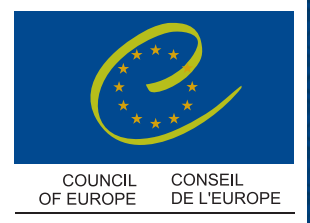




**1ST COUNCIL OF EUROPE CONFERENCE
OF MINISTERS RESPONSIBLE FOR MEDIA
AND NEW COMMUNICATION SERVICES**

A new notion of media?

28 - 29 May 2009, Reykjavik, Iceland



BACKGROUND TEXT

Internet governance and critical internet resources

Internet governance and critical internet resources

**a report prepared by
the Council of Europe Secretariat**

Media and Information Society Division
Directorate General of Human Rights and Legal Affairs
Council of Europe

April 2009

Edition française : *La gouvernance de l'Internet et ses ressources critiques*

The opinions expressed in this work are the responsibility of the author and do not necessarily reflect the official policy of the Council of Europe.

Media and Information Society Division
Directorate General of Human Rights and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex

© Council of Europe, 2009

Printed at the Council of Europe

Contents

Executive summary, page 3

Introduction, page 5

Evolution of the Internet, page 7

Social networks and the Internet of Services, page 7

Internet of Things, page 7

Convergence, page 7

Nomadic use, page 8

Increasing data transfer, page 8

Part 1. Internet as a critical infrastructure, page 9

1.1 Root servers, page 9

1.2 Backbone structures, page 11

1.3 Broadband access, page 13

1.4 Internet system of names and numbers, page 15

1.5 Internet as a critical resource, page 20

Part 2. Internet protection in international law, page 23

2.1 Internet as a global resource, page 23

2.2 Internet protection against technical risks, page 24

2.3 Internet protection against cyber attacks, page 25

2.4 Internet protection in case of interstate conflict, page 26

Conclusion, page 27

Appendix I, page 29

Extracts from international human rights law which includes Council of Europe standards related to the right to freedom of expression, page 29

Appendix II, page 33

Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, page 33

Appendix III, page 39

Extracts from "Responsibility of States for Internationally Wrongful Acts" (2001), page 39

Executive summary

Internet has the potential to improve our quality of life, in particular our economic, social and cultural development, and our democratic citizenship. Internet's openness and accessibility have become preconditions for the enjoyment of fundamental rights. The potential for us all to develop and improve the quality of our lives will be limited unless we make the Internet sustainable, robust, secure and stable.

Stability, security and ongoing functioning of the Internet depend on Critical Internet Resources and their management, including the root name servers, the backbone structures, the Domain Name System and Internet Protocols. Critical Internet resources are managed by various entities, without any common governance approach.

The Council of Europe has an important part to play in guaranteeing the protection of its values and standards on democracy, law and human rights through Internet governance. In its Recommendation CM/Rec (2007) 16¹, the Committee of Ministers underlined the public service value of the Internet, noting the "legitimate expectation [of people] that Internet services be accessible and affordable, secure, reliable and ongoing" and stating that its "protection should be a priority with regard to the governance of the Internet".

There are several issues related to Critical Internet resources which need to be addressed in order to protect freedom of expression and information (Article 10, ECHR). These resources often have transboundary implications. Some of them are:

- **Broadband access for everyone:** Broadband access is an important element in avoiding what could be called "info-exclusion" and in ensuring the participation in the Information Society.

- **Transition to IPv6:** The implementation of IPv6 is essential for the connectivity of networks. Without connectivity, people will be deprived of access to an important part of the Internet.
- **Internationalised Domain Names:** Multilingualism in cyberspace is a key concept to ensure cultural diversity and participation of all linguistic groups in the Information Society.
- **Equal distribution of Internet Exchange Points:** Ensuring local access on Internet Exchange Points is an important element in making the Internet affordable and ongoing, due to the high costs and latency associated to the need of international links.

The issues are global issues, so there is a need for multilateral co-operation. Multilateral co-operation is also essential in protecting the Internet. There are various risks of damage to Internet infrastructure such as mismanagement, cyber attacks or other malicious acts, or technical accidents. The repercussions of such events could be global, and prevention therefore also needs to be global. Critical issues need to be identified in order to avoid the risks. There is a real need to define the responsibility and the accountability of the different stakeholders, in case of mismanagement, technical accidents, aggression or other events, which could have a serious impact on the ongoing functioning of the Internet. In order to fulfil their responsibility to ensure the public service value of the Internet, and to protect the right to freedom of expression and information on the Internet, states may need to enter into interstate arrangements comparable to those that apply to certain natural resources or risks.

1. Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet, adopted by the Committee of Ministers on 7 November 2007, Council of Europe.

Introduction

Internet has the potential to improve the quality of life, in particular our economic, social and cultural development, and our democratic citizenship. It can thus contribute to the United Nations Millennium Development Goals. Access to and usage of the Internet are becoming more and more important in our daily life. Over the last decade the Internet has brought significant changes in our societies. Internet is changing our lifestyle. With further technological development, the importance of Internet will increase. The revolution of the Internet is not over: due to the development of broadband, Internet will become even faster, available anytime and anywhere. The “Internet of Things” will emerge, connecting objects, rooms, machines.

The increasing importance of the Internet raises the question of its governance, which is currently defined 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.

In the outcome documents of the *World Summit on the Information Society* (2003–2005), it is recognised that building an inclusive Information Society requires new forms of solidarity, partnership and co-operation among governments and other stakeholders, i.e. the private sector, civil society and international organisations (Article 17, Geneva Declaration).

In order to enhance co-operation, the Internet Governance Forum (IGF) was organised. The Council of Europe takes an active part in the IGF. In its *Submission to the Internet Governance Forum in Brazil* in 2007, the Council of Europe stated its objective “to secure peoples’ enjoyment of a maximum of rights and services, subject to a minimum of restrictions, while at the same time seeking to ensure the level of security that users are entitled to expect”.

The Internet must be governed in full respect of human rights; in particular, the fundamental right to freedom of expression, which includes the “freedom to hold opinions and to receive and impart information

and ideas without interference by public authority and regardless of frontiers.”²

Human rights are one of the three core values of the Council of Europe, along with the rule of law and the concept of genuine democracy (1949 Statute, recital 3 of the preamble and Article 3). More particularly, individual freedom, political liberty and the rule of law are referred to as “principles which form the basis of all genuine democracy” (recital 3 of the preamble).

The preamble to the European Convention on Human Rights (ECHR; 1950) expresses the resolve of governments of European countries which are like-minded and have a common heritage of political traditions, ideals, freedom and rule of law, to take the first steps of the collective enforcement of certain of the rights stated in the Universal Declaration on Human Rights (recital 6).

In the *Vienna Declaration* (1993), the guarantee of freedom of expression and, in particular, of the media was seen as a decisive criterion for assessing any application for Council of Europe membership. The Declaration also states the intention to “render the Council of Europe fully capable of thus contributing to democratic security as well as meeting the challenges of society in the 21st century, giving expression in the legal field to the values that define our European identity, and to fostering an improvement in the quality of life”.

In the *Strasbourg Final Declaration and Action Plan* (1997) the Council of Europe Heads of State and Government solemnly reaffirmed their attachment to the fundamental principles of the Organisation – pluralist democracy, respect for human rights, and the rule of law. They underlined the contribution of the Council of Europe’s essential standard-setting role to the development of international law through European conventions. They confirmed the goal of the Council of Europe to achieve a greater unity between its member states, with a view to building a freer, more tolerant and just European society based on common values, such as freedom of expression and information, cultural diversity and the equal dignity of all human beings.

2. cf. Article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (the “European Convention of Human Rights”).

In order to attain this goal, it was decided to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe. The Action Plan set out an agenda for action in five fields, including democracy and human rights. Regarding new information technologies, the Heads of State and Government resolved to develop a European policy for their application, with a view to ensuring respect for human rights and cultural diversity, fostering freedom of expression and information and maximising the educational and cultural potential of these technologies. They invited the Council of Europe to seek, in this respect, suitable partnership arrangements.

In the *Declaration on freedom of communication on the Internet* (2003), through the Committee of Ministers of the Council of Europe, member states recalled their commitment to the fundamental right to freedom of expression and information, as guaranteed by Article 10 of the European Convention of Human Rights. The Declaration states that member states should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price (principle 4).

In its *Recommendation CM/Rec (2007) 16*, the Committee of Ministers underlined the public service value of the Internet:

Convinced that access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the information society;

Recalling the 2003 UNESCO Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace, which calls on member states and international organisations to promote access to the Internet as a service of public interest;

Aware of the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing;

Firmly convinced that the Internet and other ICT services have high public service value in that they serve to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use them, and that their protection should be a priority with regard to the governance of the Internet,

The Committee of Ministers recommended that member states adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the Information Society (Article 1). In this connection, a human right based Internet governance is essential.

The Internet's openness and accessibility have become preconditions for the enjoyment of fundamental rights. The potential for us all to develop and improve the quality of our lives will be limited unless we make the Internet sustainable, robust, secure and stable.

Stability, security and ongoing functioning of the Internet depend on "critical Internet resources" including the name root servers, Internet's backbone structures as well as the domain name system, addresses and Internet transmission protocols.

Root servers and backbone structures are operated by a variety of private and public actors, without any common governance structure. The Internet system of names and numbers is managed by the Internet Corporation for Assigned Names and Numbers (ICANN), a non-profit entity established under the laws of the United States, at present answerable only to the Department of Commerce. The Joint Project Agreement (JPA), defining the relationship between ICANN and US Department of Commerce, will expire in September 2009, when ICANN is expected to become *more* independent. At the same time, the Internet will continue its development and become more and more important in day-to-day activities. Main developments concern critical issues, such as the transition from IPv4 to IPv6, the creation of new top level domains (TLDs) and broadband access. These developments have led to the emergence of new issues which have to be addressed in order to protect human rights in the Information Society.

Critical Internet resources need to be governed in a way that permits the exercise and enjoyment of human rights and fundamental freedoms. Due to its increasing importance in daily life, Internet functioning is also crucial for providing other services, such as health services or security services. Therefore, the Internet itself is becoming a critical resource for users generally.

The aim of this report is to describe the issues relating to critical Internet resources while having regard to the need to ensure the fundamental right to freedom of expression and information.

Evolution of the Internet

Social networks and the Internet of Services

The wide take-up of broadband has caused a shift in the way the Internet is used. In particular, we have moved from the information provision that typified the Web in the mid-1990s, to the increasingly participative Web of today known as “Web 2.0”. Experts are already talking about a further generation of the Web that will permit Web usage to be automated.³ The “Semantic Web” shall bring structure to the meaningful content of webpages, creating an environment where software agents roaming from page to page can readily carry out sophisticated tasks for users. The real power of the

Semantic Web will be realised when people create many programs that collect Web content from diverse sources, process the information and exchange the results with other programs. The effectiveness of such software agents will increase exponentially as more machine-readable Web content and automated services (including other agents) become available. The Semantic Web promotes this synergy: even agents that were not expressly designed to work together can transfer data among themselves when the data come with semantics.⁴

Internet of Things

The notion of the Internet of Things refers to the seamless connection of devices, sensors, objects, rooms, machines, vehicles, etc. through fixed and wireless networks. Connected sensors, devices and tags can interact with the environment and send the information to other objects through machine-to-machine communication. One possibility is for example the “Health Monitoring”:

Body-worn sensors and the Internet of Things facilitate the use of lightweight systems for monitoring vital health parameters like heart rate, respiration rate and blood pressure. Patients can simply wear monitoring systems while continuing to go about their daily business.⁵

Convergence

Before the rapid development of the Internet, separate systems – telephone, television and video, individual computer systems – stored and transmitted voice, video and data. Today, these systems are converging onto the Internet. In addition to convergence of network platforms, convergence is also taking place at several other levels: at the content level with Video on Demand (VoD) and television over Internet Protocol networks (IPTV); at the business level, with companies offering combined television, Internet and telephone services to subscribers; and at the device level, with multi-purpose devices that can combine e-mail, telephone and Internet, for

example. Indeed, this has become the era of converged media. Users upload some 10 hours of video per minute alone to the video sharing site YouTube. By 2008, nearly 300 million people are registered to use free VoIP (Voice over Internet Protocol) software Skype, enabling them to make phone calls worldwide at little or no extra cost via their existing Internet access. Converged media are also increasingly becoming mobile with the expansion of wireless broadband networks. As convergence takes place and investment in next generation networks (NGN) begins, the role of very fast optical fibre networks “to the home” becomes increasingly important

3. Commission of the European Communities: Communication on future networks and the Internet, COM (2008) 594 final, Brussels, 29 September 2008.
4. The Semantic Web was first proposed by the inventor of the World Wide Web, Tim Berners-Lee. See Berners-Lee, Tim/Hendler, James/Lassila, Ora, “The Semantic Web: A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities”, *Scientific American Magazine*, 17 May 2001, <http://www.sciam.com/article.cfm?id=the-semantic-web>.
5. *Communication on future networks and the Internet*, op.cit.

given that emerging applications, such as high-definition television and video-on-demand, require increasing amounts of bandwidth. The regulatory challenges associated with convergence are significant. With migration to Internet Protocol-based networks, one net-

work can handle many types of converged services. This means that governments face a fundamental shift in the way they regulate broadcasting and telecommunication services.⁶

Nomadic use

Consumers are increasingly adopting a range of portable devices such as laptop computers, PDAs, MP3 players, mobile TV sets, GPS navigation devices or portable gaming consoles. Citizens and businesses will want to access their preferred Internet services easily and cheaply wherever they roam. This development – a Web

