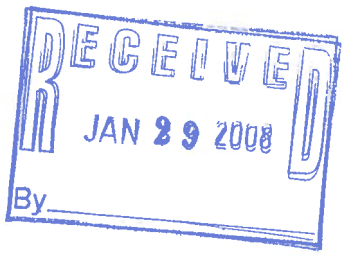

Council of Europe

The Deputy Secretary General

Strasbourg, 21 January 2008

Dear Mr Twomey,

I was very pleased to have met you during the Internet Governance Forum in Rio de Janeiro. Some of the ideas which we discussed merit further consideration, and I share your view that this is best done in the form of concrete proposals.

The impact of ICANN's actions and decisions with regard to international law and human rights should be a matter of ongoing concern for both of our organisations. In my opinion, it would therefore be interesting for ICANN to consider establishing an advisory group to engage in dialogue with, and to seek the advice of, experts and officials from relevant international organisations (such as the Council of Europe) on matters pertaining to international law and human rights with regard to its action and decisions.

In my view, setting up such an advisory group would further ICANN's principles of transparency and accountability. This would also go in the direction of oversight by and accountability to the international community evoked in the Council of Europe's submission to the 2007 Internet Governance Forum, a copy of which you will find enclosed.

I look forward to exploring this proposal with you.

Yours sincerely,

Maud de Boer-Buquicchio

Dr Paul Twomey
President & Chief Executive Officer
The Internet Corporation for Assigned Names and Numbers (ICANN)
4676 Admiralty Way, Suite 330
Marina del Rey
California 90292-660
USA

F - 67075 Strasbourg Cedex
France

Tel. + 33 (0)3 88 41 32 87
+ 33 (0)3 88 41 20 00

Fax : + 33 (0)3 88 41 27 40
+ 33 (0)3 88 41 27 99

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 10 August 2007

BUILDING A FREE AND SAFE INTERNET

Council of Europe Submission to the Internet Governance Forum
Rio de Janeiro, Brazil, 12 to 15 November 2007

TABLE OF CONTENTS

Introduction

For almost 60 years, the Council of Europe has been finding solutions and responding to issues that affect now 800 million people and organisations in Europe, by working with and influencing member states' policies and legal frameworks.[1] These responses are set out in our conventions and other standard-setting documents.

[1]The now 47 Council of Europe member states are Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russian Federation, San Marino, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, "the former Yugoslav Republic of Macedonia", Turkey, Ukraine and the United Kingdom, representing 800 million individuals.

Even if many of these texts were developed before the Internet came into existence, many of the provisions of those conventions and documents apply equally to online environments. The most notable example is the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (frequently referred to as the European Convention on Human Rights). Using this convention, ordinary citizens can get redress for human rights violations by applying to the European Court of Human Rights - probably the best-known Council of Europe institution. The case law of the Court contributes to shaping the obligations of states on how rights and freedoms are exercised and protected online.[2]

A number of other Council of Europe texts, most notably the Convention on cybercrime, deal specifically with the Internet.

Internet-related issues cannot be enclosed within territorial borders. The Internet governance[3] responses worked out by the Council of Europe are therefore of interest to the Internet community as a whole. The platform for debate that we provide brings together member states and other stakeholders (i.e. civil society organisations and representatives of industry). In certain cases, states that are not members of the Council of Europe take part in the discussions and help draw up standards. This has been the case for a number of treaties (some of which are mentioned later in this submission) that could have a global application, i.e. states that are not part of the Council of Europe can also become parties to them.

The Council of Europe perspective on Internet governance

Our objective

By drafting treaties and setting standards about the Internet, the Council of Europe seeks 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.[4] The concrete and practical Council of Europe responses to Internet governance issues mentioned later significantly contribute to the development, sustainability, value, robustness and security of the Internet.

Human rights and democratic values

The Internet must be governed in full respect of human rights; in particular, the fundamental right to freedom of expression, that includes the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers".[5]

The functioning of the Internet must also be underpinned by democratic values that guarantee its openness and accessibility. With ever more people using the Internet, its openness and accessibility have become not only preconditions for the enjoyment

---

[2]See Council of Europe submission to the 2006 IGF http://www.coe.int/t/e/human_rights/media/1_Intergovernmental_Co-operation/MC-S-IS/CoEsubmissionIGF_en.pdf. See also the web page of the European Court of Human Rights http://www.echr.coe.int/echr

[3]Internet governance as per the accepted working definition consists of "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".

[4]See Council of Europe web page www.coe.int/t/e/human_rights/media/Links/Events/1IGFAthens2006Homepage_en.asp#TopOfPage

[5] Cf. Article 10 of the European Convention on Human Rights

of fundamental rights, particularly so people can freely express opinions and receive and give information, but also a measure for democratic participation and improving the transparency and accountability of democratic institutions.

