Distr. RESTRICTED

E/CN.4/2006/WG.21/BP.1
9 January 2006

ENGLISH ONLY

COMMISSION ON HUMAN RIGHTS
Sixty-second session

INTERGOVERNMENTAL WORKING GROUP ON THE EFFECTIVE IMPLEMENTATION OF THE DURBAN DECLARATION AND PROGRAMME OF ACTION
FOURTH SESSION
GENEVA, 16 – 27 January 2006
Item 5 (a) of the Provisional Agenda

HIGH LEVEL SEMINAR

Stocktaking on efforts to combat racism on the Internet

Background Paper Prepared by
By Dr. Yaman Akdeniz*

* Dr. Yaman Akdeniz – is a senior lecturer at the School of Law, University of Leeds where he teaches and writes mainly about Internet related legal and policy issues. He is also the director of the LLM in CyberLaw programme, and the co-ordinator of the CyberLaw Research Unit. Akdeniz is also the founder and director of Cyber-Rights & Cyber-Liberties (UK) <http://www.cyber-rights.org>), a non-profit civil liberties organisation since 1997. His forthcoming publications include *Internet Child Pornography and the Law: National and International Responses*, Ashgate, (to be published in late 2006). For further information in relation to his work see <http://www.cyber-rights.org/yamancv.htm>.

Note: The opinions expressed in this paper are those of the author.

TABLE OF CONTENTS

I. Introduction

"As we see all around us, racism and racial discrimination continue unabated. Although we refer to our world as a global village, it is a world sadly lacking in the sense of closeness towards neighbour and community which the word village implies. In each region, and within all countries, there are problems stemming from either a lack of respect for, or lack of acceptance of, the inherent dignity and equality of all human beings. Our world is witness to serious ethnic conflicts; to discrimination against minorities, indigenous peoples and migrants workers; the accusation of institutionalized racism in police forces; harsh immigration and asylum policies; hate sites on the Internet and youth groups promoting intolerance and xenophobia." (Mary Robinson, 1999)[1]

1. Racism was a pressing social problem long before the emergence of the digital age. The advancement of communication technologies such as the internet has, however, added a new dimension to the problem, providing individuals and organisations "with modern and powerful means to support racism and xenophobia" which "enables them to disseminate easily and widely expressions containing such ideas."[2] Concerns about "digital hate" date back to the mid 1980s with the documented use of computers, computer bulletin boards and networks to disseminate racist views and content.[3] New methods of dissemination of anti-Semitic propaganda including video games, computer programmes and the Minitel system in France were noted by a United Nations Secretary-General report in 1994,[4] and the growing use of modern electronic media in international communications between right-wing radical groups (computer disks, databanks etc.) was recorded in 1995.[5] The use of electronic mail and the Internet was firstly observed as a growing trend amongst racist organisations to spread racist or xenophobic propaganda in 1996,[6] and the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and

---

[1] Mary Robinson, United Nations High Commissioner for Human Rights, 24 March 1999, at <http://www.un.org/WCAR/e-kit/fact1.htm>.

[2] Explanatory Report of the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, as adopted by the Committee of Ministers on 7 November 2002, at <http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>, para 3.

[3] Note The Washington Post article "'Neo-Nazis' Inspire White Supremacists," 26 December, 1984 which refers to the dissemination of racist comments through computer bulletin boards in North America. Note also the Anti-Defamation League report entitled *Computerized Networks of Hate* published in January 1985.

[4] Elimination Of Racism And Racial Discrimination: Note by the Secretary-General, A/49/677, 23 November 1994.

[5] Implementation Of The Programme Of Action For The Second Decade To Combat Racism And Racial Discrimination, Report by Mr. Maurice Glélé-Ahanhanzo, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, submitted pursuant to Commission on Human Rights resolution 1994/64, E/CN.4/1995/78, 19 January 1995.

[6] Elimination Of Racism And Racial Discrimination: Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Note by the Secretary-General, A/51/301, 20 August 1996.

related intolerance, in his 1997 report[7] submitted pursuant to Commission on Human Rights resolution 1996/21, declared that

> "The Internet has become the new battleground in the fight to influence public opinion. While it is still far behind newspapers, magazines, radio and television in the size of its audience, the Internet has already captured the imagination of people with a message, including purveyors of hate, racists and anti-Semites." [8]

2. Although the majority of racist content was disseminated in 1996 through North America, it was predicted that this would alter with the rapid growth in Internet use around the globe. Easy and inexpensive access to the Internet, as well as the development of the World Wide Web, provided ready opportunities for publishing and this extended to material of a racist nature. Flyers and pamphlets that had traditionally been distributed locally by hand and had limited visibility are now accessible to a global audience. In time, this type of content would be presented in more attractive high quality formats including in the format of online racist videos, games, cartoons as well as audio/radio transmissions.