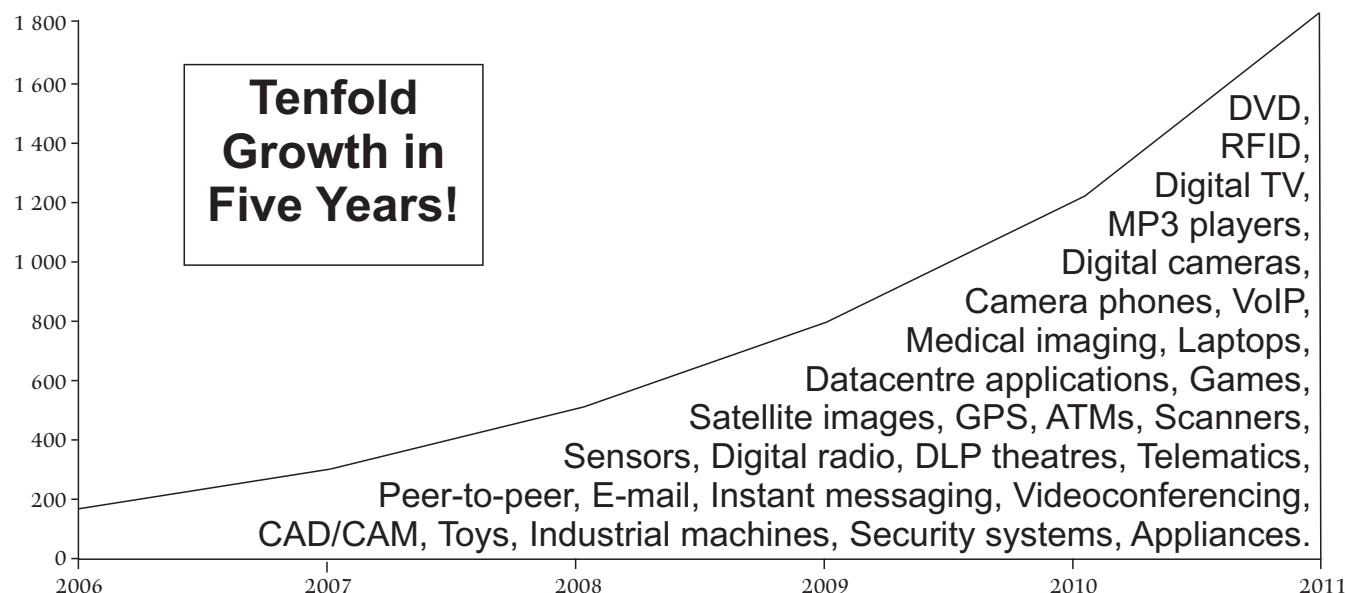
2.0 on the move adapted to user needs – will not only generate many new business opportunities and transform work organisation patterns; there will also be many applications of social benefit such as support to disabled travellers or emergency workers.⁷

Increasing data transfer

One immediate consequence of the previous trends is the explosion of data traffic over the net. By 2011, as the diagram below shows, the digital information on net-

works and the Internet is expected to be 10 times greater than in 2006.⁸

Figure 1: Digital information created, captured, replicated worldwide



Source: IDC, 2008.

6. OECD (2008): *Policy Brief: The Future of the Internet Economy*.

7. *Communication on future networks and the Internet*, op.cit.

8. Gantz, John F. et al, *An IDC White Paper: The Diverse and Exploding Digital Universe: An Updated Forecast of Worldwide Information Growth Through 2011*, IDC, 2008.

Part 1. Internet as a critical infrastructure

1.1 Root servers

1.1.1 Importance of root servers

Effective root server operations are an essential component in providing a stable and secure, globally interoperable Internet. There are 12 operators running 13 root servers that provide a key element of the underlying domain name system infrastructure of the Internet. Root servers provide an authoritative directory ensuring Internet services that are accessed with names, the URLs, which are translated from human readable names

into network addresses that a computer can find. The root server system overall answers well over 100 000 queries per second, providing the first step in determining the requested network address.⁹ Root server operators undertake to maintain adequate hardware, software, network and other resources to ensure secure and stable domain name system interoperability with the global Internet.¹⁰

1.1.2 Authority over root servers

1.1.2.1 ICANN

ICANN co-ordinates the operation and evolution of the DNS root name server system (Article I, Sect. 1.2; ICANN Bylaws). Decisions are taken by the Board, and there is a Root Server System Advisory Committee (Article XI, Sect. 2.3). The role of the RSSAC is:

to advise the Board about the operation of the root name servers of the domain name system. The RSSAC shall consider and provide advice on the operational requirements of root name servers, including host hardware capacities, operating systems and name server software versions, network connectivity and physical environment. The RSSAC shall examine and advise on the security aspects of the root name server system. Further, the RSSAC shall

review the number, location, and distribution of root name servers considering the total system performance, robustness, and reliability.

Membership in the RSSAC consists of each operator of an authoritative root name server and such other persons as are appointed by the ICANN Board. The Root Server System Advisory Committee annually appoints one non-voting liaison to the ICANN Board of Directors, without limitation on re-appointment, and annually appoints one non-voting liaison to the ICANN Nominating Committee (Article XI, Sect. 2.3).

1.1.2.2 Root server operators

The root servers are controlled by a variety of government, academic institutions and private/business entities. A number of the Internet root name servers are implemented as large numbers of clusters of machines using “anycast” (for best management of not pre-determined routing responses). “Anycast” means a net-

work service where multiple servers respond to the same IP address and provide the same service for that address. The C, F, I, J, K, L and M servers exist in multiple locations on different continents, using anycast announcements to provide a decentralised service.

9. ICANN Website: www.icann.org/en/announcements/announcement-04jan08.htm.

10. *Mutual Responsibilities Agreement*, 2007, <http://www.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf>.

Table 1: Root name servers

A	VeriSign	Dulles, Virginia, US
B	USC-ISI	Marina Del Rey, California, US
C	Cogent Communications	distributed using anycast
D	University of Maryland	College Park, Maryland, US
E	NASA	Mountain View, California, US
F	ISC	distributed using anycast
G	Defense Information Systems Agency	Columbus, Ohio, US
H	US Army Research Lab	Aberdeen Proving Ground, Maryland, US
I	Autonomica	distributed using anycast
J	VeriSign	distributed using anycast
K	RIPE NCC	distributed using anycast
L	ICANN	distributed using anycast
M	WIDE Project	distributed using anycast
Source: www.root-servers.org .		

The operators have the operational authority over the root server. There is no central authority that controls the operation of all root name servers. Neither ICANN nor the Internet Assigned Numbers Authority (IANA), operated by ICANN, have any executive authority over the operation of root name servers.¹¹ Root server operators are generally not bound by any agreement. Only those operated by ICANN itself and by VeriSign under contract with the US Department of Commerce, are contractually or legally bound to the

ICANN regime or accountable to the US Government. The others, however, are operated by heterogeneous actors in different nations.¹² There is only one agreement between ICANN and a root server operator (ISC), setting out the formal written recognition of the mutual roles ICANN and the root server operator perform with respect to each other: The “Mutual Responsibilities Agreement”.¹³ The Agreement is the first formalisation of mutual responsibilities between a root server operator and an ICANN.

1.1.3 Root server as a critical Internet resource

1.1.3.1 Lack of formal relationship

The operation of root servers is critical insofar as they perform their functions today without any formal relationship with any authority. The operators of root servers restrict themselves to operational matters; they are not involved in policy making and data modifications. However, operators have no clearly defined responsibilities

and accountability, especially in relation to the stability and secure functioning of the Internet.¹⁴ The issue has also been addressed by the Working Group on Internet Governance which noted in its report the “lack of formal relationships with root server operators”.¹⁵

1.1.3.2 Geographical distribution

The geographical distribution of root servers plays the most important role for overall performance. Today, it is highly uneven, with six root servers on the US East

coast, four on the US West coast, two in Europe (respectively in the United Kingdom and in Sweden), and one in Japan.

11. Karrenberg, Daniel, “DNS Root Name Server FAQ”. *Internet Society*, 2007, <http://www.isoc.org/briefings/020/>.

12. The Internet Governance Project, *Internet Governance. The State of Play*, 2004, <http://www.internetgovernance.org/pdf/ig-sop-final.pdf>.

13. The Mutual Responsibilities Agreement can be found on the ICANN website, <http://www.icann.org/en/froot/ICANN-ISC-MRA-26dec07.pdf>.

14. The Working Group on Internet Governance, *Background Report*, 2005, <http://www.wgig.org/docs/BackgroundReport.doc>.

15. The Working Group on Internet Governance, *Report*, 2005, <http://www.wgig.org/docs/WGIGREPORT.doc>.

Figure 2: Map of the Root Servers



Source: <http://www.icann.org/correspondence/root-map.gif>.

If the Asian Root Server should fail, for example, latency would increase by a significant amount for a large percentage of its “clients”. According to a Study of the Cooperative Association for Internet Data Analysis, today, US root clients appear to be overprovisioned. If

the root servers were distributed in accordance with the current geographic distribution of their clients, it could benefit clients that are currently away from the 13 root servers.¹⁶

1.2 Backbone structures

1.2.1 The importance of backbone structures

The Internet backbone consists of many different *networks*. Usually, the term is used to describe large networks that interconnect with each other and may have individual ISPs as clients. These backbone providers usually provide connection facilities in many cities for their clients, and they themselves connect with other backbone providers at *Internet Exchange Point (IXPs)*. An IXP interconnects Internet service providers (ISPs) in a region or country, allowing them to exchange domestic Internet traffic locally without having to send those

messages across multiple international hops to reach their destination.¹⁷ Backbone structures are one of the most effective mechanisms to accomplish both cost and service gains. With global growth in Internet data traffic and the digitalisation of traditionally analogue services, IXPs are also growing in importance as critical infrastructures. IXPs are normally governed by the connected IPS as a mutually-owned membership organisation.

1.2.2 Internet Exchange Points as a critical Internet resource

1.2.2.1 Unequal distribution

Internet Exchange Points provide important benefits for Internet users. However, only 79 countries around the world have operational IXPs. This problem has been addressed at the IGF Rio de Janeiro Meeting 2007 in a

Best Practice session titled *Internet Traffic Exchange in Less Developed Internet Markets and the Role of Internet Exchange Points (IXPs)* organised by the Internet Society (ISOC).

16. Lee, Tony/Huffaker, Bradley/Fomenkov, Marina, *On the problem of optimisation of DNS root servers' placement*, 2003, <http://www.caida.org/publications/papers/2003/dnsplacement/dnsplacement.pdf>.

17. McLaughlin, Andrew, “Internet Exchange Points. Their Importance to Development of the Internet and Strategies for their Deployment – The African Example”, *Global Internet Policy Initiative*, 2002, rev. 2004.

Figure 3: Density distribution of the Internet Exchange Points (IXPs):



Source: Packet Clearing House, <https://prefix.pch.net/applications/ixpdir/summary/>.

Poor connectivity between ISPs in developing countries often results in the routing of local traffic over expensive international links simply to reach destinations within the country of origin. For example, traffic between Tanzania and Kenya or between Malawi and South Africa goes via Europe.¹⁸ Due to the lack of fibre optic links, most developing country ISPs use VSAT satellite circuits for international connectivity to upstream ISPs. Satellite connections introduce significant latency (delay) in the network.¹⁹ IXPs can improve the quality of Internet services in a country by reducing the delay associated with packet delivery. In Kenya, for example, implementing KIXP (Kenyan Internet exchange point) helped reduce latencies from over 700ms to below 100ms.

The lack of an IXP could also have an impact on local content: without an IXP, local content is hosted outside the country and encouraging the growth of local content becomes more difficult. Kenya and Argentina, for example, implemented local instances of the Internet's F and J root servers in addition to local .com and .net resolution services. As a result, locally originated lookup requests for these services no longer need to transit international links for a response. The local presence of these services helps build resilience in the national Internet infrastructure.²⁰

The main challenge will be a more equitable distribution of IXPs in all countries. Many developing countries are lagging behind the developed world.

Table 2: Annualised growth rate of IXPs (as of November 2007)

Region	IXPs	Growth
Africa	17	21%
Asia Pacific	67	15%
Europe	107	54%
Latin America	20	94%
North America	87	87%

Presented by Bill Woodcock, Packet Clearing House. Source: ISOC, <http://www.isoc.org/educpillar/resources/igf-ixp-report-2007.shtml>

1.2.2.2 Connectivity costs

ISPs connectivity costs are allocated according to bilateral contracts, which can be classified as peering or transit agreement. Countries which use the Internet less have to sign transit agreement because there is no incentive for the international providers to enter a shared-cost peering agreement with it. The result is that developing countries have much higher costs because they have to pay the main part of both outbound and

inbound traffic. In its 2005 Report, the Working Group on Internet Governance pointed out the uneven distribution of costs: "Internet service provider (ISPs) based in countries remote from the Internet backbones, particularly in the developing countries, must pay the full cost of the international circuits".²¹

Another major concern is the growth of Internet Exchange Points (IXPs) such as LINX in London, AMSIX

18. IGF Rio, *Best Practice Forum: Internet Traffic Exchange in Less Developed Internet Markets and the Role of Internet Exchange Points (IXP)*, Transcript, 2007, <http://www.isoc.org/educpillar/resources/docs/igf-ixp-transcript-2007.pdf>.

19. *Internet Exchange Points. Their Importance to Development of the Internet and Strategies for their Deployment – The African Example*, op.cit.

20. Internet Society, *Internet Exchange Points*, 2007, <http://www.isoc.org/educpillar/resources/igf-ixp-report-2007.shtml>.

21. Report of the Working Group on Internet Governance, op.cit.

in Amsterdam, DECIX in Frankfurt etc. ISPs often use IXPs to reduce the costs of peering. Peering Arrangements between ISPs with a large number of content providers are in both providers' interests because it avoids paying for transit. However, large ISPs often refuse to peer with significantly smaller ISPs because they perceive them as potentially paying customers. The value of joining an IXP is higher the more ISPs join, so that there is an obvious economic pressure towards winner-take-all scenarios where one IXP is much larger than its local rivals. The economic pressures towards a dominant IXP could then lead to failure when there is a problem with the IXP itself. The largest IXPs deal with this through diversity within the IXP itself. For example,

1.2.2.3 Backbone interconnection

Problems could also arise as a result of two ISPs not being willing to enter into a direct traffic exchange relationship. In the United States, the Network Reliability and Interoperability Council (NRIC), an advisory committee composed of members of the communications industry, has explored the issue:

There is a potential problem if certain backbone ISPs fail to interconnect either by peering or transit. In principle, this could result in a loss of full connectivity in the Internet. Full connectivity between any two ISPs requires that the two ISPs either peer directly, that one of them obtains transit from the other, or that at least one of them obtains transit service from a third ISP.²³

Such dangers are expected to be avoided by pressure upon a network which fails to offer Internet connectivity from its customer. However, business pressure is not always sufficient for avoiding the risks.