A democratic system of governance is the best guarantor of fundamental rights such as the freedom of expression and association and, by implication, of the openness of the Internet. Genuine popular participation, and people feeling they can influence a decision if they want to, can ensure appropriate reactions if a fundamental right is called into question, threatened or violated. This applies in the online as much as in the offline world. E-tools for public participation could be used to enhance democratic governance of the Internet and to involve all relevant stakeholders in the process.

Public service value of the Internet

The Internet has great potential to serve the common good, positively affecting many aspects of life, including communication, information, knowledge, business and growth. It can be a means to deliver valuable public services, facilitate participation in democratic decision-making and can promote the exercise and enjoyment of human rights and fundamental freedoms for all who use it.

Consequently, the Council of Europe advances the concept of 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 are accessible and affordable, secure, reliable and ongoing.[6] This notion should help provide responses to many public policy questions that arise under the IGF themes, inter alia in respect of general confidence, stability and sustainability of the Internet.[7] We believe in the need to promote and protect this public service value of the Internet.

It should be stressed that, for the many people who are at present information-poor (in contrast to the information-rich on the flip-side of the so-called digital divide), access to the Internet is a legitimate aspiration linked to their very prospects of development and democratic citizenship. This is a clear example where states have an essential role to play in providing a framework for the private sector to operate or by taking concrete steps towards filling essential gaps left by private operators.

The reliability (quality, authenticity and diversity) of information on the Internet is a key factor in making informed choices and decisions. This helps to foster the Internet as a space of trust, freedom and confidence. Developing and promoting 'islands of trust' on the Internet, for example by means of content provided by public service media or public authorities, is one important way forward which we are currently examining and developing at the Council of Europe.

---

[6]Cf. among many other definitions of public service, the following from *Wikipedia*: Public services is a term usually used to mean services provided by government to its citizens, either directly (through the public sector) or by financing private provision of services. The term is associated with a social consensus (usually expressed through democratic elections) that certain services should be available to all, regardless of income. Even where public services are neither publicly provided nor publicly financed, for social and political reasons they are usually subject to regulation going beyond that applying to most economic sectors.

[7]Paragraph 72 e) of the mandate of the IGF highlights the need to "[D]iscuss public policy issues related to key elements of Internet governance in order to foster the sustainability, robustness, security, stability and development of the Internet."

In our view, the public service value of the Internet needs to be recognised as a cross-cutting multifaceted aspect of Internet governance closely linked to the IGF mandate and its themes (i.e. openness, security, access, diversity and critical Internet resources). The security of and confidence in the Internet are preconditions for the full realisation of its public service value, which in turn require partnerships between private sector and public authorities (and recognition of their respective roles and responsibilities) and that users/citizens are empowered and enabled to make effective and well-informed use of the Internet.

Building on our existing standards, we are currently preparing a document as a basis for states to understand their role in 'public service' on the Internet, thus contributing to states' response to Internet governance issues. Existing best practice and measures will be identified and collected to assist states to respond to the IGF in a comprehensive and pragmatic way.

Diversity

The Internet substantially reduces the cost of producing and distributing content and serves as a framework for participation. The availability on the Internet of a wide range of content from multiple sources contributes to a pluralistic information society in which a variety of opinions, ideas and information are exchanged.

The emergence of fora for user-generated content and interactive communities has contributed positively to the creation of new content and services. The Council of Europe is a firm believer in the value of promoting public participation in using and contributing content to the Internet.

Internet users reflect the diversity of society (represented in terms of age, gender or sexual preferences, national, linguistic or cultural background, education level, persons with disabilities, etc.). By providing different groups in society - including cultural, linguistic, ethnic, religious or other minorities - with an opportunity to receive and impart information, to express themselves and to exchange ideas, the Internet is an essential tool for safeguarding cultural and linguistic diversity.

This requires, for example, promoting and protecting locally developed content, including content that is not commercially viable, and the involvement of language communities in developing multilingual content, including content in indigenous and minority languages.

Security

Internet users are entitled to expect a certain level of security. They will turn to various stakeholders to satisfy this demand, but they will ultimately hold the state to account for major failings. This is especially true as regards prejudice suffered in the enjoyment of fundamental rights. States therefore have a vested interest in "find(ing) solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users".[8]

The possibility to exploit the web in a way that poses a threat to society or to vulnerable groups such as children or that undermines confidence, for example when buying goods and services online, is a risk for everyone using the Internet. People's rights can be put at risk if their personal data, identity and anonymity are threatened or exposed. Our objective is to restrict possibilities for such abuse and help create

[8]See paragraph 72 k) of the mandate of the IGF http://www.itu.int/wsis/implementation/igf/index.html

and maintain the Internet as a free and trustworthy space that people can use with confidence. Council of Europe treaties designed to combat Internet crime, which serve as a framework for pan-European cooperation in this area, reconcile an effective fight against crime with respect for human rights.