3. The use of the Internet as an instrument for the widespread dissemination of racist content can be traced to the mid-1990s. The Simon Wiesenthal Center identified a single website in 1995,[9] and approximately 70 websites disseminating racist content in 1996.[10] Ten years later, it has been estimated that there are more than 5,000 websites in a variety of languages which promote racial hatred and violence, anti-Semitism and xenophobia around the world.[11] A study by the Simon Wiesenthal Center entitled *Digital Terrorism & Hate 2005* reported a 25% increase in such websites compared to 2004 which indicates that the problem of racism and xenophobia is growing over the Internet.[12]

4. These disturbing developments have naturally informed the global fight against racism. A significant number of international instruments acknowledge and attempt to address the problem. The Universal Declaration of Human Rights, the International Convention on the Elimination of All Forms of Racial Discrimination (1963) (ICERD),[13] the International Convention on Civil and Political Rights (ICCPR),[14] the

---

[7] Implementation Of The Programme Of Action For The Second Decade To Combat Racism And Racial Discrimination, Report by Mr. Maurice Glélé-Ahanhanzo, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, submitted pursuant to Commission on Human Rights resolution 1996/21, E/CN.4/1997/71, 16 January 1997.

[8] *Ibid*.

[9] The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/59/329, 7 September 2004, para. 29.

[10] Elimination Of Racism And Racial Discrimination: Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Note by the Secretary-General, A/51/301, 20 August 1996, para. 45.

[11] Canada NewsWire, "Digital Terrorism & Hate 2005 Report Shows 25 Per Cent Increase In Hate Sites," 07 October, 2005.

[12] Note also the International Network Against Cyber Hate report, *Hate on the Net: Virtual Nursery for In Real Life Crime*, June 2004, at <http://www.inach.net/content/inach-hateonthenet.pdf>.

[13] Adopted in 1965, the ICERD entered into force on 4 January 1969. As of 13 December 2005, the total number of member states to this treaty numbered at 170, making it one of the most widely ratified human rights treaties.

International Convention on Economic, Social and Cultural Rights (ICESCR),[15] the International Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), [16] the International Convention on the Suppression and Punishment of the Crime of Apartheid (Apartheid Convention),[17] the Convention on the Rights of the Child (CRC) [18] are some of the more important international instruments to note.

5. In addition to the adoption of normative standards, the international community has responded to the persistence of racism since the entry into force of ICERD, by proclaiming three consecutive Decades to Combat Racism and Racial Discrimination (1973 – 1983; 1983 – 1993; 1993 – 2003), and by organizing, three World Conferences to Combat Racism and Racial Discrimination in 1978, 1983 and 2001.

6. The growing problem of racist content on the Internet has also prompted vigorous responses from a variety of agents, including Governments, supranational and international organisations as well as from the private sector.[19]

7. The Office of the United Nations High Commissioner for Human Rights ("OHCHR") has played a key role in the debate. The OHCHR organised a seminar on the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination in 1997.[20] The purpose of the seminar was to find ways and means to ensure responsible use of the Internet.[21] This was followed with the Commission on Human Rights resolution 1999/78 requesting the United Nations High Commissioner for Human Rights to undertake research and consultations on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and to study ways of promoting international cooperation in this area. [22] The work conducted by the United Nations High Commissioner for Human Rights led to the UN General Assembly, at the request of the UN Commission on Human Rights, to convene the third World Conference

---

[14] Adopted in 1966, the ICCPR entered into force in 1976. As of 13 December 2005, 154 States had ratified the ICCPR.

[15] Adopted in 1976, the ICESCR entered into force in 1976. As of 13 December 2005, there were 151 state parties to the ICESCR.

[16] CEDAW was adopted in 1979, and entered into force in 1981. As of 13 December 2005, its membership stood at 180 state parties.

[17] The 1973 Apartheid Convention entered into force in 1976, and as of 13 December 2005, 104 states have become party thereto.

