004 confirmed 114,000 e-commerce fraud cases in Germany alone. Compared to 2003, this is an increase by 45,000 criminal fraud cases. Forty-two per cent of all cases were related to fraudulent business on the Internet.[232] They estimated loss as a result of phishing at 4.5 million euros in Germany alone.[233]

The police confirm that the volume of Internet criminality is growing rapidly, that losses are mounting and that many cases will never be closed. Many legal issues seem to be unclear. Until these are clarified users are worried and hold back from making full use of the Internet.

The legal situation regarding phishing is also confusing. Take for example the state of California in the USA, which passed the country's first anti-phishing law, making this form of identity theft punishable by thousands of dollars in fines. Under the Anti-Phishing Act of 2005, victims may seek to recover either the cost of the damages they have suffered or 500,000 dollars, whichever is greater; government prosecutors can also seek penalties of up to 2,500 dollars per phishing violation.[234] California is one of the USA's trendsetting states. It will be interesting to see how successful California will be at containing phishing by applying this law. The EU and other countries would be well advised to look at the Californian example and experience and prepare their own anti-phishing acts.

The comments presented above have focused on two stakeholders: governments and industry. What about the users? What should they do? How can they work with the other stakeholders for a safer Internet?

[232] "The police confirms 114 thousand e-commerce fraud cases in Germany alone in 2004", *heise online*, 16 August 2005.

[233] "Theft of bank access codes results in loss of seven digit number of Euro in Germany alone", *Focus online*, 23 October 2005.

[234] "The state of California has passed the country's first antiphishing law, making this form of identity theft punishable by thousands of dollars in fines", *Computerworld USA*, 24 October 2005.

For example, studies show that awareness-raising about safe online trading is urgently needed. Occasional users in particular are not adequately informed about security. This is the result of a study commissioned by the online auction house eBay and conducted by TMS Infratest. It is mostly elementary knowledge that is lacking and as a result occasional users are more open to fraud, because they are not aware of security measures.[235]

For eBay, security is also a critical factor for its business success. In the virtual world there is no 100 per cent guarantee against criminal activities. Therefore eBay calls on its members to practice self-reliance. Stefan Gross-Sebeck, CEO of eBay German, was quoted as saying: “People must develop an Internet common sense”.[236]

Some national authorities are offering advice on their websites. That is also very good but is too far removed from the regular customer. He or she needs to be reached through the regular media and not have to comb through the maze of pages on a website to get to the advice. This has to be done through the media that people consume every day, i.e. TV and/or print media.

A final example comes from *Computerworld USA*. Unfortunately, *Computerworld* is a trade media, not something most people read over breakfast. US shoppers were expected to buy about 25 per cent of their holiday goods online in 2006, with a typical shopper spending nearly 800 dollars, according to the National Retail Federation. With that in mind, various vendors and consumer groups issued warnings to online shoppers because the increase of buying online is accompanied by an increase in the likelihood of fraud. According to the US Federal Trade Commission (FTC) Internet-related fraud cost an estimated 340 million dollars last year.

[235] “Awareness raising about safe online trading is urgently needed”, *heise online*, 8 November 2005.
[236] “For eBay security is a business critical success factor”, *heise online*, 24 November 2005.

The advice quoted in Computerworld stated that online shoppers should[237]:

- Know your retailer. Stick with reputable businesses with contact numbers and physical addresses. Some websites display seals that vouch for their security, but these can also be faked.
- Use secure websites. Sites that use encryption to protect data should display "https://" rather than "http://" in the address bar. Secure sites should also display a padlock symbol to show that the website has a secure, encrypted connection. EDS advises against sending a retailer more information than they need to complete a purchase.
- Be aware of phishing e-mail. Most people have received fraudulent e-mail asking for personal information. Never send information and never click on links in such e-mails, which are likely to be directed to lookalike websites designed to harvest identity and financial details. Reputable businesses do not ask for information through e-mails. However, it's safe to type a website address into a browser.
- Review privacy and security policies. Most companies will tell you what information they collect and how they use it. Also, foreign websites may be bound by different laws concerning how they can handle your personal information.
- Use antivirus and firewall software.
- Check your credit report and credit card balances regularly.