More transparent processing and presentation of information on the Internet help inform and guide users in making choices and decisions, especially given the rapid evolution of Internet services and technologies. Informing and empowering users about their personal anonymity, the profiling and retention of their data, illegal and harmful content and communications, search engine listings and filters are all important areas in which the Council of Europe is working.

Examples of our pioneering achievements in this area include the 2001 Convention on cybercrime and its 2003 Additional Protocol on the criminalisation of racist and xenophobic acts committed through computer systems and the Convention on the protection of children against sexual exploitation and sexual abuse (which will open to signature later in 2007). Other examples are the 2005 Convention on the prevention of terrorism and the 1981 Convention for the protection of individuals with regard to automatic processing of personal data together, with its 2001 Additional Protocol regarding supervisory authorities and trans-border data flows.

Critical Internet resources

The Internet consists of various elements that are critical to its functioning[9].They range from basic telecommunications infrastructure to the Domain Name System. But, as was pointed out by a number of speakers at the recent Internet Governance Workshop[10] organised by the Internet Corporation for Assigned Names and Numbers (ICANN), the term critical Internet resources should be understood in a broader context which includes the institutional and human elements that are critical to the functioning of the Internet, such as organisations, regulatory frameworks, creators and users.

The management of critical Internet resources has significant public policy implications. Given the global and seamless nature of the Internet, management of infrastructure and critical Internet resources is of global interest and importance. Responses must therefore be worked out within frameworks that can bring about consensus among all stakeholders. Consequently, the basic structure supporting decision-making on critical Internet resources should be internationally recognised and clearly mandated. As well as this, for Internet governance processes to satisfy democratic needs and for the responses provided to be truly people-centred, the part to be played by users should also be recognised.

There is a need to introduce as soon as possible international domain names (or IDNs), i.e. domain names that include non-ASCII characters. Multilingual content and domain names are essential for the Internet's continued development. A multilingual Internet environment will increase local interest in Internet content and increase the possibilities for all language groups to share and access information in their own languages. This will also help to bridge the digital divide. The opportunity of increased address space that the new Internet Protocol (IPv6) will offer should not be missed.

---

[9]Paragraph 72 j) of the mandate of the IGF stresses the importance to "discuss inter alia issues relating to critical Internet resources". http://www.itu.int/wsis/implementation/igf/index.html

[10]See transcript from the 28 June 2007 Internet Governance Workshop in San Juan, Puerto Rico http://www.intgovforum.org/icann_meeting_sj.html

All decisions regarding these and other critical Internet resources issues must be taken in full respect of and based on international human rights law.[11] Particular attention has to be paid to the fundamental right to freedom of expression and information. Arguably, the use of domain names, including generic top-level domain names (gTLDs), concerns forms of expression that are protected by international human rights law, which requires that any restriction has to be prescribed by law and be necessary in a democratic society.[12] According to the case law of the European Court of Human Rights, any restrictions have to be necessary, proportionate and respond to a pressing social need.[13]

This has obvious implications for decisions about domain names (or other critical resources) and accountability for such decisions. Recent controversy on the (non) registration of certain gTLDs shows the need for transparency of decision-making processes and of the criteria applied when taking decisions in accordance with the requirements of the rule of law. In our view, governments should ensure that safeguards are in place so that such decisions conform to the highest internationally accepted standards. Otherwise, decisions could have a restrictive effect rather than promoting and protecting an Internet which is open, fair and diverse.

The role of states

The important role of states in respect of Internet governance, outlined in the Council of Europe submission to the 2006 IGF, should be underlined once again.[14]

When private organisations such as ICANN are relied upon to take decisions on critical Internet resources which concern the state, in effect they become agents of the state. Such delegation brings with it a right and duty of oversight for the state(s) in question, which should respect Council of Europe standards and principles.[15]

---

[11]This is reflected in the bylaws of ICANN where it is stated that one of the core values of ICANN shall be to respect the creativity, innovation and flow of information made possible by the Internet (ICANN bylaws, Article I, Section 2). See also the principles developed by the Governmental Advisory Committee (GAC) to ICANN, where it is stated that new gTLDs should respect *inter alia* "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". (GAC principles regarding new gTLDs, March 28, 2007, para. 2.1).

[12]This test is laid down in a number of international human rights instruments, including Article 10, paragraph 2, of the European Convention on Human Rights. See also the United Nations' International Covenant on Civil and Political Rights (ICCP), which prescribes that the exercise of the rights to freedom of expression and to seek, receive and impart information 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; b) For the protection of national security or of public order (ordre public), or of public health or morals." (ICCP, Article 19, paragraph 3). See also United Nations' Universal Declaration of Human Rights (UDHR), which states that in the exercise of his rights and freedoms, everyone shall be subject only to such limitations as "are determined by law solely for purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (UDHR, Article 29, paragraph 2).