On March 2008 Cogent stopped routing packets from Swedish network provider Telia. Their network lost mutual connectivity. Millions of Telia subscribers across northern Europe lost access to parts of the Internet. Cogent's mostly US customer base lost access to the smaller collection of (mostly Swedish) websites that Telia controlled. The connection was re-established only 15 days later.²⁴

1.3 Broadband access

1.3.1 The importance of broadband access

Broadband is an enabling technology. As broadband connections proliferate, connections are faster – and less expensive – than they were just three years ago. The average speed of advertised connections increased from 2 Mbit/s in 2004 to almost 9 Mbit/s in 2007.²⁵

Benefits are realised through the delivery of advanced applications and services expected to bring about pro-

LINX operates in multiple buildings in London Docklands with two physically separate peering LANs from two different vendors, so that there is little chance of a common-mode failure. AMSIX in Amsterdam has an entire redundant fail-over system. However, not all IXPs have taken such steps, mainly because of the expense. For larger ISPs there is no problem; they will be connected to IXPs in multiple countries, so if AMSIX fails they can exchange traffic at LINX and vice versa. However, smaller ISPs cannot afford international links, so they have to use transit for all of their traffic. It may cause partial or complete failure for their customers if the transit link cannot handle the traffic, or if their transit traffic goes via the IXP as well.²²

The same problem could also occur in case of de-peering. Peering relationships are settled by contracts. In case of de-peering, there is generally an agreed period of notice during which both Autonomous System make arrangements so that their respective customers can continue to communicate. There have been, however, instances when such arrangements have not been put in place by the time de-peering occurs. In such instances the customers of both networks may not be able to communicate between each other until this is corrected. These cases almost invariably raise the spectre for regulatory intervention.²⁵

One example: In one instance of de-peering, in April 2005, France Telecom claimed Cogent had breached some aspect of their agreed peering arrangements. Cogent countered that the termination of the peering agreement had occurred because it was seen as an increasing competitive threat in Europe.²⁶ In this instance, one or both of the players had not, for whatever reason, put alternative arrangements into place. This had some impact on traffic exchange and on the use of Internet until alternative arrangements were put in place.²⁷

ductivity gains both for businesses and public administrations. Distance education and learning are stimulated through real-time services, resulting in the upgrade of skills, improved human capital and life-long learning. In healthcare, high-speed Internet access allows diagnosis and patient treatment to be carried out independently of geographical location. In the context of e-government,

22. Anderson, Ross/Böhme, Rainer/Clayton, Richard/Moore, Taylor, *Security economics and the internal market*, 2008, http://www.enisa.europa.eu/doc/pdf/report_sec_econ_int_mark_20080131.pdf.

23. Federal Communications Commission, Network Reliability and Interoperability Council (NRIC): *Service Provider Interconnection for Internet Protocol Best Effort Service, Focus Group 4 Final Report*, Appendix B, www.nric.org/pubs/nric5/2B4appendixb.doc.

24. Woolley, Scott, "Telecom Knockout", *Forbes.com*, 13 October 2008, http://www.forbes.com/forbes/2008/1013/064_print.html.

25. OECD (2006): *Internet Traffic Exchange. Market Developments and Measurement of Growth*, DSTI/ICCP/TISP(2005)11/FINAL.

26. "France Telecom severs all network links to competitor Cogent", *Heise Online*, <http://www.heise.de/english/newsticker/news/58835>.

27. Internet Traffic Exchange. *Market Developments and Measurement of Growth*, op.cit.

28. OECD, *Broadband Growth and Policies in OECD countries*, pre-publication version, 2008.

broadband facilitates the online supply of existing and new public services. It improves the efficiency of public

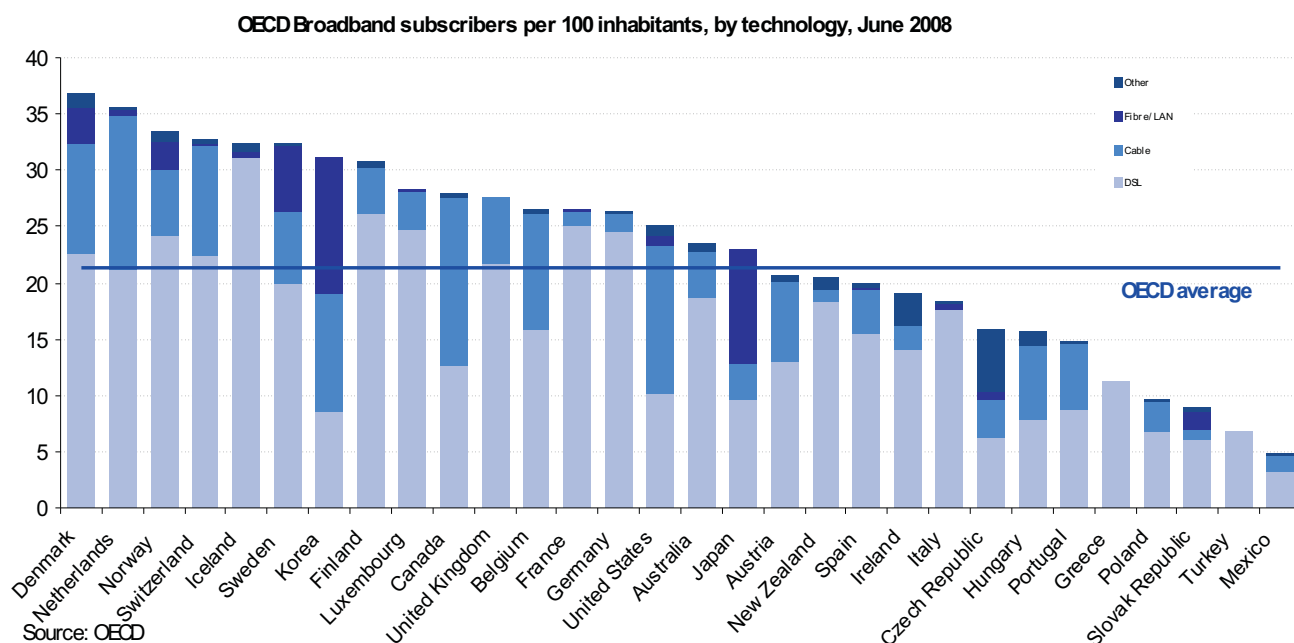
administrations and facilitates contacts between citizens and government.²⁹

1.3.2 Broadband as a critical Internet resource

1.3.2.1 Unequal access

Today, there are still substantial differences in broadband access among different countries, as shown by recent OECD statistics:

Figure 4: OECD Broadband subscribers per 100 inhabitants, by technology, June 2008



Source: OECD Broadband Portal, <http://www.oecd.org/dataoecd/21/35/39574709.xls>.

In the European Union, broadband has been taken up by around 40% of households. Even if broadband connectivity has improved, significant divides remain between rural and urban areas. Differences in income, education, as well as gender are factors influencing the uptake and use of broadband. The qualitative aspects of rural connections vary significantly more than those in urban areas.³⁰ Thus, as we move towards the Internet of the future, today's digital divide may become tomorrow's "info-exclusion", with some members of society – due to geography or disparities in resources and skills – left behind and permanently disadvantaged.³¹ Governments need to help ensure that all citizens have access to high-speed broadband networks.

Some concrete examples:

In 2006 the European Commission started its strategy "Broadband for all". Challenge stems from the high

investment cost of the civil engineering works necessary to build the ducts for these new fibre-rich networks, representing up to 80% of the total costs.³² In its Communication on future networks and Internet, the European Commission stated that "public funding in underserved areas is frequently considered necessary to provide incentives and stimulate investment."³³

In Switzerland, there is today a right to broadband access. Prices and speed are fixed by the government. Companies are free in choosing the technique. Swisscom, which is the company delivering broadband access, can ask for a co-finance. To this end, a fund has been established, to which other operators contribute.

In Iceland, high speed access will also be made available to everybody in the beginning of next year. Companies have been chosen in an open competition, prices and bandwidth have been established by the government.³⁴ In France too, a plan has been announced for

29. Commission of the European Communities: *Connecting Europe at High Speed: National Broadband Strategies*, COM (2004) 369 final, Brussels, 12 May 2004.

30. *Broadband Growth and Policies in OECD countries*, op.cit.

31. *Connecting Europe at High Speed: National Broadband Strategies*, op.cit.

32. *Communication on future networks and the Internet*, op.cit.

33. *Connecting Europe at High Speed: National Broadband Strategies*, op.cit.

34. *European Dialogue on Internet Governance (EuroDIG)*, Strasbourg 20 and 21 October 2008): contributions by Thomas Schneider (Swiss Federal Office of Communication) and Elfa Gylfadottir (Ministry of Education and Culture, Iceland).

providing access to all citizens in 2012. Croatia has also adopted a strategy for the Development of Broadband Internet Access. Funds were allocated for an open competition for areas which are not covered. In two years,

access has been significantly improved in Croatia while the access in South-eastern Europe remains generally low.³⁵

1.3.2.2 Net neutrality

Telecom and cable operators are increasingly bundling TV, Internet, and fixed and mobile telephony (“quadruple play”). It is against this background that concerns have been raised about preserving “net neutrality” as the Internet evolves. New network management techniques allow traffic prioritisation. Traffic management could be used for anti-competitive practices such as unfairly prioritising some traffic or slowing it down and, in extreme cases, blocking it.³⁶ Today, in most countries worldwide, there are no regulations

establishing a neutrality duty for access providers.³⁷ Recently, the European Commission made some proposals on this topic. It was proposed to empower the European Commission to impose a minimum quality of services in order to prevent network operators from degrading their customers. In addition, an obligation of transparency was also proposed to limit network operators’ ability to set up restrictions on end-users’ choice of lawful content and applications.³⁸

1.3.2.3 Increasing risks

Two other issues are security and interoperability. The ‘always-on’ feature of broadband increases the vulnerability of networks and of the information transmitted on them. Fully interactive applications, including in

the field of public services, require an adequate level of confidence in areas such as identity management or e-payment.³⁹ Trust is an important element regarding the Internet: if people do not trust it, Internet cannot work.

1.4 Internet system of names and numbers

The Internet system of names and numbers is governed by the Internet Corporation for Assigned Names and Numbers (ICANN). The tasks of ICANN include responsibility for Internet Protocol (IP) address space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top Level Domain name system management, and root server functions. More generically, ICANN is responsible for managing the assignment of domain names and system.

ICANN is formally organised as a non-profit corporation under the California Nonprofit Public Benefit Corporation Law. It is managed by a Board of Directors, which is composed of six representatives of the Supporting Organisations, subgroups that deal with specific sections of the policies under ICANN’s purview; eight independent representatives of the general public interest, selected through a Nominating Committee in which all the constituencies of ICANN are represented; and the President and CEO, appointed by the rest of the Board.

There are currently three Supporting Organisations. The *Generic Names Supporting Organization* (GNSO) deals with policy making on generic top-level domains (gTLDs). The *Country Code Names Supporting Organiza-*

tion (ccNSO) deals with policy making on country-code top-level domains (ccTLDs). The *Address Supporting Organization* (ASO) deals with policy making on IP addresses.

ICANN also relies on some advisory committees to receive advice on the interests and needs of stakeholders that do not directly participate in the Supporting Organisations. These include the *Governmental Advisory Committee* (GAC), which is composed of representatives of a number of national governments from across the world and the European Commission, as well as certain observer organisations including UNESCO and OECD;⁴⁰ the *At-Large Advisory Committee* (ALAC), which is composed of representatives of organisations of individual Internet users from around the world; the *Root Server System Advisory Committee* which provides advice on the operation of the DNS root server system; the *Security and Stability Advisory Committee* (SSAC), which is composed of Internet experts who study security issues pertaining to ICANN’s mandate; and the *Technical Liaison Group* (TLG), which is composed of representatives of other international technical organisations that focus, at least in part, on the Internet.

35. Croatia: Central State Administrative Office for e-Croatia, <http://e-hrvatska.hr/sdu/en/ProgramEHrvatska/Provedba/Broadband.html>. France: France numérique 2012, http://francenumerique2012.fr/pdf/081020_FRANCE_NUMERIQUE_2012.pdf.

36. *Communication on future networks and the Internet*, op.cit.

37. ISOC France: *Net neutrality*, Legal note number 2, 18 May 2008, <http://isoc.fr/net-neutrality-article0073.html>.

38. Commission of the European Communities: Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection co-operation, COM(2007) 698 final, Brussels, 13 November 2007.

39. *Connecting Europe at High Speed: National Broadband Strategies*, op.cit.

40. According to ICANN Bylaws, GAC “Membership shall also be open to Distinct Economies as recognised in international fora, and multinational governmental organisations and treaty organisations, on the invitation of the Governmental Advisory Committee through its Chair.” (Article XI, Sect. 2). The list of all Members and Observer can be found on the GAC website: <http://gac.icann.org/web/contact/rep/index.shtml>.

The powers of ICANN are exercised by the Board. The Supporting Organisations and the Advisory Committees advise the Board, without any obligation for following the advice. This regulation also applies the for GAC (Governmental Advisory Committee), which “provides advice on the activities of ICANN as they relate to concerns of government, particularly on matters where there may be an interaction between ICANN’s policies and various laws and international agreements or where they may affect public policy issues”:

The advice of the Governmental Advisory Committee on public policy matters shall be duly taken into account, both in the formulation and adoption of policies. In the event that the ICANN Board determines to take an action that is not consistent with the Governmental Advisory Committee advice, it shall so inform the Committee and state the reasons why it decided not to follow that advice. The Governmental Advisory Committee and the ICANN Board will then try, in good faith and in a timely and efficient manner, to find a mutually acceptable solution.

If no such solution can be found, the ICANN Board will state in its final decision the reasons why the Governmental Advisory Committee advice was not followed, and such statement will be without prejudice to the rights or obligations of Governmental Advisory Committee members

1.4.1 DNS root zone

The TLDs are divided into two classes, namely generic Top-Level Domains (gTLDs) (e.g. “.com” or “.org”) and country code Top-Level Domains (ccTLDs). The Internet Assigned Numbers Authority (IANA) is responsible for

1.4.1.1 gTLD

1.4.1.1.1 Authority over gTLDs⁴²

gTLDs do not generally have geographic or country designations and are governed by rules set up by the Internet Corporation for Assigned Names and Numbers (ICANN).