This is indeed a fine example of advice. If this were presented on national television before the evening news it would get lots of attention and be very effective – something for the banks and the auction houses to think about.

Conclusions

Phishing in particular is a serious problem and a threat to the use and development of the Internet. Banking and online shopping are particularly

[237] "FTC offers guidelines to reduce online shopping risks", *Computerworld USA*, 21 November 2006.

in danger. Every week and sometimes every day users see reports in the media, reports of people being ripped off by Internet criminals and left with empty bank accounts. This makes some users drop Internet banking and online shopping altogether and those thinking about starting using those services hesitate and wait. Here is a problem all stakeholders have to work on together.

It is hard to believe that only one state, California, has passed an anti-phishing law. Admittedly California is a USA trendsetting state but others need to follow suit. Governments can learn from the California experience when they prepare a new law for their own jurisdiction. Phishing is much more dangerous than spam. And it calls for action now.

The industry has to provide better protection against phishing. Software producers have to apply the best available technology to their products and service providers also have to use all the technological means available to provide better protection for their customers.

But the users also have to accept a certain amount of responsibility for their own protection, similar to not leaving the door to the house unlocked when leaving home. The “Internet machine” has to have some minimum security installed, e.g. a virus protection program. Maybe no machine should be sold without such protection. User awareness has to be raised on this issue. There are various ways to do so and governments and the private sector should co-operate. The private sector has a lot at stake, particularly banks and online shops.

Legal issues, such as where does the responsibility of the user end, need to be clarified as well. When are net banks and online shops responsible? In the past most banks have compensated their customers for phishing thefts. But there are indications that this is changing. This leaves the bank’s customers in an impossible situation. Here governments have their work set out. Waiting for the courts is not good enough.

It is not enough to pass a law; the law also has to be enforced. How well equipped are law enforcement agencies to do this? Do they have the necessary training and equipment? The Internet criminals certainly have the best people and the latest equipment so they are no easy match.

Finally, much more research is needed in this area. This report is based on media reports but in the long run that is not good enough. Each of the issues raised here need to be researched and presented. This will give better understanding and also raise awareness about the situation and what needs to be done.

The OSCE could have a role in this process by raising awareness in the OSCE region and stimulating discussion and debate. Harmonization across the region is also an important issue. Until this has been achieved, users will not feel they have a safe Internet.

IV. Biographies

Yaman Akdeniz

Dr. Yaman Akdeniz is a senior lecturer (associate professor) at the Cyber Law Research Unit, School of Law, University of Leeds where he teaches and writes mainly about Internet related legal and policy issues. Akdeniz is also the founder and director of Cyber-Rights & Cyber-Liberties (www.cyber-rights.org), a non-profit civil liberties organization. More recently, Akdeniz acted as an expert to the United Nations High Commissioner for Human Rights Office (UNHCHR) in relation to the work of the Intergovernmental Working Group on the Effective Implementation of the Durban Declaration and Programme of Action. His report entitled *Stocktaking on efforts to combat Racism on the Internet* was published during a High Level Seminar on Racism and the Internet in Geneva in January 2006.

Arnaud Amouroux

Arnaud Amouroux has been Project Co-ordinator at the Office of the OSCE Representative on Freedom of the Media since February 2004. He has been engaged in a number of activities with regard to promoting media freedom, fighting undue speech restrictions and monitoring press violations in the OSCE region (Balkans, Turkey, Southern Europe). Arnaud holds a Master's degree in International Administration Law from the University of Pantheon-Sorbonne in Paris and a BA in Political Science from Toulouse's Institut d'Etudes Politiques.

Laurent Baup

Laurent Baup graduated from EDHEC Business School of Management in 2001. Laurent holds a Master of Law in Intellectual Property and New Technologies. After some years working as a legal counsel for several lawyers' firms, he joined the Forum des droits sur l'internet (Internet Rights Forum) in 2006 where he is in charge of issues related to minors' protection, freedom of expression, cyber-criminality, and online video games.