[13]See for example, Judgment of 7 December 1976 , *Handyside v. United Kingdom*, Series A, No. 24, § 49. It might be added that, according to the case law of the European Court of Human Rights, the mere fact that something disturbs, shocks or even offends does not suffice in itself to justify an interference with the right to freedom of expression.

[14]See also in this context the Operating Principles of the Governmental Advisory Committee (GAC) of ICANN - http://gac.icann.org/web/index.shtml

[15]In addition to Article 10 of the European Convention on Human Rights) the Council of Europe has elaborated on the freedom of communication on the Internet and on the importance of self regulation and co-regulation of the Internet (see Council of Europe Declaration of the Committee of Ministers on Freedom of Communication on the Internet, 2003
http://www.coe.int/t/e/human_rights/media/H-Inf(2003)007_en.pdf

From an international law perspective, ICANN operates de facto by delegation on behalf of the international community and, ultimately, on behalf of each state and other stakeholders that make up the Internet community. If this model of governance continues, governments need to ensure that there are safeguards in place so that ICANN conforms to the highest standards. Only in this way can states be satisfied that they will not be held accountable for shortcomings that could have been avoided[16].

But delegation (to ICANN) does not preclude the responsibility of individual states under international human rights law; proper oversight is therefore necessary. Given the global nature of Internet resources and that it would not be practicable for each and every state to exercise such oversight, ICANN (or any other body entrusted with management of critical Internet resources) should ultimately be answerable to the international community.

Some concrete Council of Europe responses to Internet governance issues

E-tools for public participation

The Council of Europe has addressed several key elements of the Internet as an indispensable channel for democratic governance and participation. The Committee of Ministers has adopted recommendations for e-voting systems[17] and e-governance[18] strategies. An intergovernmental Committee of experts on e-democracy is currently preparing a toolkit of generic e-democracy applications and will advise the Committee of Ministers on e-democracy's potential to facilitate democratic reform and practice, and on possible further Council of Europe action in this field. The policy objective underlying this work is to maximise freedom by exploring opportunities and countering threats.

The ever growing number of Internet users and the availability of numerous tools for e-participation continuously broaden the scope for public participation in policy-making processes, including in the field of Internet governance. Using ICT for public participation has the potential to strengthen relationships between citizens and public bodies, to build civic capacity and to change the attitudes and culture of policy-making bodies to become more transparent and genuinely participative.

E-tools can be used at different levels of public involvement and degrees of responsiveness of institutions, i.e. to inform, consult, involve, collaborate, empower[19]. Each place on this spectrum is perfectly valid. The issue is to make the right decision in each case as to where to place an activity and then to make this clear, to manage expectations and deliver against the promise. Another important choice to be made is what methods and tools to use to meet objectives and how to combine them with offline means of participation. Public institutions need to refrain from resorting to e-democracy solutions simply because they are 'modern' and, instead, look for ways that will fulfil their needs.

---

[16]According to its bylaws, ICANN, in performing its mission, should be guided by, *inter alia*, the following core value: "While remaining rooted in the private sector, recognizing that governments and public authorities are responsible for public policy and duly taking into account governments' or public authorities' recommendations." (ICANN bylaws, Article I, Section 2).

[17]See http://www.coe.int/t/e/integrated_projects/democracy/02_activities/02_e-voting/01_Recommendation/index.asp#TopOfPage

[18]See http://www.coe.int/t/e/integrated_projects/democracy/02_activities/01_e-governance/00_Recommendation_and_Explanatory_Memorandum/index.asp#TopOfPage

[19]Cf. the five levels of public participation identified by the International Association for Public Participation.

Examples of e-responses adapted to specific purposes include: posting documents and webcasts (for displaying information); posting personal experience on webcasts or forums; e-mails, questionnaires, policy forum tools (to seek information or respond to requests); webchats, discussion forums (for questioning and scrutiny); e-mail lists, project software, blogs (for campaigning); e-petitions (for lobbying); using geographic, economic, and social information tools to scope issues, understand consequences and develop preferred options (for modelling); voting on issues and options (for polling). In addition, the Internet can be used for community-building (either geographical or interest based) and to show the impact of public participation on decisions taken (thus offering transparency and accountability).

Public service media

There is an increasing need to develop and promote trust (in content) and assurances that the Internet is a space of freedom that people can use with confidence, especially as the capacity to use the Internet directly, immediately and regardless of frontiers becomes easier.

According to the latest Council of Europe standard-setting instrument on this area[20], states should ensure that public service media are present in all platforms, including the Internet. Such media have to be provided with the specific legal, technical, financial and organisational conditions necessary to this end.

Public service media should provide a space of credibility and reliability among the plethora of digital media, fulfilling their role as an impartial and independent source of information, opinion and comment, satisfying high ethical and quality standards. Although they are not alone in this task, public service media are therefore key actors in offering reliable and 'trusted' content on the internet.