Since 1999, ICANN has been working on the introduction of new top-level domains. New gTLDs are added to the root and evaluated. The further development of the domain name space impacts strongly on key issues such as the equitable distribution of resources, access for all, and multilingualism.

Advisory Committees

The Generic Names Supporting Organization (GNSO) is responsible for developing and recommending to the ICANN Board substantive policies relating to generic top-level domains. The GNSO consist of (i) various Constituencies representing particular groups of stakeholders and (ii) a GNSO Council responsible for managing the policy development process of the GNSO. No two representatives selected by a Constituency are citizens of the same country or of countries located in the same geographic region. The stakeholders are:

with regard to public policy issues falling within their responsibilities (Article XI, 2).

The relation between ICANN and the US Department of Commerce is governed by the Memorandum of Understanding signed in 2006. In this Joint Project Agreement, which ends on the 31 September 2009, the Department “reaffirms its policy goal of transitioning the technical co-ordination of the DNS to private sector”. The Department continues to provide expertise and advice, to consult with the managers of root name servers operated by the US Government and to participate in the Governmental Advisory Committee.

In September 2009, at the end of the Joint Project Agreement, ICANN shall become totally independent from US Government. It is not yet decided how ICANN should then be organised. The President’s Strategy Committee (PSC), responsible for making observations and recommendations concerning strategic issues facing ICANN, published a Transition Action Plan, setting out the requirements of a post-JPA ICANN. ICANN shall be safeguarded against capture (by governments or even by itself, by the Board or the staff) and be accountable to the Community. It also shall be internationalised and be financially and operationally secure. Different proposals will be discussed during the next year.⁴¹

management of the DNS root zone. This role means assigning the operators of top-level domains, such as .uk and .com, and maintaining their technical and administrative details.

- a. gTLD Registries (representing all gTLD registries under contract to ICANN);
- b. Registrars (representing all registrars accredited by and under contract to ICANN);
- c. Internet Service and Connectivity Providers (representing all entities providing Internet service and connectivity to Internet users);
- d. Commercial and Business Users (representing both large and small commercial entity users of the Internet);
- e. Non-Commercial Users (representing the full range of non-commercial entity users of the Internet); and
- f. Intellectual Property Interests (representing the full range of trademark and other intellectual property interests relating to the DNS).

Decision-making

In the event that the GNSO Council is able to reach a Supermajority Vote on the Supplemental Recommendation, the Board shall adopt the recommendation unless more than 66% of the Board determines that such policy is not in the interests of the ICANN community or ICANN. In any case in which the Council is not able to

41. ICANN, *Transition Action Plan*, 2008, <http://www.icann.org/en/psc/iic/transition-action-plan-revised-en.pdf>; EuroDIG: contribution by Yrjö Lansipuro (Ambassador, Finnish Foreign Ministry/member of the ICANN President’s Strategy Committee).

42. For the whole part see ICANN Bylaws, <http://www.icann.org/en/general/bylaws.htm>.

reach Supermajority, a majority vote of the Board will be sufficient to act.

1.4.1.1.2 gTLDs as critical Internet resources

1.4.1.1.2.1 gTLD distribution

The creation of new gTLDs raises the question of *freedom of expression* (Article 10, ECHR) and of freedom of assembly and association (Article 11, ECHR) that include “the right to freedom of peaceful assembly and to freedom of association with others, including the right to form and to join trade unions for the protection of his interests.”

Having a TLD increases the freedom of expression and the freedom of association of a group. Arguably, the use of domain names concerns forms of expression that are protected by human rights law which, within a European context, requires that any restriction has to be prescribed by law and be necessary in a democratic society.⁴³ European associations expressed their concern that American groups could be privileged in the allocation of TLDs.⁴⁴ The issue has also been addressed by the German Parliament which were asking the German Government to plead within the GAC for the allocation of regional and local TLDs.⁴⁵

The gTLD distribution also raises the issue of language diversity. The utilisation of a website in own language is an important element of access to the Internet. In the 1999 Declaration on a European policy for new information technologies, the Committee of Ministers urged member states to:

promote the full use by all, including minorities, of the opportunities for exchange of opinion and self-expression offered by the new information technologies

and to:

encourage the provision of cultural, educational and other products and services in an appropriate variety of languages.

In the distribution of new gTLDs, the diversity of language should also be respected.⁴⁶

1.4.1.1.2.2 Name registration

The introduction of new gTLDs also bring on the question of the Domain name. In its recommendation on *GAC principles regarding new gTLDs*⁴⁷, the GAC states that new gTLDs should respect:

- a) The provisions of the Universal Declaration of Human Rights which seek to affirm “fundamental human rights, in the dignity and worth of the human person and in the equal rights of men and women”;
- b) The sensitivities regarding terms with national, cultural, geographic and religious significance.

The provision clearly raises the question of freedom of expression, i.e. which names are allowed in the name of this fundamental right and which are not.⁴⁸

1.4.1.1.2.3 Internationalised Domain Names (IDNs)

Multilingualism is a key concept to ensure cultural diversity and participation for all linguistic groups in cyberspace. Domain Names, which are currently mainly limited to characters from the Latin or Roman scripts, are seen as an important element in enabling the multilingualisation of the Internet, reflecting the diverse and growing language needs of all users. One of the most important challenges relating to cultural diversity on Internet will be the introduction of Internationalised Domain Names (IDNs). The implementation could open the door for billions of people in the global Internet community to use top level domains in their native script.

As regards cultural rights, the 2005 UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions⁴⁹ states in Article 2.1:

Cultural diversity can be protected and promoted only if human rights and fundamental freedoms, such as freedom of expression, information and communication, as well as the ability of individuals to choose cultural expressions, are guaranteed (Article 2.1).

Equitable access to a rich and diversified range of cultural expressions from all over the world and access of cultures to the means of expressions and dissemination constitute important elements for enhancing cultural diversity and encouraging mutual understanding (Article 2.7).

Relating to the Internet, it is expressly stated in Article 12 that:

Parties shall endeavour to strengthen their bilateral, regional and international co-operation for the creation of conditions conducive to the promotion of the diversity of cultural expressions ... notably in order to:

(d) promote the use of new technologies, encourage partnerships to enhance information sharing and cultural understanding, and foster the diversity of cultural expressions;

International co-operation should help countries create their own cultural expression:

International co-operation and solidarity should be aimed at enabling countries, especially developing countries, to create and strengthen their means of cultural expression, including their cultural industries, whether nascent or established, at the local, national and international levels.

The issue has already been addressed by the Council of Europe. In its *Recommendation Rec (2006) 3 on the UNESCO Convention on the protection and promotion of the diversity of cultural expressions*,⁵⁰ the Committee of ministers “welcomes the adoption by the General Conference

43. Article 10, paragraph 2, of the European Convention on Human Rights. See also Council of Europe submission to the Internet Governance Forum, *Building a free and safe Internet*, 2007.

44. EuroDIG: contributions of Dirk Kirschenowski (.berlin) and Bertrand de la Chapelle (French Ministry of Foreign and European Affairs).

45. Deutscher Bundestag, 16. Wahlperiode, Drucksache 16/4564 (7 March 2007), <http://dip21.bundestag.de/dip21/btd/16/045/1604564.pdf>.

46. EuroDIG: contribution of Sebastian Bachollet (ISOC France/ISOC ECC/Euralo).

47. Governmental Advisory Committee: *GAC principles regarding new gTLDs* (28 septembre 2007), http://gac.icann.org/web/home/gTLD_principles.pdf.

48. Wolfgang Kleinwächter, University of Aarhus (dialogue on the EuroDIG, 20-21 October in Strasbourg).

49. Convention on the Protection and Promotion of the Diversity of Cultural Expressions 2005, Paris, 20 October 2005, UNESCO.

50. *Recommendation Rec (2006)3 of the Committee of Ministers to member states on the UNESCO Convention on the protection and promotion of the diversity of cultural expressions*, adopted by the Committee of Ministers on 1 February 2006, Council of Europe.

of UNESCO of the Convention on the protection and promotion of cultural expressions". The Recommendation states that "the Council of Europe will have due regard to the provisions of the UNESCO Convention and will contribute to their implementation". It is recommended to the member states to "ratify, accept, approve or accede to the Convention on the protection and promotion of the diversity of cultural expressions".

The Recommendation CM/Rec (2007) 16 on measures to promote the public service value of the Internet⁵¹ states that:

Member states are encouraged to ensure that Internet and ICT content is contributed by all regions, countries and communities so as to ensure over time representation of all peoples, nations, cultures and languages, in particular by [...] encouraging and promoting the growth of national or local cultural industries, especially in the field of digital content production, including that undertaken by public service media, where necessary crossing linguistic and cultural barriers (including all potential content creators and other stakeholders), in order to encourage linguistic diversity and artistic expression on the Internet and other new communication services.

ICANN states in its Bylaws that "seeking and supporting broad, informed participation reflecting the functional, geographic, and cultural diversity of the

Internet at all levels of policy development and decision-making" is part of its mission. In ICANN's strategic plan 2008-2011, the introduction of Internationalised Domain Names (IDNs) at the top level is referred to as a "major priority for ICANN".

ccTLD registries have been implementing IDN since 2000.⁵² Compared to ccTLD registries, gTLD registries have higher restrictions on IDN implementations, as they need to follow the IDN Guidelines set by ICANN.⁵³ To implement IDNs, web browsing and compatibility of software applications and e-mail systems also need to be considered.⁵⁴

In its report (2005), the Working Group on Internet Governance underlined the need for further development of policies and procedures for generic top-level domain names (gTLDs), noting the "lack of international co-ordination."⁵⁵

At the second IGF in Rio de Janeiro in November 2007, UNESCO, ITU and ICANN organised a joint workshop on "Multilingualism in Cyberspace" where the three organisations committed themselves to co-operate in developing international standards for building a truly multilingual Internet including Internationalised Domain Names (IDNs).

1.4.1.2 ccTLD⁵⁶

1.4.1.2.1 Authority over ccTLDs

Distribution of ccTLDs is organised by IANA. However, IANA is not in the business of deciding what is and what is not a country, nor what code letters are appropriate for a particular country. Instead, IANA employs a neutral list of two-letter codes maintained by the ISO 3166 Maintenance Agency. The only way to enter a new country name into ISO 3166-1 is to have it registered in one of the following two sources: United Nations Terminology Bulletin *Country Names* or *Country and Region Codes for Statistical Use* of the UN Statistics Division.

ccTLDs are under national jurisdiction for the definition of their policies and legal responsibilities. ccTLD registries have different status depending on the country. In some cases, ccTLDs are subject to an agreement/contract with a government or legislation and oversight mechanisms, or are government-run. In other cases, the relationship between ccTLDs and government is very informal, such as in the cases of the German .de and the British .uk. ccTLDs are responsible to the global Internet community for interoperability with the global Internet through relationships with, *inter alia*, ICANN, Regional Internet Registries, other TLDs, or the Internet Engineering Task Force.⁵⁷

ICANN's mission with respect to ccTLD Registries is to co-ordinate the Internet's systems of top-level domain unique identifiers, and to ensure their stable and secure operation, in particular: the allocation and assignment of the sets of unique Internet identifiers, the operation and evolution of the root name server system, and the policy development related to these technical functions.

Although a majority of ccTLDs managers lack a formal agreement with ICANN, some ccTLDs have entered into or are in the process of formalising their relationship with ICANN. They do this by entering into "Accountability Frameworks", which list the set of responsibilities of both the ccTLD and ICANN or by a less formal "exchange of letters" whereby each party recognises its respective responsibilities.⁵⁸

Advisory Committee

The Country-Code Names Supporting Organization (ccNSO) is responsible for developing and recommending to the Board global policies relating to country-code top-level domains, nurturing consensus across the ccNSO's community, including the name-related activities of ccTLDs, and co-ordinating with other ICANN Supporting Organisations, committees, and constituencies under ICANN.

51. See Appendix II for the whole Recommendation.

52. Subbiah, S. (2005): IDN *Global Deployment – The Wider History and Status*. IDN Workshop ICANN Vancouver, <http://www.icann.org/en/announcements/idn-global-deployment-17nov05.pdf>.

53. The actual version of the guidelines can be found on ICANN Website: <http://www.icann.org/en/general/idn-guidelines-14nov05.htm>.

54. OECD (2006): *Working Party on Telecommunication and Information Services Policies: Evolution in the Management of Country Code Top-Level Domain Names (ccTLDs)*, DSTI/ICCP/TISP(2006)6/FINAL

55. Report of the Working Group on Internet Governance, op.cit.

56. For the whole part see ICANN Bylaws, op.cit.

57. *Evolution in the Management of Country Code Top-Level Domain Names (ccTLDs)*, op.cit.

58. *ibid*.

The ccNSO consist of (i) ccTLD managers and (ii) a ccNSO Council responsible for managing the policy-development process of the ccNSO. The ccNSO Council consist of (a) three ccNSO Council members selected by the ccNSO members within each of *ICANN's Geographic Regions*; (b) three ccNSO Council members selected by the ICANN Nominating Committee; (c) liaisons and (d) observers.

Decision-making

The ccNSO Council can make recommendation. In the event that more than 66% of the votes cast by ccNSO Members during the voting period are in favour of the Supplemental Recommendation that recommendation shall be conveyed to ICANN's Board as the ccNSO Supplemental Recommendation, and the Board shall adopt the recommendation unless by a vote of more than 66% of the Board determines that acceptance of such policy would constitute a breach of the fiduciary duties of the Board to the Company.

1.4.1.2.2 ccTLDs as critical Internet resources

1.4.1.2.2.1 No common governance of ccTLDs

There are only some principles and guidelines for the delegation of the country code Top Level Domain which have been adopted by the GAC: A general principle states that "the Internet naming system is a public resource in

the sense that its functions must be administered in the public or common interest". This should be ensure by "the relevant government or public authority (...) within the framework of its national public policy and relevant laws and regulations." The GAC principles further specify that the ccTLD manager "has a duty to serve the local Internet community as well as the global Internet community." These principles are not binding and there is no international framework regulating the country code Top Level Domain policies.