Bertrand de La Chapelle

Bertrand de La Chapelle is the Special Envoy for the Information Society of the French Foreign Affairs Ministry, in charge of Internet Governance and follow-up processes to WSIS. A career diplomat with an engineering background and entrepreneurial experience, de La Chapelle has specialized in multi-stakeholder governance mechanisms and the use of information technologies to facilitate them. He participated in the World Summit on the Information Society (WSIS) between 2002 and 2005. His nine year business experience includes being co-founder and President (from 1994 to 1998) of VIRTOOLS, the leading provider of development tools for the video games and interactive 3D markets. Bertrand de La Chapelle is a graduate of Ecole Polytechnique and Ecole Nationale d'Administration.

Ana Dolidze

Currently a Visiting Scholar at Columbia University, Ana Dolidze is the former president and current board member of the Georgian Young Lawyers' Association (GYLA). A graduate of Tbilisi State University, Dolidze has also conducted extensive legal studies abroad, including receiving her Master of Laws Degree in Public International Law from Leiden University in the Netherlands. In addition to chairing GYLA, she contributes to the work of a number of other organizations such as the Media Council, the Stakeholders Committee of the Millennium Challenge Georgia Fund, and the Human Rights Monitoring Council of the Penitentiary and Detention Places.

Nico van Eijk

Prof. Dr. Nico van Eijk studied law and received his Ph.D. in Information Law at the University of Amsterdam. He is currently working as a professor in Media and Telecommunications Law at the Institute for Information Law (Instituut voor Informatierecht, IViR), University of Amsterdam. The Institute for Information Law, created in 1987 as a centre of excellence for research, is one of the largest research facilities in the field of information law in Europe.

Isabelle Falque-Pierrotin

Isabelle Falque-Pierrotin is a Member of the French Council of State and Chairman of the Forum des droits sur l'internet (Internet Rights Forum), a multi-stakeholder organization supported by the French Government which works on the rights and user issues related to the Internet. Counsel to the French Government on Internet issues, she is a member of the Intellectual Property Commission, of the National French Commission for UNESCO and the French Data Protection Authority (CNIL). Isabelle graduated from Ecole Nationale d'Administration, HEC School of Management as well as the French Institute of Multimedia.

Ina Gudele

Ms. Gudele has been Minister for Special Assignments for Electronic Government Affairs of Latvia since April 2006. Between 2003 and 2005, she was Head of the Information Society Bureau at the State Chancellery. Her previous posts include being Executive Director of the Latvian Internet Association from 2000 till 2003 and founder of *Apollo*, the biggest Latvian ISP in 1997. Ms. Gudele is one of Latvia's most experienced specialists in the area of e-Government and the Information Society. She is a graduate in engineering from the Riga Polytechnic Institute.

Miklós Haraszti

Writer, journalist, human rights advocate and university professor, Miklós Haraszti was appointed the OSCE Representative on Freedom of the Media in March 2004. Haraszti studied philosophy and literature at Budapest University. In 1976 he co-founded the Hungarian Democratic Opposition Movement and in 1980 he became editor of the samizdat periodical *Beszélő*. In 1989, Haraszti participated in the "roundtable" negotiations on transition to free elections. A member of the Hungarian Parliament from 1990 to 1994, he then moved on to lecture on democratization and media politics at numerous universities. Haraszti's books include *A Worker in a Worker's State* and *The Velvet Prison*, both of which have been translated into several languages.

Wolfgang Kleinwächter

Wolfgang Kleinwächter is a Professor for International Communication Policy and Regulation at the Department for Media and Information Sciences of the University of Aarhus, Denmark. Since 1998 he has been teaching a full course on "Internet Policy and Regulation". He studied Communication, International Law and International Relations at the University of Leipzig. In 2004 he was appointed by UN Secretary General Kofi Annan as a member of the UN Working Group on Internet Governance (WGIG). In 2006 he was appointed as "Special Adviser" to the Chair of the UN Internet Governance Forum (IGF). He is also a member of the "Panel of High Level Advisers" of the "Global Alliance for ICT and Development", the follow-up of the UN ICT Task Force.