For public service media, the Internet constitutes an excellent platform to address people of all generations, communities and social groups, including minority groups. It should encourage diversity through freedom of speech and opinion and promote a culture of dialogue, tolerance (including both inter-cultural and inter-religious tolerance), mutual understanding and social cohesion. Public service media should involve all social groups in active forms of communication. It should in particular encourage the provision of user-generated content and a diversity of cultural expressions, promote genuine pluralism (including through recourse to independent and alternative sources of information or content) and establish other participatory schemes. Using the Internet, public service media should continue to play a central role in education, media literacy and life-long learning, and actively contribute to the formation of a knowledge-based society.

In short, the Internet provides a platform for public service media to realise its objectives, disseminating democratic values and promoting democratic citizenship.

The Convention on cybercrime

A sound legislative basis with effective law enforcement is essential to fight cybercrime and a response to everyday users who are victims of the misuse of the

---

[20]Recommendation Rec(2007)3 on the remit of public service media in the information society, adopted by the Committee of Ministers of the Council of Europe on 31 January 2007 http://wcd.coe.int/ViewDoc.jsp?id=1089759&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

Internet by others. So it is important to strengthen country laws and practices to fight such crime effectively, at both national and international levels.

Compatible and common minimum legal standards are necessary for this. Such standards can be found in the Convention on cybercrime and its Additional Protocol concerning the criminalisation of acts of a racist and xenophobia nature through computer systems. It is the only treaty in the world to address this alarming phenomenon and has therefore attracted widespread international support; as indicated above, the Convention is open to accession by all states.[21]

The Convention contains comprehensive standards and procedures. By defining conduct rather than technology, it ensures that laws and procedures are able to operate even as technology evolves. The Convention requires the criminalisation by states of certain conducts such as computer-related fraud and offences related to child pornography, and contains provisions dealing with the investigation and prosecution of cybercrime. Virtually all new legislation and draft legislation closely follow the provisions of the Convention which helps to develop national legislation and also serves as a framework for efficient international co-operation.

During its meetings (most recently in June 2007) a Cybercrime Convention Committee examines the implementation of the Convention. Further, the Council of Europe Project on cybercrime is co-operating with a wide range of partner organisations representing both industry and civil society and provides specific support to countries including technical assistance to strengthen legislation and training workshops.[22]

The Convention on the prevention of terrorism

The Council of Europe has drawn up several innovative international treaties addressing terrorism, some as early as the 1970s. More recently, in 2005, we adopted a Convention on the prevention of terrorism[23] which, like the Cybercrime convention, has a global application and has received considerable international support; it is regarded as a precursor to certain developments at global level, notably to the adoption by the United Nations Security Council of Resolution 1624 in September 2005. [24]

This treaty is the first to require that states establish as criminal offences conduct that may lead to the commission of acts of terrorism, including public provocation or indirect incitement, recruitment and training for terrorist purposes. The Convention applies, for example, to the glorification and justification of terrorism and terrorist

---

[21] To date, the Convention on cybercrime [ETS No 185] has been ratified by 21 States (including the United States) and signed by 22 States (including Canada, Japan and South Africa). Numerous other States will become Parties once their internal legislative procedures have been completed. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG
Its Additional Protocol [ETS No 189] has been ratified by 11 States and signed by 20 States. See http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=&CL=ENG

[22] For more information see: www.coe.int/cybercrime

[23] The Council of Europe Convention on the prevention of terrorism [CETS No 196] entered into force on 1 June 2007 and to date, it has been signed by 32 and ratified by 7 Council of Europe member states http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm

[24] In addition to United Nations' endorsement, the Convention and its approach have been supported by fellow organisations such as the Organisation for Security and Co-operation in Europe (OSCE), in a Ministerial Decision adopted in December 2006, and the European Union, with a Presidential statement on the occasion of the entry into force of the Convention. The European Commission is currently looking at reviewing the relevant European Union legislation with the possibility of including the offences from the Council of Europe Convention.

acts, to recruitment for terrorism and to terrorist training carried out using the Internet or other electronic communication systems. The Convention also requires that the establishment, implementation and application of the pertinent criminal law provisions respect human rights obligations, in particular the rights to freedom of expression, association and religion. Because of this, the Convention has been characterised as "a sound response which would respect human rights".[25]

If the Council of Europe Convention on the prevention of terrorism effectively addresses the Internet *as a means,* the question then arises: what about the Internet and other electronic communication systems *as a target* of what has been labelled 'cyberterrorism'? Examples of massive attacks on private and national Internet resources already exist.

A Recommendation by the Council of Europe Parliamentary Assembly[26] signalled the danger of large scale terrorist attacks against critical media infrastructures. There is a growing consensus that the combined effect of the Cybercrime convention and its Additional Protocol, and the Council of Europe Convention on the prevention of terrorism allows states to respond adequately to Internet security challenges. However, there is still some way to go. The Council of Europe Committee of Experts on Terrorism (CODEXTER) is considering whether there are gaps in international law and what further action should be taken in this respect.