1.4.1.2.2.2 ccTLD distribution

Even if the distribution of ccTLDs is well-regulated, it is also an important policy issue. A country's top-level domain represents the national or territorial interests of a domain, and is often viewed as the flagship of a country's Internet participation and as a strategic asset with symbolic, socio-economic and/or Internet stability and security implications. Recently, the Flemish Parliament was asking for its own top-level-Domain .vla, a short-cut of "vlaanders". Catalonia, as a cultural community, has been granted its own domain .cat. However, even if granted as a gTLD on cultural grounds, rather than a ccTLD, for certain communities having their own TLD could be sensed as a first step toward or vocation for independence. In this context, distribution of TLDs becomes a highly important public policy issue.

1.4.2 Internet protocol

The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. As communication platforms converge towards using the Internet Protocol (IP), IP addresses are crucial to the scalability of the Internet and thus to the continued growth of the Internet econ-

omy, as all devices connected to the Internet need IP addresses to communicate. Currently there are two types of Internet Protocol addresses in active use: IP version 4 (IPv4) and IP version 6 (IPv6). IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users or connected devices. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

1.4.2.1 Authority over Internet protocol

The Internet Assigned Numbers Authority (IANA) is responsible for global co-ordination of the Internet Protocol addressing systems, as well as the Autonomous System Numbers used for routing Internet traffic. These functions are performed by ICANN staff under contract with the United States Government's Department of Commerce.⁵⁹

Users are assigned IP addresses by Internet service providers (ISPs). ISPs obtain allocations of IP addresses from a local Internet registry (LIR) or national Internet registry (NIR), or from their appropriate Regional Internet Registry (RIR). There are currently five RIRs: AfriNIC, APNIC, ARIN, LACNIC and RIPE NCC.⁶⁰

Regional Internet Registries (RIRs) manage, distribute, and register public Internet Number Resources within their respective regions.⁶¹ ICANN delegates Internet resources to the RIRs, which then allocate the resources within their regions. Internet Number Resources (IP addresses and AS Numbers) are distributed in a hierarchical way. ICANN, in performance of the IANA functions contract, allocates blocks of IP address space to RIRs. RIRs allocate IP address space and Autonomous System Numbers to Local Internet Registries (LIRs), such as ISPs or enterprises, that assign these resources to the end users.⁶²

59. IANA contract, <http://www.icann.org/en/general/iana-contract-14aug06.pdf>.

60. The Réseaux IP Européens/Network Coordination Centre (RIPE NCC) is the Regional Internet Registry (RIR) for Europe, the Middle East and parts of Central Asia.

61. Ripe NCC, Internet Ressource Administration, <http://www.ripe.net/info/resource-admin/index.html>.

62. *Internet Traffic Exchange. Market Developments and Measurement of Growth*, op.cit.

1.4.2.2 Internet protocol as a critical Internet resource

1.4.2.2.1 IP allocation

Over 85% of the total four billion IPv4 address blocks are already allocated and expectations are that the current pool of unallocated IP version 4 address blocks will be depleted within the next few years. Deploying the newer IP version 6 address blocks is necessary to enable growth in use of the Internet. But making the switch is difficult and it takes time and resources as well as a commitment by all stakeholders, including governments.⁶³

There is a historical geographical imbalance in the allocation of IPv4 addresses.⁶⁴ The problem was also

pointed out by the ITU in a report regarding concerns about IPv6 distribution: “It is important to ensure that no such geographical imbalance makes its way into allocation of IPv6 addresses. In particular, “first come, first served” methods are not the best”.⁶⁵

1.4.2.2.2 IPv4 to IPv6 transition

When the Internet was first implemented, every connection to a particular network allowed to reach all of the other networks on the Internet using IP version 4 address space. But in today’s terms, IPv6 is not uniformly implemented.

Table 3: Root name servers

A	VeriSign	IPv6
B	USC-ISI	IPv6
C	Cogent Communications	
D	University of Maryland	
E	NASA	
F	ISC	IPv6
G	Defense Information Systems Agency	
H	US Army Research Lab	IPv6
I	Autonomica	
J	VeriSign	IPv6
K	RIPE NCC	IPv6
L	ICANN	IPv6
M	WIDE Project	IPv6

Source: Root Server Technical Operations Association, <http://www.root-servers.org/>.

The problem is that this new protocol is not backwards compatible with the old Internet protocol.⁶⁶ To date, there seems to be a lack of awareness concerning the transition from IPv4 to IPv6. In its “*Plan Numérique 2012*”, the French authorities recognised the delay of IPv6 deployment due to its lack of immediate benefits for industrial actors. There shall be a progressive transition to IPv6, introduced step-by-step.⁶⁷ In Sweden, the Telecom Agency is promoting IPv6 in discussion with ISPs. The transition has already started.⁶⁸ Measures in

encouraging IPv6 transition are also taken by RIPE NCC, the European Internet Registry.⁶⁹

1.4.2.2.3 IPv6 in the future

The sheer scale and complexity of nomadic computing and the Internet of Things will place the existing Internet architecture under strain. It is not yet certain that there will be the spectrum resources to connect this number of tagged objects, sensors and other smart devices, nor that, unless the transition to IPv6 runs smoothly, there will be enough addresses for all these objects.⁷⁰

1.5 Internet as a critical resource

1.5.1 Definition

Stable, secure and ongoing functioning of the Internet is crucial in order to protect the fundamental right of freedom of expression. Furthermore, functioning of the Internet is also crucial for providing other services,

such as health care or security services. Internet as a whole needs to be protected as a critical resource. In its *Green Paper on a European Programme for Critical Infrastructure Protection*,⁷¹ European Commission defined

63. *The Future on the Internet Economy*, op.cit.

64. *Report of the Working Group on Internet Governance*, op.cit.

65. International Telecommunication Union (2006): *Report of the Ad-Hoc Group regarding concerns about IPv6 distribution and allocation strategy from the public policy point of view* (Temporary Document), http://www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0003MSWE.doc.

66. Internet Governance Forum (2007), Workshop on critical Internet resources. Transcription, http://www.intgovforum.org/Rio_Meeting/IGF2-Critical%20Internet%20Resources-12NOV07.txt.

67. *Plan Numérique 2012*, op.cit.

68. EuroDIG: contribution by Anders Johanson (The Swedish Post and Telecom Agency).

69. EuroDIG: contribution by Roland Perry (RIPE NCC).

70. *Connecting Europe at High Speed: National Broadband Strategies*, op.cit.

critical infrastructure as follows: "Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments." Critical infrastructure (CI) can be damaged, destroyed or disrupted by deliberate acts of

terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. Even if the Internet is not physical, it is a critical infrastructure in the sense that it is also important for other critical infrastructures and that its dysfunction could also have serious impacts on those infrastructures.

1.5.2 Internet as a critical resource: risks

1.5.2.1 Cyber attacks

There is in fact a risk of hacking the critical national infrastructure. The most noteworthy European hacking attack has been the denial-of-service attack on Estonia in April/May 2007. The crisis unleashed a wave of so-called DDoS, or Distributed Denial of Service, attacks, where websites were suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers running the sites. The main targets have been the websites of government, political parties, news organisations and

banks. The attack was relatively small: they were only of the order of 90Mbits/s. The real problem was that Estonia had a fairly low-bandwidth infrastructure and a lack of experience in dealing with DDoS attacks.⁷² These facts confirm the need of a multi-stakeholder approach, including the owners and operators of infrastructure, regulators, professional bodies and industry associations in co-operation with all levels of government, and the public.

1.5.2.1 Technical risks

There is also a risk of technical failure. Technical failure on the Internet could also have severe impact on other parts of the critical national infrastructure such as finance, food and health. One example: The Buncefield oil refinery explosion in December 2005 severely damaged a Northgate Information Solutions building, taking out systems for over 200 different customers, including payroll systems for over 180 clients and patient administration systems for hospitals.⁷³ Reportedly, an Internet failure in Duisburg in Germany, led to significant delays in the payment of unemployment benefits which had to be re-organised manually.⁷⁴

However, technical failure can also occur at an international level, involving more than one state. On 30 January 2008, India and other countries such as Egypt, Saudi Arabia and Sri Lanka suffered from an Internet disruption from a cable failure. The problem was traced to two submarine cable systems in the Mediterranean between Alexandria, Egypt and Palermo in Italy that were cut. According to Egyptian officials, around 70% of the country's online traffic was blocked. In Mumbai, officials said that more than half of India's Internet capacity had been erased. Due to the lack of alternative routes for Internet traffic, only a small proportion of users were managing to get online.⁷⁵ Disrup-

tions extended to a number of Middle East countries and their telephone communications with Europe and the US.

In Sweden, the state (through the Swedish Post and Telecom Agency), telecom operators and the power sector have come together in different partnership projects in order to work on robustness and preparedness issues in electronic communication in the event of severe disruptions. The partnership is based on volunteer participation. It is a public-private partnership where both parties are willing to venture resources.⁷⁶ The Swedish experience will be discussed during the IGF in Hyderabad in a Forum called "Public-Private Partnership – Swedish experience of establishing Robust Electronic Communication networks".

In the European Union, the access, interconnection and interoperability of electronic communication services has been addressed in a *Directive on access to, and interconnection of, electronic communications networks and associated facilities* (2002).⁷⁷

The aim of the Directive is to:

establish a regulatory framework, in accordance with internal market principles, for the relationships between suppliers of networks and services that will result in sustainable competition, interoperability of electronic communications services and consumer benefits.

71. Commission of the European Communities: Green Paper on a European Programme for Critical Infrastructure Protection, COM (2005) 576 final, 17 November 2005, Brussels.

72. Traynor, Ian, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, 17 March 2007, <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.

73. Security economics and the internal market, op.cit.

74. EuroDIG: contribution by Anette Mühlberg (United Services Union (ver.di), ALAC / ICANN).

75. Johnson, Bobby, "Faulty cable blacks out Internet for millions", *The Guardian*, 31 January 2008; Shahine, Alaa, "Internet disrupted in Egypt and India", *Reuters*, 30 January 2008.

76. EuroDIG: contribution by Anders Johanson (The Swedish Post and Telecom Agency).

77. Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities.

[...] National regulatory authorities shall ... encourage and where appropriate ensure ... adequate access and interconnection, and interoperability of services, exercising their responsibility in a way that promotes efficiency, sustainable competition, and gives the maximum benefit to end-users. In particular ... national regulatory authorities shall be able to impose: (a) to the extent that is necessary to ensure end-to-end connectivity, obligations on undertakings that control access to end-users, including in justified cases the obligation to interconnect their networks where this is not already the case;

When imposing obligations on an operator to provide access ... national regulatory authorities may lay down technical or operational conditions to be met by the provider and/or beneficiaries of such access, in accordance

with Community law, where necessary to ensure normal operation of the network.

The examples clearly show the relevance of the issue. However, in protecting the Internet as a critical infrastructure, there is a need for multi-stakeholder co-operation on a global level. This has been recognised by the European Union in 2004 that agreed a European Programme for Critical Infrastructure Protection (EPCIP) and a Critical Infrastructure Warning Information Network (CIWIN). The European Union want to develop a common approach in protecting critical infrastructure, including participation of all stakeholders. This also shows the need for interstate co-operation.

1.5.2.3 Internet in case of interstate conflict

Risks could also arise in case of interstate conflict. States in conflict could try to block each other's Internet access or to block access to certain domains or content. A recent example was the conflict between the Russian Federation and Georgia. Allegedly, measures taken in those countries also had an impact on Internet access in at least another country, i.e. Armenia. Armenia is connected to the Web principally through a fibre optic line that runs through Georgian and Russian territory on its

way to an upstream Ukrainian provider. During the conflict between Russia and Georgia, Georgia blocked access on the domain name .ru. Russia allegedly also interfered with the traffic passing through Georgia. Reportedly, the conflict had severe impact on Internet access in Armenia. Alternative Internet access routes for Armenia pass through Turkey and Iran which, it has been alleged, also involve some degree of content filtering.

Part 2. Internet protection in international law

2.1 Internet as a global resource

Internet is a critical resource. In order to make it sustainable, robust, secure and stable, it is necessary to protect it in the same way that other critical common resources are protected. In a Council of Europe context, co-operation of all states is necessary to ensure the optimal utilisation and adequate protection of the Internet. Co-operation may also imply a joint management mechanism involving public-private partnership. There is also a need for planning the sustainable development of the Internet. Internet has an impact on climate change: It is estimated that the ICT industry alone produces CO₂ emissions that is equivalent to the carbon output of the entire aviation industry. It is also estimated that ICT energy consumption and emissions will grow faster than any sector in society, doubling by 2010. This is a huge challenge for the operation and the use of the Internet.⁷⁸ Measures taken in one state relating to the Internet could also have serious implications on other states. There is a need for close communication between states concerning planned measures. Key governance attributes should include the prevention and/or mitigation of harmful conditions as well as the mutual obligations of states not to cause significant harm.

Inspiration can be drawn from international law relating to certain natural common resources. Water and the associated state responsibility are governed by international law. Like water, Internet can be considered a global resource requiring global protection using international law. One example is the UN *Convention on the Law on the non-navigational Uses of International Watercourses* (1997).⁷⁹ The objective of the Convention is the reasonable use of international watercourse for all states concerned.

Article 5 (Equitable and reasonable utilisation and participation) stipulates:

1. Watercourse States shall in their respective territories utilise an international watercourse in an equitable and reasonable manner. In particular, an international watercourse shall be used and developed by watercourse States with a view to attaining optimal and sustainable utilisation thereof and benefits therefrom, taking into account the interests of the watercourse States concerned, consistent with adequate protection of the watercourse.

2. Watercourse States shall participate in the use, development and protection of an international watercourse in an equitable and reasonable manner. Such participation includes both the right to utilise the watercourse and the duty to co-operate in the protection and development thereof, as provided in the present Convention.

The Convention also fixes the mutual obligation of states (Article 7, Obligation not to cause significant harm):

1. Watercourse States shall, in utilising an international watercourse in their territories, take all appropriate measures to prevent the causing of significant harm to other watercourse States.