Katerina Maniadaki

Katerina Maniadaki studied law at the University of Athens. She holds an advanced LL.M. degree with distinction in European Business Law (with specialization in EC competition law) from the University of Amsterdam. She is currently completing her internship as a research assistant at the Institute for Information Law, University of Amsterdam. Katerina Maniadaki's research interests are in competition law, particularly in its application to the electronic communications sector, the regulation of telecommunications and media content, Internet Governance and Internet content regulation, freedom of expression and the protection of intellectual property rights in the area of ICT.

Christian Möller

Christian Möller has been Project Officer at the Office of the OSCE Representative on Freedom of the Media since 2003. Before that he worked from 1999 until 2002 for the Unabhängige Landesanstalt für das Rundfunkwesen (ULR) in Kiel, one of Germany's federal media authorities. He holds an M.A. in Media Studies, German Language and Public Law from Christian Albrechts University, Kiel. He has edited many publications on Internet policy and is co-founder of the "Dynamic Coalition on Freedom of Expression and Freedom of the Media on the Internet" (FOE online) an outcome of the United Nations Internet Governance Forum (IGF).

Rachid Nougmanov

Rachid Nougmanov is General Director of the International Freedom Network, an NGO devoted to promoting democracy and human rights in Eurasia. He graduated from the Architectural Institute in Almaty and the State Film Institute in Moscow (VGIK). An internationally acclaimed filmmaker, he is considered the founder of the "Kazakh New Wave". Rachid was responsible for international relations of various organizations, including the Forum for Democratic Forces of Kazakhstan and Central Asia, Republican People's Party of Kazakhstan, Democratic Choice of Kazakhstan, and For a Just Kazakhstan. In 2001, he founded KUB.kz, one of the first and most popular blog services in Central Asia, with the aim of supporting freedom of expression in the region.

Viesturs Pless

Viesturs Pless is executive director of the Latvian Internet Association (www.lia.lv). Viesturs is actively involved in several governmental initiatives pertaining to e-Government, the Information Society and information technologies policy development (Ministry of Transport, Ministry of Economics and Special Assignments Minister for Electronic Government Affairs). Most notably he is participating in the development of an Information Society strategy for 2006 to 2013. Viesturs Pless has developed e-services for governmental institutions, individuals as well as companies in Latvia. He is also a regular contributor to the European Commission's Program Safer Internet Plus.

Jennifer Siebert

Jennifer Siebert is Project Manager at jugendschutz.net in Mainz, Germany, which she joined in 2001. Jugendschutz.net is the cross-national bureau for youth protection on the Internet in Germany. The Youth

Ministries of the federal states founded jugendschutz.net in 1997 and since 2003 jugendschutz.net has been assigned to the Kommission für Jugendmedienschutz (Commission for Youth Protection in the Media) – KJM – in order to achieve a consistent control of broadcasting and the Internet. Jennifer Siebert has a legal background and is responsible for international co-operation at jugendschutz.net.

Jon Thorhallsson

Dr. Thorhallsson is President of the Confederation of European Computer User Associations (CECUA). He is also Founder and CEO of European Consulting International, a network of international partner consultants focusing on ICT (www.ecpint.com) and Chairman and CEO of Knowledge Solution Group, a business development and management consulting company based in Riga, Latvia (www.ksg.lv). He is an adviser to the Icelandic Software Fund, the New Business Venture Fund as well as an international consultant for GTZ GmbH (Deutsche Gesellschaft für Technische Zusammenarbeit). Dr. Thorhallsson is a former associate professor in Business Administration and Commerce at the University of Iceland and former board member of the National Research Council of Iceland.

www.osce.org/fom

OSCE Organization for Security and Co-operation in Europe

ISBN 3-9501955-4-8