The Convention on the protection of individuals and automatic processing of personal data

The Internet is a breeding ground for intrusive practices into people's privacy. It is possible to record and store virtually every online activity of Internet users for an indefinite period of time. Often, users are not aware of the large amount of personal data about them on the Internet.

In order to provide effective personal data protection it is vital to strengthen laws and practices so that privacy-compliant practices can spread on the Internet and foster users' trust in the processing of their data. As trans-border data flows are an intrinsic feature of the Internet, it is essential to take measures to protect personal data at a global level.

The Convention on the protection of individuals with regard to automatic processing of personal data and its Additional Protocol on supervisory authorities and trans-border data flows contain minimum standards for personal data protection. The Convention has received widespread support, is open to accession by all states and has already been used by many countries as a model when preparing new laws on data protection. In addition, the Convention and its Protocol provide a sound basis for international co-operation.[27]

---

[25] See Report of Martin Scheinin, United Nations Special Rapporteur on the protection of human rights and fundamental freedoms while countering terrorism, E/CN.4/2006/98, para. 56 (c), available at http://www.ohchr.org/english/bodies/chr/sessions/62/listdocs.htm This position was also underlined in the Report of the Counter-Terrorism Committee to the Security Council on the implementation of Resolution 1624(2005).

[26] Recommendation 1706 (2006) on Media and Terrorism http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta05/EREC1706.htm

[27] To date, 38 Council of Europe member states have ratified and 5 have signed the Convention for the protection of individuals with regard to automatic processing of personal data [CETS No 108] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=7/31/2007&CL=ENG; and 16 member states have ratified and 16 signed its Additional Protocol [CETS No 181] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=7/31/2007&CL=ENG.

The Convention on action against trafficking in human beings

The rapid development in the use of information technologies, in particular the Internet, has given a new dimension to trafficking in human beings. Traffickers now have, literally at their fingertips, an effective, unrestricted and often anonymous means of recruiting their victims. Online employment agencies, in particular model or artist agencies, and matrimonial agencies can all be ploys to lure potential victims. Internet chat websites are also often used to befriend potential victims. The risks for young people to fall into the traffickers' net have substantially increased.

The 2005 Council of Europe Convention on action against trafficking in human beings - aimed at preventing trafficking, prosecuting traffickers and protecting victims - extends to the use of new information technologies, the Internet in particular, to entice potential victims. The international cooperation arrangements in the Convention on cybercrime are applicable to trafficking in human beings. This Convention is also open to accession by all states.[28]

The Convention on the protection of children against sexual exploitation and sexual abuse

Protecting children from all forms of violence is one of our top priorities. Misuse of the Internet is a major concern in relation to the sexual exploitation and sexual abuse of children. The Council of Europe has therefore recently drawn up a new Convention on the protection of children against sexual exploitation and abuse. It will be opened for signature in October 2007 and will be open to accession also by states that are not members of the Council of Europe.

Among the Convention's many references to use of information and communication technologies in the context of the sexual exploitation and sexual abuse of children, it requires states to criminalise conduct such as knowingly accessing child pornography on the Internet. In response to the increasingly worrying phenomenon of children being sexually harmed by adults whom they have met in cyberspace, the Convention also requires the criminalisation of soliciting children for sexual purposes ("grooming").

In addition, as a preventive measure, the Convention recommends that children at primary and secondary level are educated about the risks of sexual exploitation and sexual abuse, especially risks resulting from the use of the Internet and other information and communication technologies.[29]

Distribution of pharmaceutical products and counterfeit medicines

The Internet offers everything, everywhere, anytime. This is also true in the field of medical care. The quality of medical counselling and pharmaceutical products obtained via the Internet cannot be taken for granted; they could entail considerable risks. Moreover, criminal activities concerning pharmaceutical products (including the distribution of counterfeit medicines and the illegal distribution of other pharmaceutical products) are widespread and the Internet is frequently misused for this purpose.

---

[28]To date, 7 Council of Europe member states have ratified and 7 have signed the Convention on Action against Trafficking in Human Beings [CETS No 197]
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=197&CM=1&DF=7/31/2007&CL=ENG
[29]For more information see http://conventions.coe.int/Treaty/EN/projets/v3Projets.asp
See also, as regards education/empowering children, footnote 38

At the Council of Europe, we are actively working to reduce fraud in medicine sales via the Internet and to eradicate counterfeit medicines, as well as to improve patient information and safety as well as the quality of health care that can be obtained online. To this end, we have produced a practical information guide for users. By showing how to distinguish doubtful from reliable medical information and warning about risky behaviour regarding the purchase of medicines through the Internet, the guide is a good tool to empower users.[30]

In addition, we have developed a comprehensive risk-management strategy to address the sale of counterfeit medicines on the Internet and deal with related criminal activities. Guidance provided ranges from responsibility for delivery to rules on counselling and handling of prescriptions. We are developing early warning systems to identify suspect pharmaceuticals, guidelines for analytical verification and frameworks for public health risk assessment and for the taking of remedial action.[31] Policies on good practices for distributing medicines via mail order in general, designed to protect patient safety and the quality of medicines delivered in this way, will be adopted in the coming weeks.