2. Where significant harm nevertheless is caused to another watercourse State, the States whose use causes such harm shall, in the absence of agreement to such use, take all appropriate measures, having due regard for the provisions of Articles 5 and 6, in consultation with the affected State, to eliminate or mitigate such harm and, where appropriate, to discuss the question of compensation.

This obligation is specified in Article 27 (Prevention and mitigation of harmful conditions):

Watercourse States shall, individually and, where appropriate, jointly, take all appropriate measures to prevent or mitigate conditions related to an international watercourse that may be harmful to other watercourse States, whether resulting from natural causes or human conduct, such as flood or ice conditions, water-borne diseases, silta-

78. A workshop on "Internet and Climate Change" will take place at the IGE. Further information see: http://www.intgovforum.org/cms/workshops_08/showmelist.php?mem=85.

79. Convention on the Law on the non-navigational Uses of International Watercourses, adopted by the General Assembly of the United Nations on 21 May 1997. Not yet in force.

tion, erosion, salt-water intrusion, drought or desertification.

To attain the objective of the Convention, there is a general obligation to co-operate (Article 8):

1. Watercourse States shall co-operate on the basis of sovereign equality, territorial integrity, mutual benefit and good faith in order to attain optimal utilisation and adequate protection of an international watercourse.
2. In determining the manner of such co-operation, watercourse States may consider the establishment of joint mechanisms or commissions, as deemed necessary by them, to facilitate co-operation on relevant measures and procedures in the light of experience gained through co-operation in existing joint mechanisms and commissions in various regions.

The optimal utilisation and adequate protection of an international watercourse may imply a joint management mechanism (Article 24):

1. Watercourse States shall, at the request of any of them, enter into consultations concerning the management of an international watercourse, which may include the establishment of a joint management mechanism.
2. For the purposes of this article, "management" refers, in particular, to:
 - (a) Planning the sustainable development of an international watercourse and providing for the implementation of any plans adopted; and
 - (b) Otherwise promoting the rational and optimal utilisation, protection and control of the watercourse.

All measures taken should be taken in consideration of the implications which the measures could have on another state. There should be close communication between states concerning planned measures:

2.2 Internet protection against technical risks

Equal and reasonable utilisation and participation of Internet also strongly depend on technical aspects. Technical incidents and/or accidents in one part of the Internet can have important implications on other parts on the Internet. There is need for the prevention of technical accidents causing transboundary effects on the Internet. In order to protect Article 10 of the Convention, states should have a responsibility in guaranteeing access to the Internet. This responsibility should include the protection of Internet infrastructure against technical incidents or accidents.

In this context, the Internet is comparable to other fields, such as industrial accidents arising from hazardous activities. This subject has been addressed in the 1992 *Convention on the Transboundary Effects of Industrial Accidents*.⁸⁰ The Convention shall:

apply to the prevention of, preparedness for and response to industrial accidents capable of causing transboundary effects, including the effects of such accidents caused by natural disasters, and to international co-operation concerning mutual assistance, research and development, exchange of information and exchange of technology in the area of prevention of, preparedness for and response to industrial accidents (Article 2).

Article 11 (Information concerning planned measures):

Watercourse States shall exchange information and consult each other and, if necessary, negotiate on the possible effects of planned measures on the condition of an international watercourse.

Article 12 (Notification concerning planned measures with possible adverse effects):

Before a watercourse State implements or permits the implementation of planned measures which may have a significant adverse effect upon other watercourse States, it shall provide those States with timely notification thereof. Such notification shall be accompanied by available technical data and information, including the results of any environmental impact assessment, in order to enable the notified States to evaluate the possible effects of the planned measures.

More than 20 states, among them 8 member states of the Council of Europe, signed the Convention on the Law on the non-navigational uses of international watercourses i.e. Germany, Norway, Portugal, Finland, the Netherlands, Sweden, Hungary and Luxembourg. Several of them share international watercourses: Norway and Finland share the Tana river, which runs for 256 km along the Finnish-Norwegian border; Finland and Sweden share the border river Torneälvi; Germany shares the border river Mosel with Luxembourg and also the Rhine with the Netherlands. Like international watercourses, Internet connections transit through different countries. International water protection could thus serve as an example for Internet protection.

States have a responsibility in protecting human beings and environment against industrial accidents:

Article 3.1. The Parties shall, taking into account efforts already made at national and international levels, take appropriate measures and co-operate within the framework of this Convention, to protect human beings and the environment against industrial accidents by preventing such accidents as far as possible, by reducing their frequency and severity and by mitigating their effects. To this end, preventive, preparedness and response measures, including restoration measures, shall be applied.

2. The Parties shall, by means of exchange of information, consultation and other co-operative measures and without undue delay, develop and implement policies and strategies for reducing the risks of industrial accidents and improving preventive, preparedness and response measures, including restoration measures, taking into account, in order to avoid unnecessary duplication, efforts already made at national and international levels.

States also shall induce measures taken by operators with a view to preventing industrial risks (Article 6, Prevention):

1. The Parties shall take appropriate measures for the prevention of industrial accidents, including measures to induce action by operators to reduce the risk of industrial

80. *Convention on the Transboundary Effects of Industrial Accidents* (1992), United Nations Economic Commission for Europe.

accidents. Such measures may include, but are not limited to those referred to in Annex IV hereto.

2. With regard to any hazardous activity, the Party of origin shall require the operator to demonstrate the safe performance of the hazardous activity by the provision of information such as basic details of the process, including but not limited to, analysis and evaluation as detailed in Annex V hereto.

Article 7 points out the responsibility of States in establishing policies:

Within the framework of its legal system, the Party of origin shall, with the objective of minimising the risk to the population and the environment of all affected Parties, seek the establishment of policies on the siting of new hazardous activities and on significant modifications to existing hazardous activities. Within the framework of their legal systems, the affected Parties shall seek the establishment of policies on significant developments in areas which could be affected by transboundary effects of an industrial accident arising out of a hazardous activity so as to minimise the risks involved.

Article 8.1 relates to emergency preparedness:

The Parties shall take appropriate measures to establish and maintain adequate emergency preparedness to respond to industrial accidents. The Parties shall ensure

that preparedness measures are taken to mitigate transboundary effects of such accidents, onsite duties being undertaken by operators. These measures may include, but are not limited to those referred to in Annex VII hereto. In particular, the Parties concerned shall inform each other of their contingency plans.

Article 12 provides for mutual assistance:

If a Party needs assistance in the event of an industrial accident, it may ask for assistance from other Parties, indicating the scope and type of assistance required. A Party to whom a request for assistance is directed shall promptly decide and inform the requesting Party whether it is in a position to render the assistance required and indicate the scope and terms of the assistance that might be rendered (12.1).

This Convention applies to activities involving hazardous substances. However, there are some analogies with critical Internet resources. The aim of the Convention is the protection of human beings on the global level. Citizens of one state should be protected from effects of industrial accidents in another state. The same logic could apply to the Internet: citizens should be protected from effects that action or accident in another state could have on their Internet access.

2.3 Internet protection against cyber attacks

Due to the strong interdependency of networks, attacks on Internet are mostly cross-border or global. Even if the attack concerns only one country, it could have important repercussions on other countries. Therefore, we should deal with risk of Internet attacks at global level and also develop a common approach to protection.

The issue has partly been addressed by the Council of Europe in its Convention on Cybercrime.⁸¹ Three objectives are addressed by the Convention:

- Harmonise national law at European level;
- Complete legislation in procedural matters;
- Enforce international co-operation (regarding extradition and criminalisation).

The Convention also include some "General principles relating to mutual assistance" in case of "the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence" (Article 25).

In their global structure, cyber attacks are comparable to terrorism. The common prevention of terrorism has been addressed, *inter alia*, in the *International Convention for the Suppression of the Financing of Terrorism*.⁸²

States Parties shall co-operate in the prevention of the offences set forth in Article 2 by taking all practicable measures, *inter alia*, by adapting their domestic legisla-

tion, if necessary, to prevent and counter preparations in their respective territories for the commission of those offences within or outside their territories. (...)

States Parties shall further co-operate in the prevention of the offences set forth in Article 2 by exchanging accurate and verified information in accordance with their domestic law and co-ordinating administrative and other measures taken, as appropriate, to prevent the commission of offences set forth in Article 2 (...) (Article 18).

Reference could also be made in this context to the Council of Europe *Convention on the Prevention of Terrorism* (2005)⁸³ which states that:

Parties shall, as appropriate and with due regard to their capabilities, assist and support each other with a view to enhancing their capacity to prevent the commission of terrorist offences, including through exchange of information and best practices, as well as through training and other joint efforts of a preventive character. (Article 4)

Like this Convention on preventing terrorism, there is a need for a common approach in preventing cyberattacks on critical Internet resources. In order to ensure security, critical infrastructure should be protected with the aid of international instruments. Weak points should be identified and remedial action should be taken. Because of the global character of the Internet infrastructure, measures should at least be taken at a European level, possibly with global vocation.

81. Convention on Cybercrime, Budapest, 23 November 2001, Council of Europe.

82. International Convention for the Suppression of the Financing of Terrorism, Adopted by the General Assembly of the United Nations on 9 December 1999.

83. Convention on the Prevention of Terrorism, Warsaw, 16 May 2005, Council of Europe.

2.4 Internet protection in case of interstate conflict

Protecting critical infrastructure in times of crisis is important in terms of security and stability of a country. Internet is comparable to other critical resources, as for example gas: In 2006, Gazprom, the world's largest natural gas producer, suspended shipments of natural gas to Ukraine in the middle of winter. This disruption also had an impact on Western Europe because 80% of the supplies that Gazprom furnishes to Western Europe transit via Ukrainian territory. Like gas, Internet can be seen as a public service (basic necessity) and critical infrastructures carrying such commodities or ensuring the service need to be protected in order to ensure stability and security in a state.

From a Council of Europe perspective, the protection of the Internet in times of crisis would be important in order to ensure the right to freedom of expression, as stated in Article 10 of the Convention.

The issue has been addressed by the 7th Ministerial Conference on Mass Media Policy in its Resolution No. 1 on the Freedom of expression and information in times of crisis. The Ministers,

Affirming that freedom of expression and information and media freedom must be respected in crisis situations, since the public's right to be informed about the actions of public authorities and all other parties involved in order to keep them under scrutiny is especially important in these situations,

Reaffirm their determination to ensure in times of crisis respect for freedom of expression and information as a basic element of a democratic and pluralist society;

Agree to promote in any other international instances where questions concerning freedom of expression and information during times of crisis might be addressed, the democratic principles established in this field within the Council of Europe.

However, this fundamental right is not expressly translated by international law at present to the Inter-

net. It would nonetheless be possible to rely on certain international law principles in this context.

Some main principles could be derived from the *Hel-sinki Final Act* (1975) of OSCE, in the Declaration on Principles Guiding Relations between Participating States, even if they are not binding:

The participating States recognise the universal significance of human rights and fundamental freedoms, respect for which is an essential factor for the peace, justice and wellbeing necessary to ensure the development of friendly relations and co-operation among themselves as among all States.

They will constantly respect these rights and freedoms in their mutual relations and will endeavour jointly and separately, including in co-operation with the United Nations, to promote universal and effective respect for them.

Express their intention in particular:

To facilitate the improvement of the dissemination, on their territory, of newspapers and printed publications, periodical and non-periodical, from the other participating States.

To contribute to the improvement of access by the public to periodical and non-periodical printed publications imported on the bases indicated above.

To promote the improvement of the dissemination of filmed and broadcast information.

Reference could also be made in this context to Article 10 ECHR ("regardless of frontiers") and to the Council of Europe Convention on Transfrontier Television.

Except to the extent that the above-mentioned declaration and instruments apply, Internet protection in times of crisis is not ensured by international law. We need to address the issue in order to protect the right to freedom of expression also in case of interstate conflict.

Conclusion

Internet is a critical infrastructure which needs to be protected in order to ensure security, stability and the protection of Human rights in a country. Internet is a transboundary, global resource. It is hence comparable to other global resources, such as water or gas. There are various risks of damage to Internet infrastructures. In case of technical incident or accident, as happened in the Mediterranean when a cable were cut. In case of interstate conflict, what has happened in respect of gas could also be done to the Internet infrastructure. The Internet is also critical in its governance: It depends on critical Internet resources which are highly important in terms of functioning and access. However, to date, in an interstate context there is no enforceable right of Internet access. The responsibility and accountability of the different stakeholders in case of technical accident or other events, which could have a serious impact on access to the Internet by a significant number of users, are not clearly defined. Regarding the responsibility of states, some principles can be derived from the text on *Responsibility of States for Internationally Wrongful Acts* (2001)⁸⁴, adopted by the International Law Commission.

Article 2 – Elements of an internationally wrongful act of a State

There is an internationally wrongful act of a State when conduct consisting of an action or omission:

- Is attributable to the State under international law; and
- Constitutes a breach of an international obligation of the State. (Article 2)

Article 31 – Reparation

- The responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act.
- Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State.

Article 49 – Object and limits of countermeasures

- An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two.
- Countermeasures are limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State.
- Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question.

However, without a definition of state responsibility, it is not clear to which extent this text applies to Internet protection. In a multi-stakeholder Internet governance model, we have to define the accountability and responsibility of all stakeholders. In order to ensure the protection of the Internet as a critical infrastructure at European level, there is clearly a need for multilateral co-operation. The Council of Europe has an important part to play in guaranteeing the protection of its values and standards on democracy, rule of law and human rights through Internet governance. It would be desirable to identify the relevant issues concerning the protection of critical Internet resources in order to safeguard these values. The organisation of a European Dialogue on Internet Governance (EuroDIG),⁸⁵ an IGF-like meeting at European level, was an important step in identifying European concerns in a multistakeholder approach. There is a need to explore further ways to ensure international supervision and accountability of the management of critical Internet resources that have a transnational function, and to provide advice to the various corporations, agencies and entities that manage those resources with a view to ensure that decisions take full account of international law and international human rights law.

84. *Responsibility of States for Internationally Wrongful Acts*, adopted by the International Law Commission in 2001. See Appendix III for all relevant articles of this text.