Access for all

To ensure the full realisation of the public service value of the Internet there needs to be easy, universal and affordable access to ICT infrastructure. All users, irrespective of age, special needs, gender, ethnic or social origin, should be able to take advantage of the opportunities that the information society offers. Facilitating easy access for all means removing barriers, making ICT tools easier for everyone to use and encouraging people to use them by raising awareness of their economic and social benefits.[32]

This needs stable legal and regulatory frameworks, as well as business environments, which make it attractive for the private sector to invest in ICT-infrastructure and services. The Council of Europe has called on states to create public access points offering a minimum set of communication and information facilities, in accordance with the principle of universal community service. To this end, public administrations, educational institutions and private owners of access facilities should encourage public use of their ICT facilities.[33]

Specific reference should be made to our work on the role of the Internet in ensuring a better quality of life for people with disabilities. The Internet should be used to offer them better access to information, enhanced opportunities for participation in political, cultural and social life, more opportunities for education and employment, and the use of e-governance services, from filling in tax returns online to voting or making applications for social security support.[34]

---

[30]The guide is available in English, French, Russian, Spanish and German. For more information see Core message of user-oriented guidance at
http://www.coe.int/t/e/social_cohesion/soc-sp/Health Information Sources.tif

[31]See also the Council of Europe Survey on counterfeit medicines, by Dr J. Harper, Mr B. Gellie, available through Council of Europe Publishing: http://book.coe.int

[32]Paragraph 72 e) of the mandate of the IGF stresses the importance of "proposing ways and means to accelerate the availability and affordability of the Internet (...)":
http://www.itu.int/wsis/implementation/igf/index.html

[33]See Recommendation No. R (99)14 of the Committee of Ministers to member states on Universal Community Service concerning New Communication and Information Services
http://wcd.coe.int/ViewDoc.jsp?Ref=Rec(99)14&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC

[34]Specific Council of Europe action and recommendations on these areas can be found in Resolution ResAP(2001)3 "Towards full citizenship of persons with disabilities through inclusive new technologies"

The Disability Action Plan (2006 to 2015) agreed by Council of Europe member states highlights the importance of e-accessibility.[35] A specific action line is devoted to information and communication, calling upon states to ensure that public authorities and other public bodies make their information and communication - including websites - accessible for people with disabilities in line with current international accessibility guidelines. Care should be shown with people who risk double discrimination, such as people with disabilities from minorities and migrant groups, women with disabilities, and people with disabilities in need of a high level of support.

To ensure accessibility, people with disabilities should be involved at the design stage of new technologies, products or services. Attention must also be paid to their specific information, training and education needs and to the implications of constant and rapid innovation. The principle of barrier-free (or access for all) design applied in architecture should be adapted to the technological environment and the Internet. We have identified specific criteria and conditions that need to be respected for people with disabilities to be able to take full advantage of the opportunities offered by the Internet.[36]

A people-centred approach also requires addressing the potential added risks that misuse of the Internet can pose for people with disabilities, ranging from increased exclusion or isolation to exposure to abuse or exploitation.

Education and access to knowledge

Given that users belonging to all social groups and of almost all ages are both recipients and creators of Internet content, education for responsible use of the Internet is now a major challenge, including from a public service perspective. In 2003, the Council of Europe Ministers for Education resolved to give priority to the

---

(http://wcd.coe.int/ViewDoc.jsp?id=233261&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75) and Recommendation Rec(2004)11 on legal, operational and technical standards for e-voting http://wcd.coe.int/ViewDoc.jsp?id=778189&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75 and the Recommendation Rec(2004)15 on electronic governance http://wcd.coe.int/ViewDoc.jsp?id=802805&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

[35]The Council of Europe Disability Action Plan (Recommendation Rec(2006)5) can be found at http://wcd.coe.int/ViewDoc.jsp?Ref=Rec(2006)5&Language=lanEnglish

[36]These criteria and conditions are set out in Council of Europe Resolution ResAP(2001)3 as follows:
Availability: Products and services should be available to all potential users, including people with disabilities, and be provided, where required, with additional equipment e.g. special interfaces, or an equivalent alternative (e.g. personal assistance).
Accessibility: The requirements of people with disabilities should be taken into account in the design and application of all products and services in accordance with Universal Design principles.
Ease of use: Products and services aimed at the general public should be designed in such a way that all people, irrespective of whether or not they have a disability, can use them. User instructions should be easy to follow.
Affordability: Products and services should be available at the same price to everyone. Extra costs in providing access to products and services should not be borne by persons with disabilities.
Awareness: Decision-makers in politics, industry, employment and education should be made aware of the needs of people with disabilities – and people with disabilities should be made aware of the new technologies: both their existence and the possibilities and opportunities offered by the new technologies.
Appropriateness and attractiveness: Products/services should be functional, age-appropriate and aesthetically pleasing.
Adaptability: Products and services should be adaptable to the user's functional limitations and individual circumstances (e.g., auxiliary applications).
Compatibility: New products and services should be compatible with existing products used by people with disabilities, including assistive technology devices. Several aspects of compatibility should be taken into account: hardware and software, mechanical and electrical, and avoidance of interference.

integration of information and communication technologies in our education systems.[37]

Education should seek to enable people to use the Internet to its full potential safely and in a way that respects the rights of others. As creators or suppliers of Internet content (for example when placing information on personal pages or participating in online academic, specialist or other discussions) users have obligations and responsibilities but also may compromise their own safety. The concepts of transparency, accountability and Internet ethics should be emphasised in Internet education for students generally but also for researchers and academic staff at all levels.

Council of Europe's policy documents and practical tools contribute to improving national policies, developing governance, and serve also as educational tools for universities and schools. For example, we have recently adopted guidelines for states on how to develop coherent information literacy and training strategies which are conducive to empowering children and their educators.[38] We have also developed a set of fact sheets (the Internet literacy handbook) to promote safe and ethical use of the Internet.[39] The Internet literacy handbook aims to help teachers, parents and children get the most out of their use of the Internet. It provides concrete and practical guidance on a number of issues such as chat rooms and online-gaming.

There is ongoing debate within the Internet community on the question of freedom of expression and free flow of information from the perspective of access to knowledge and education, the promotion of research and scientific development and the protection and promotion of the diversity of cultural expressions and artistic creation.[40] Paradigms may well be changing in respect of access to knowledge, user generated content, information sharing and the inter-relationships between them. The outcome can have a positive (or negative) impact on freedom of expression but also on the potential for innovation, education and development.

Against this background, we are studying emerging trends in intellectual property rights (IPR's) and their protection, including through digital rights management (DRM) systems and technical protection measures (TPM). From a Council of Europe perspective, these questions always have to be examined taking account of 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". But this right is not absolute. It can be limited as prescribed by law to the extent necessary in a democratic society (restrictions have to be necessary, proportionate and respond to a pressing social need) for the protection of the rights of others.[41]

---

[37]See http://www.coe.int/t/e/cultural_co-operation/education/standing_conferences/e.21stsessionathens2003.asp#P106_10768 http://www.culturalpolicies.net and www.european-heritage.coe.int

[38]Recommendation (2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment (available at http://www.coe.int/t/e/human_rights/media/4_documentary_resources/1CM_en.asp#TopOfPage

[39]See http://www.coe.int/T/E/Human_Rights/Media/hbk_en.html

[40]The access to knowledge movement unifies various ideals such as Open Access, Open Content, or Open Knowledge. A work is open if it is accessible, reproducible and re-usable without legal, social or technological restriction. This allows greater sharing, and incorporation of information into future developments and has significantly increased the availability of online educational and cultural resources.

[41]Cf. Article 10.2 of the European Convention on Human Rights and see also footnote 12. See also Recommendation no. Rec. (2001)7 of the Committee of Ministers to member states on measures to

Conclusions

Council of Europe treaties and standards provide a comprehensive and readily available framework for addressing Internet governance issues. The main themes of the second Internet Governance Forum (access, diversity, openness, security and critical Internet resources) are all directly addressed in and closely linked to our work.

For the Council of Europe it is important that the public service value of the Internet is acknowledged and discussed from the outset within the framework of the IGF. The Internet has huge potential to enhance our rights and freedoms, giving us access to an unparalleled amount of information and ideas while allowing us to be creative and participate in democratic decision-making. We must make sure that this public service value of the Internet is effectively promoted and protected.

However, much remains to be done and on-going work in the Council of Europe will continue to aim at providing timely responses to Internet governance issues. Looking ahead, we will be identifying concerns and solutions on emerging issues, such as the use and impact of technical filtering measures, respect for human dignity and the respective roles of state and non-state actors.

We have developed international standards and frameworks for co-operation in respect of emerging issues such as on-line grooming of children for sexual abuse or the sale of counterfeit medicines through the Internet. The Council of Europe is now considering drawing up a specific treaty dealing with the latter.

In these and other areas we will continue to make sure that human rights and fundamental freedoms are effectively protected and that an enabling environment is created to allow everyone to exercise fully those rights and freedoms in the online world. This is the only way forward if we want the Internet to be an open, accessible, diverse, secure and people-centred environment.

---

protect copyright and neighbouring rights and combat piracy, especially in the digital environment http://www.coe.int/t/e/human_rights/media/4_documentary_resources/CM/1Rec(2001)007_en.asp#TopOfPage