85. EuroDIG took place in Strasbourg on 20 and 21 October 2008: www.eurodig.org.

Appendix I

Extracts from international human rights law which includes Council of Europe standards related to the right to freedom of expression

International Covenant on Civil and Political Rights

Article 19

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
 - (a) For respect of the rights or reputations of others;
 - (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Convention on the Rights of the Child

Article 13

1. The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.
2. The exercise of this right may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
 - (a) For respect of the rights or reputations of others; or
 - (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.

Article 17

States Parties recognise the important function performed by the mass media and shall ensure that the child has access to information and material from a diversity of national and international sources, especially those aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health. To this end, States Parties shall:

- (a) Encourage the mass media to disseminate information and material of social and cultural benefit to the child and in accordance with the spirit of Article 29;
- (b) Encourage international co-operation in the production, exchange and dissemination of such information and material from a diversity of cultural, national and international sources;
- (c) Encourage the production and dissemination of children's books;
- (d) Encourage the mass media to have particular regard to the linguistic needs of the child who belongs to a minority group or who is indigenous;

(e) Encourage the development of appropriate guidelines for the protection of the child from informa-

tion and material injurious to his or her well-being, bearing in mind the provisions of Articles 13 and 18.

European Convention on Human Rights

Article 10 – Freedom of expression

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such for-

malities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Council of Europe standards

In its *Declaration on a European Policy for new Information Technologies* adopted 7 May 1999, the Committee of Ministers urged the Government to “encourage the free flow of information, opinions and ideas through the use of the new information technologies”; to “encourage effective international co-operation to deliver the benefits of improved access and increased transparency” and to “contribute towards equal possibilities in the use of new technologies for all European countries.”

In its *Recommendation Rec (2001) 8 on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services)*, the Committee of Ministers stressed “that the continued development of new communications and information services should serve to further the right of everyone, regardless of frontiers, to express, seek, receive and impart information and ideas for the benefit of every individual and the democratic culture of any society” and “that the freedom to use new communications and information services should not prejudice the human dignity, human rights and fundamental freedoms of others, especially of minors”.

In its *Declaration on freedom of communication on the Internet* adopted on 28 May 2003, the Committee of Ministers underlined that “freedom of expression and the free circulation of information on the Internet need to be reaffirmed”.

It recommended that “member states should foster and encourage access for all to Internet communication and information services on a non-discriminatory basis at an affordable price” and that “member states should seek measures to promote a pluralistic offer of services via the Internet which caters to the different needs of users and social groups.”

It also recommended allowing service providers “to operate in a regulatory framework which guarantees them non-discriminatory access to national and international telecommunication networks”.

In its *Recommendation Rec (2004) 15 on electronic governance*, the Committee of Ministers recommended developing an e-governance strategy which “enables and improves access to appropriate ICT infrastructure

and services that are simple and fast to use” and “ensures system availability, security, integrity and interoperability”.

In its 2005 *Declaration on Human Rights and the Rule of Law in the Information Society*, the Committee of Ministers reaffirmed “that all rights enshrined in the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) remain fully valid in the Information Age and should continue to be protected regardless of new technological developments”.

The member states reasserted that “Freedom of expression, information and communication should be respected in a digital as well as in a non-digital environment, and should not be subject to restrictions other than those provided for in Article 10 of the ECHR, simply because communication is carried in digital form”.

They recognised that “limited or no access to ICTs can deprive individuals of the ability to exercise fully their human rights”.

It was also stated that “any regulatory measure on the media and new communication services should respect and, wherever possible, promote the fundamental values of pluralism, cultural and linguistic diversity, and non-discriminatory access to different means of communication”.

In its *Recommendation CM/Rec (2007) 11 on promoting freedom of expression and information in the new information and communications environment*, the Committee of Ministers were “mindful of the potential impact, both positive and negative, that information and communication technologies and services can have on the enjoyment of human rights and fundamental freedoms in the information society and the particular roles and responsibilities of member states in securing the protection and promotion of those rights”.

It underlined “in this connection, that the development of information and communication technologies and services should contribute to everyone’s enjoyment of the rights guaranteed by Article 10 of the ECHR, for the benefit of each individual and the democratic culture of every society”.

The Committee of Ministers stressed the “importance of free or affordable access to content and services in view of the convergence of the media and new communication service sectors and the emergence of common platforms and services between telecommunication operators, hardware and software manufacturers, print, electronic and new communication service outlets, Internet service providers and other next generation network operators”.

It also stressed the need “for member states to constantly examine and review the legal and regulatory framework within which stakeholders operate, which impacts on the exercise and enjoyment of human rights and fundamental freedoms.”

Member states recommended “that the governments of member states take all necessary measures to promote the full exercise and enjoyment of human rights and fundamental freedoms in the new information and communications environment, in particular the right to freedom of expression and information pursuant to Article 10 of the ECHR and the relevant case-law of the European Court of Human Rights”.

In point III of the relating guidelines is stated that “affordable access to ICT infrastructure is therefore a prerequisite for affordable access to the Internet, thereby helping to bridge the digital divide, in order to maximise the enjoyment of these rights and freedoms.”

In this connection, member states, in co-operation with the private sector and civil society, are “encouraged to promote and enhance access to ICT infrastructure by:

- i. creating an enabling environment that is attractive for the private sector to invest in ICT infrastructure and services, including a stable legal and regulatory framework;
- ii. facilitating and promoting community based networks;
- iii. facilitating policies and partnerships which promote the qualitative and quantitative development of ICT infrastructure with a view to ensuring universal and affordable access to the Internet;
- iv. reviewing and creating universal service obligations, taking into account, *inter alia*, converging next generation networks.”

Resolution No. 3 of the 7th Ministerial Conference on Mass Media Policy states:

“Determined to ensure that the development of the Information Society in Europe will be based on respect for human rights and the rule of law through concerted action by public authorities and civil society,

Reaffirm their commitment, in line with the principles of the *Declaration on freedom of communication on the Internet* adopted by the Committee of Ministers on 28 May 2003, to remove, when technically feasible, any

hindrances to the free flow of information through new communication services;

Undertake to step up efforts to ensure an effective and equitable access for all individuals to the new communication services, skills and knowledge, especially with a view to preventing digital exclusion, as well as to encourage media education for the general public.”

Appendix II

Recommendation CM/Rec (2007) 16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet

(Adopted by the Committee of Ministers on 7 November 2007 at the 1010th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve greater unity between its members for the purpose of safeguarding and realising the ideals and principles which are their common heritage;

Recalling that States Parties to the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights – ETS No. 5) have undertaken to secure to everyone within their jurisdiction the human rights and fundamental freedoms defined in the Convention;

Mindful of the particular roles and responsibilities of member states in securing the protection and promotion of these rights and freedoms;

Noting that information and communication technologies (ICTs) can, on the one hand, significantly enhance the exercise of human rights and fundamental freedoms, such as the right to freedom of expression, information and communication, the right to education, the right to assembly, and the right to free elections, while, on the other hand, they may adversely affect these and other rights, freedoms and values, such as the respect for private life and secrecy of correspondence, the dignity of human beings and even the right to life;

Concerned by the risk of harm posed by content and communications on the Internet and other ICTs as well as by the threats of cybercrime to the exercise and enjoyment of human rights and fundamental freedoms, and recalling in this regard the *Convention on Cybercrime* (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) and the specific provisions in the Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (CETS No. 201);

Aware that communication using new information and communication technologies and services must respect the right to privacy as guaranteed by Article 8 of the European Convention on Human Rights and by the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), and as elaborated by Recommendation No. R (99) 5 of the Committee of Ministers to member states on the protection of privacy on the Internet;

Noting that the outcome documents of the World Summit on the Information Society (WSIS) (Geneva 2003 – Tunis 2005) recognise the right for everyone to benefit from the information society and reaffirmed the desire and commitment of participating states to build a people-centred, inclusive and development-oriented information society, respecting fully and upholding the Universal Declaration of Human Rights, as well as the universality, indivisibility, interdependence and interrelation of all human rights and fundamental freedoms, including the right to development;

Convinced that access to and the capacity and ability to use the Internet should be regarded as indispensable for the full exercise and enjoyment of human rights and fundamental freedoms in the information society;

Recalling the 2003 UNESCO *Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace*, which calls on member states and international organisations to promote access to the Internet as a service of public interest;

Recalling the 2005 UNESCO *Convention on the Protection and Promotion of the Diversity of Cultural Expressions*, which states that freedom of thought, expression and information, as well as diversity of the media, enable cultural expressions to flourish within societies, and which calls on Parties to encourage individuals and social groups to create, produce, disseminate, distribute and have access to their own cultural expressions;

Aware that the media landscape is rapidly changing and that the Internet is playing an increasingly important role in providing and promoting diverse sources of information to the public, including user-generated content;

Noting that our societies are rapidly moving into a new phase of development, towards a ubiquitous information society, and therefore that the Internet constitutes a new pervasive social and public space which should have an ethical dimension, which should foster justice, dignity and respect for the human being and which should be based on respect for human rights and fundamental freedoms, democracy and the rule of law;

Recalling the currently accepted working definition of 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;

Convinced therefore that the governance of the Internet should be people-centred and pursue public policy goals which protect human rights, democracy and the rule of law on the Internet and other ICTs;

Aware of the public service value of the Internet, understood as people's significant reliance on the Internet as an essential tool for their everyday activities (communication, information, knowledge, commercial transactions) and the resulting legitimate expectation that Internet services be accessible and affordable, secure, reliable and ongoing;

Firmly convinced that the Internet and other ICT services have high public service value in that they serve to promote the exercise and enjoyment of human rights and fundamental freedoms for all who use them, and that their protection should be a priority with regard to the governance of the Internet,

Recommends that, having regard to the guidelines in the appendix to this recommendation, the governments of member states, in co-operation, where appropriate, with all relevant stakeholders, take all necessary measures to promote the public service value of the Internet by:

- upholding human rights, democracy and the rule of law on the Internet and promoting social cohesion, respect for cultural diversity and trust between individuals and between peoples in the use of ICTs, and in particular, the Internet;
- elaborating and delineating the boundaries of the roles and responsibilities of all key stakeholders within a clear legal framework, using complementary regulatory frameworks;
- encouraging the private sector to acknowledge and familiarise itself with its evolving ethical roles and responsibilities, and to co-operate in reviewing and, where necessary, adjusting its key actions and decisions which may impact on individual rights and freedoms;
- encouraging in this regard the private sector to develop, where appropriate and in co-operation with other stakeholders, new forms of open and transparent self- and co-regulation on the basis of which key actors can be held accountable;
- encouraging the private sector to contribute to achieving the goals set out in this recommendation and developing public policies to supplement the operation of market forces where these are insufficient;
- bringing this recommendation to the attention of all relevant stakeholders, in particular the private sector and civil society, so that all necessary measures are taken to contribute to the implementation of its objectives.

I. Human rights and democracy

Human rights

Member states should adopt or develop policies to preserve and, whenever possible, enhance the protection of human rights and respect for the rule of law in the information society. In this regard, particular attention should be paid to:

- the right to freedom of expression, information and communication on the Internet and via other ICTs promoted, *inter alia*, by ensuring access to them;
- the need to ensure that there are no restrictions to the abovementioned right (for example in the form of censorship) other than to the extent permitted by Article 10 of the European Convention on Human Rights, as interpreted by the European Court of Human Rights;
- the right to private life and private correspondence on the Internet and in the use of other ICTs, including the respect for the will of users not to disclose their identity, promoted by encouraging individual users and Internet service and content providers to share the responsibility for this;

- the right to education, including media and information literacy;
- the fundamental values of pluralism, cultural and linguistic diversity, and non-discriminatory access to different means of communication via the Internet and other ICTs;
- the dignity and integrity of the human being with regard to the trafficking of human beings carried out using ICTs and by signing and ratifying the Council of Europe *Convention on Action against Trafficking in Human Beings* (CETS No. 197);
- the right to the presumption of innocence, which should be respected in the digital environment, and the right to a fair trial and the principle according to which there should be no punishment without law, which should be upheld by developing and encouraging legal, and also self- and co-regulatory frameworks for journalists and media service providers as concerns the reporting on court proceedings;
- the freedom for all groups in society to participate in ICT-assisted assemblies and other forms of associative life, subject to no other restrictions than those

provided for by Article 11 of the European Convention on Human Rights as interpreted by the European Court of Human Rights;

- the right to property, including intellectual property rights, subject to the right of the state to limit the use of property in accordance with the general interest as provided by Article 1 of The Protocol to the European Convention on Human Rights (ETS No. 9).

Democracy

Member states should develop and implement strategies for e-democracy, e-participation and e-government that make effective use of ICTs in democratic process and debate, in relationships between public authorities and civil society, and in the provision of public services as part of an integrated approach that makes full and appropriate use of a number of communication channels, both online and offline. In particular, e-democracy and e-governance should uphold human rights, democracy and the rule of law by:

- strengthening the participation, initiative and involvement of citizens in national, regional and local public life and in decision-making processes, thereby contributing to more dynamic, inclusive and direct forms of democracy, genuine public debate, better legislation and active scrutiny of the decision-making processes;
- improving public administration and services by making them more accessible (*inter alia* through access to official documents), responsive, user-oriented, transparent, efficient and cost-effective, thus contributing to the economic and cultural vitality of society.

Member states should, where appropriate, consider introducing only e-voting systems which are secure,

reliable, efficient, technically robust, open to independent verification and easily accessible to voters, in line with *Recommendation Rec (2004) 11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.

Member states should encourage the use of ICTs (including online forums, weblogs, political chats, instant messaging and other forms of citizen-to-citizen communication) by citizens, non-governmental organisations and political parties to engage in democratic deliberations, e-activism and e-campaigning, put forward their concerns, ideas and initiatives, promote dialogue and deliberation with representatives and government, and to scrutinise officials and politicians in matters of public interest.

Member states should use the Internet and other ICTs in conjunction with other channels of communication to formulate and implement policies for education for democratic citizenship to enable individuals to be active and responsible citizens throughout their lives, to respect the rights of others and to contribute to the defence and development of democratic societies and cultures.

Member states should promote public discussion on the responsibilities of private actors, such as Internet service providers, content providers and users, and encourage them – in the interests of the democratic process and debate and the protection of the rights of others – to take self-regulatory and other measures to optimise the quality and reliability of information on the Internet and to promote the exercise of professional responsibility, in particular with regard to the establishment, compliance with, and monitoring of the observance of codes of conduct.

II. Access

Member states should develop, in co-operation with the private sector and civil society, strategies which promote sustainable economic growth via competitive market structures in order to stimulate investment, particularly from local capital, into critical Internet resources and ICTs, especially in areas with a low communication and information infrastructure, with particular reference to:

- developing strategies which promote affordable access to ICT infrastructure, including the Internet;
- promoting technical interoperability, open standards and cultural diversity in ICT policy covering telecommunications, broadcasting and the Internet;
- promoting a diversity of software models, including proprietary, free and open source software;
- promoting affordable access to the Internet for individuals, irrespective of their age, gender, ethnic or social origin, including the following persons and groups of persons:
 - a. those on low incomes;
 - b. those in rural and geographically remote areas; and

c. those with special needs (for example, disabled persons), bearing in mind the importance of design and application, affordability, the need to raise awareness among these persons and groups, the appropriateness and attractiveness of Internet access and services as well as their adaptability and compatibility;

- promoting a minimum number of Internet access points and ICT services on the premises of public authorities and, where appropriate, in other public places, in line with *Recommendation No. R (99) 14 of the Committee of Ministers to member states on universal community service concerning new communication services*;
- encouraging, where practicable, public administrations, educational institutions and private owners of access facilities to new communication and information services to enable the general public to use these facilities;
- promoting the integration of ICTs into education and promoting media and information literacy and training in formal and non-formal education sectors for children and adults in order to:

- a. empower them to use media technologies effectively to create, access, store, retrieve and share content to meet their individual and community needs and interests;
- b. encourage them to exercise their democratic rights and civic responsibilities effectively;
- c. encourage them to make informed choices when using the Internet and other ICTs by using and referring to diverse media forms

III. Openness

Member states should affirm freedom of expression and the free circulation of information on the Internet, balancing them, where necessary, with other legitimate rights and interests, in accordance with Article 10, paragraph 2, of the European Convention on Human Rights as interpreted by the European Court of Human Rights, by:

- promoting the active participation of the public in using, and contributing content to, the Internet and other ICTs;
- promoting freedom of communication and creation on the Internet, regardless of frontiers, in particular by:
 - a. not subjecting individuals to any licensing or other requirements having a similar effect, nor any general blocking or filtering measures by public authorities, or restrictions that go further than those applied to other means of content delivery;
 - b. facilitating, where appropriate, “re-users”, meaning those wishing to exploit existing digital content resources in order to create future content or services in a way that is compatible with respect for intellectual property rights;
 - c. promoting an open offer of services and accessible, usable and exploitable content via the Internet which caters to the different needs of users and social groups, in particular by:
 - allowing service providers to operate in a regulatory framework which guarantees them non-discriminatory access to national and international telecommunication networks;

IV. Diversity

Member states are encouraged to ensure that Internet and ICT content is contributed by all regions, countries and communities so as to ensure over time representation of all peoples, nations, cultures and languages, in particular by:

- encouraging and promoting the growth of national or local cultural industries, especially in the field of digital content production, including that undertaken by public service media, where necessary crossing linguistic and cultural barriers (including all potential content creators and other stakeholders), in order to encourage linguistic diversity and artistic expression on the Internet and other new

and content from different cultural and institutional sources; understanding how and why media content is produced; critically analysing the techniques, language and conventions used by the media and the messages they convey; and identifying media content and services that may be unsolicited, offensive or harmful.

- increasing the provision and transparency of their online services to citizens and businesses;
- engaging with the public, where appropriate, through user-generated communities rather than official websites;
- encouraging, where appropriate, the re-use of public data by non-commercial users, so as to allow every individual access to public information, facilitating their participation in public life and democratic processes;
- promoting public domain information accessibility via the Internet which includes government documents, allowing all persons to participate in the process of government; information about personal data retained by public entities; scientific and historical data; information on the state of technology, allowing the public to consider how the information society might guard against information warfare and other threats to human rights; creative works that are part of a shared cultural base, allowing persons to participate actively in their community and cultural history;
- adapting and extending the remit of public service media, in line with *Recommendation Rec (2007) 3 of the Committee of Ministers to member states on the remit of public service media in the information society*, so as to cover the Internet and other new communication services and so that both generalist and specialised contents and services can be offered, as well as distinct personalised interactive and on-demand services.

communication services. This should apply also to educational, cultural, scientific, scholarly and other content which may not be commercially viable in accordance with the 2005 *UNESCO Convention on the Protection and Promotion of the Diversity of Cultural Expressions*;

- developing strategies and policies and creating appropriate legal and institutional frameworks to preserve the digital heritage of lasting cultural, scientific, or other values, in co-operation with holders of copyright and neighbouring rights, and other legitimate stakeholders in order, where appropriate, to set common standards and ensure compatibility

and share resources. In this regard, access to legally deposited digital heritage materials, within reasonable restrictions, should also be assured;

- developing a culture of participation and involvement, *inter alia* by providing for the creation, modification and remixing of interactive content and the transformation of consumers into active communicators and creators of content;
- promoting mechanisms for the production and distribution of user- and community-generated content (thereby facilitating online communities), *inter alia*

V. Security

Member states should engage in international legal co-operation as a means of developing and strengthening security on the Internet and observance of international law, in particular by:

- signing and ratifying the Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), in order to be able to implement a common criminal policy aimed at the protection of society against cybercrime, to co-operate for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence, and to resolve jurisdictional problems in cases of crimes committed in other states parties to the convention;
- promoting the signature and ratification of the Convention and Additional Protocol by non-member states as well as their use as model cybercrime legislation at the national level, so that a worldwide interoperable system and framework for global co-operation in fighting cybercrime among interested countries emerges;
- enhancing network and information security to enable them to resist actions that compromise their stability as well as the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems;
- empowering stakeholders to protect network and information security;
- adopting legislation and establishing appropriate enforcement authorities, where necessary, to combat spam. Member states should also facilitate the development of appropriate technical solutions related to combating spam, improve education and awareness among all stakeholders and encourage industry-driven initiatives, as well as engage in cross-border spam enforcement co-operation;
- encouraging the development of common rules on the co-operation between providers of information society services and law enforcement authorities ensuring that such co-operation has a clear legal basis and respects privacy regulations;

by encouraging public service media to use such content and co-operate with such communities;

- encouraging the creation and processing of and access to educational, cultural and scientific content in digital form, so as to ensure that all cultures can express themselves and have access to the Internet in all languages, including indigenous ones;
- encouraging capacity building for the production of local and indigenous content on the Internet;
- encouraging the multilingualisation of the Internet so that everyone can use it in their own language.

- protecting personal data and privacy on the Internet and other ICTs (to protect users against the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data, or against the intrusion of their privacy through, for example, unsolicited communications for direct marketing purposes) and harmonising legal frameworks in this area without unjustifiably disrupting the free flow of information, in particular by:

- a. improving their domestic frameworks for privacy law in accordance with Article 8 of the European Convention on Human Rights and by signing and ratifying the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108);
- b. providing appropriate safeguards for the transfer of international personal data to states which do not have an adequate level of data protection;
- c. facilitating cross-border co-operation in privacy law enforcement;

- combating piracy in the field of copyright and neighbouring rights;
- working together with the business sector and consumer representatives to ensure e-commerce users are afforded transparent and effective consumer protection that is not less than the level of protection afforded in other forms of commerce. This may include the introduction of requirements concerning contracts which can be concluded by electronic means, in particular requirements concerning secure electronic signatures;
- promoting the safer use of the Internet and of ICTs, particularly for children, fighting against illegal content and tackling harmful and, where necessary, unwanted content through regulation, the encouragement of self-regulation, including the elaboration of codes of conduct, and the development of adequate technical standards and systems;
- promoting the signature and ratification of the Council of Europe *Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* (CETS No. 201).

Appendix III

Extracts from “Responsibility of States for Internationally Wrongful Acts” (2001)

Article 2 – Elements of an internationally wrongful act of a State

There is an internationally wrongful act of a State when conduct consisting of an action or omission:

(a) Is attributable to the State under international law; and

(b) Constitutes a breach of an international obligation of the State.

Article 8 – Conduct directed or controlled by a State

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the

instructions of, or under the direction or control of, that State in carrying out the conduct.

Article 23.1 – Force majeure

The wrongfulness of an act of a State not in conformity with an international obligation of that State is precluded if the act is due to force majeure, that is the occurrence of an irresistible force or of an unforeseen

event, beyond the control of the State, making it materially impossible in the circumstances to perform the obligation.

Article 31 – Reparation

1. The responsible State is under an obligation to make full reparation for the injury caused by the internationally wrongful act.

2. Injury includes any damage, whether material or moral, caused by the internationally wrongful act of a State.

Article 42 – Invocation of responsibility by an injured State

A State is entitled as an injured State to invoke the responsibility of another State if the obligation breached is owed to:

(a) That State individually; or

(b) A group of States including that State, or the international community as a whole, and the breach of the obligation:

(i) Specially affects that State; or

(ii) Is of such a character as radically to change the position of all the other States to which the obligation is owed with respect to the further performance of the obligation.

Article 48.1 – Invocation of responsibility by a State other than an injured State

Any State other than an injured State is entitled to invoke the responsibility of another State in accordance with paragraph 2 if:

(a) The obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group; or

(b) The obligation breached is owed to the international community as a whole.

Article 49 – Object and limits of countermeasures

1. An injured State may only take countermeasures against a State which is responsible for an internationally wrongful act in order to induce that State to comply with its obligations under part two.
 2. Countermeasures are limited to the non-performance for the time being of international obligations
- of the State taking the measures towards the responsible State.
3. Countermeasures shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question.

Article 50.1 – Obligations not affected by countermeasures

Countermeasures shall not affect:

- (a) The obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations;
- (b) Obligations for the protection of fundamental human rights;
- (c) Obligations of a humanitarian character prohibiting reprisals;
- (d) Other obligations under peremptory norms of general international law.

2. A State taking countermeasures is not relieved from fulfilling its obligations:

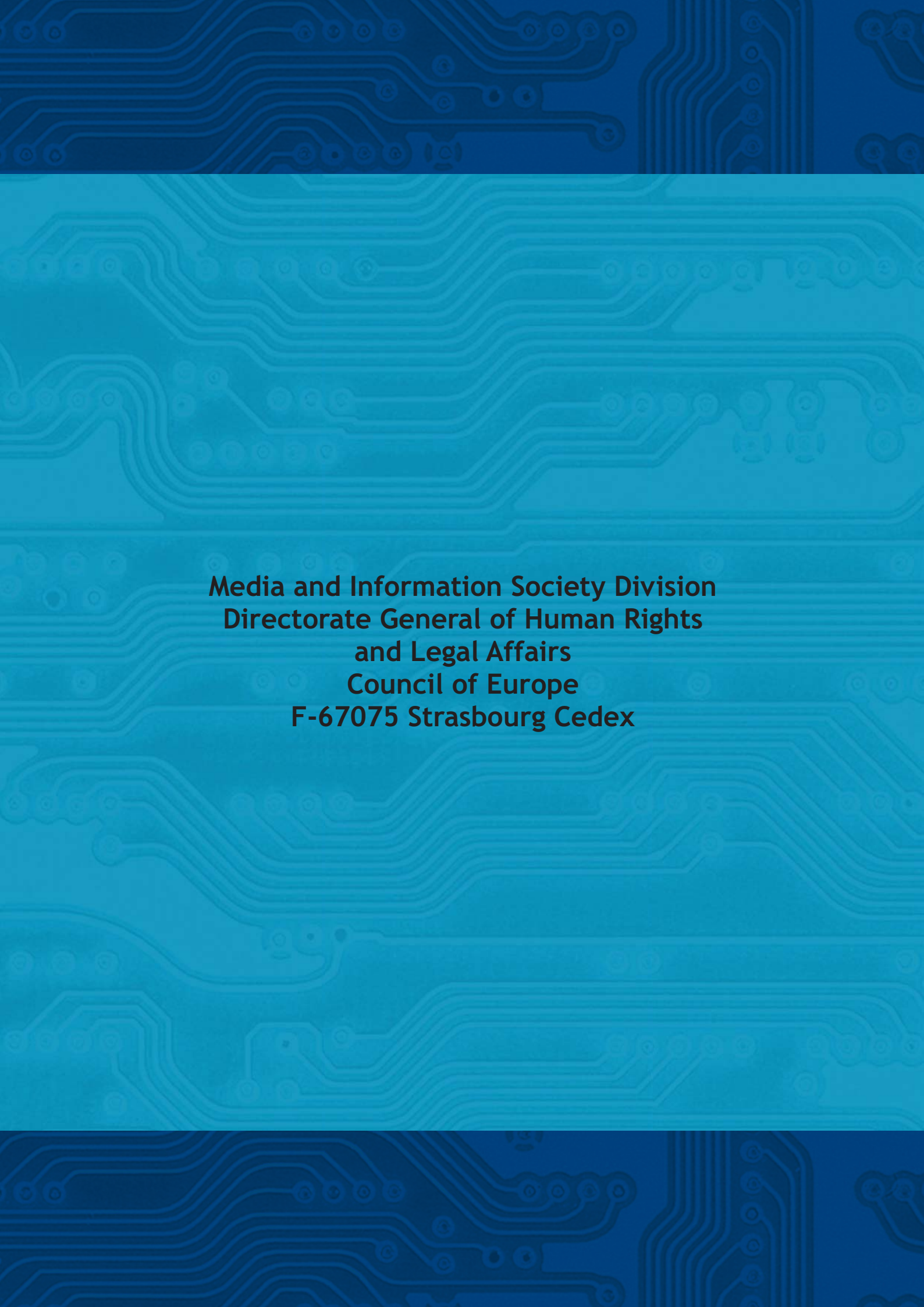
- (a) Under any dispute settlement procedure applicable between it and the responsible State;
- (b) To respect the inviolability of diplomatic or consular agents, premises, archives and documents.

Article 51 – Proportionality

Countermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question.

Article 53 – Termination of countermeasures

Countermeasures shall be terminated as soon as the responsible State has complied with its obligations under part two in relation to the internationally wrongful act.



**Media and Information Society Division
Directorate General of Human Rights
and Legal Affairs
Council of Europe
F-67075 Strasbourg Cedex**