[18] The CRC was adopted in 1989, and entered into force in 1990. With 192 state parties as of 7 October 2005, it is the UN human rights instrument enjoying most universal ratification.

[19] Note the Review of reports, studies and other documentation for the Preparatory Committee and the World Conference: Report of the High Commissioner for Human Rights on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and on ways of promoting international cooperation in this area, A/CONF.189/PC.2/12, 27 April 2001.

[20] See Racism, Racial Discrimination, Xenophobia and Related Intolerance: Report of the expert seminar on the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination (Geneva, 10-14 November 1997), E/CN.4/1998/77/Add.2, 6 January 1998.

[21] The 2000 Expert Seminar on remedies available to the victims of acts of racism, racial discrimination, xenophobia and related intolerance and on good national practices in this field should also be noted. See Preparatory Meetings And Activities At The International, Regional And National Levels, Note by the Secretary-General, A/CONF.189/PC.1/8, 26 April 2000.

[22] Report of the High Commissioner for Human Rights on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and on ways of promoting international cooperation in this area, A/CONF.189/PC.2/12, 27 April 2001.

against Racism, Racial Discrimination, Xenophobia and Related Intolerance which took place in Durban in 2001 (from 31 August to 8 September). The States participating in the United Nations World Conference adopted a Declaration and Programme of Action (*Durban Declaration and Programme of Action),* containing recommendations intended for the strengthening of the international human rights framework to combat racism, racial discrimination, xenophobia and related intolerance.

8. The Durban Declaration[23] recognized "the positive contribution that the exercise of the right to freedom of expression, particularly by the media and new technologies, including the Internet, and full respect for the freedom to seek, receive and impart information can make to the fight against racism, racial discrimination, xenophobia and related intolerance."[24] However, the document also expressed deep concern about the use of new information technologies, such as the Internet, "for purposes contrary to respect for human values, equality, non-discrimination, respect for others and tolerance, including to propagate racism, racial hatred, xenophobia, racial discrimination and related intolerance, and that, in particular, children and youth having access to this material could be negatively influenced by it."[25] The Declaration explicitly recognised "the need to promote the use of new information and communication technologies, including the Internet, to contribute to the fight against racism, racial discrimination, xenophobia and related intolerance"[26] and declared that "new technologies can assist the promotion of tolerance and respect for human dignity, and the principles of equality and non-discrimination."[27]

9. The Durban Programme of Action, among other significant recommendations, urged States to

> "implement legal sanctions, in accordance with relevant international human rights law, in respect of incitement to racial hatred through new information and communications technologies, including the Internet, and further urges them to apply all relevant human rights instruments to which they are parties, in particular the International Convention on the Elimination of All Forms of Racial Discrimination, to racism on the Internet."[28]

10. The Durban Programme of Action also called upon the States to consider the following, while taking all necessary measures to guarantee the right to freedom of opinion and expression:

> a) Encouraging Internet service providers to establish and disseminate specific voluntary codes of conduct and self-regulatory measures against the dissemination of racist messages and those that result in racial discrimination, xenophobia or any form of intolerance and discrimination; to that end, Internet providers are encouraged to set up mediating bodies at national and international levels, involving relevant civil society institutions;

---

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

[24] *Ibid*., para 90.

[25] *Ibid*., para 91.

[26] *Ibid*., para 92.

[27] *Ibid*.

[28] *Ibid*., para 145.

(b) Adopting and applying, to the extent possible, appropriate legislation for prosecuting those responsible for incitement to racial hatred or violence through the new information and communications technologies, including the Internet;

(c) Addressing the problem of dissemination of racist material through the new information and communications technologies, including the Internet, *inter alia* by imparting training to law enforcement authorities;

(d) Denouncing and actively discouraging the transmission of racist and xenophobic messages through all communications media, including new information and communications technologies, such as the Internet;

(e) Considering a prompt and co-ordinated international response to the rapidly evolving phenomenon of the dissemination of hate speech and racist material through the new information and communications technologies, including the Internet; and in this context strengthening international co-operation.

(f) Encouraging access and use by all people of the Internet as an international and equal forum, aware that there are disparities in use of and access to the Internet;

(g) Examining ways in which the positive contribution made by the new information and communications technologies, such as the Internet, can be enhanced through replication of good practices in combating racism, racial discrimination, xenophobia and related intolerance;

(h) Encouraging the reflection of the diversity of societies among the personnel of media organizations and the new information and communications technologies, such as the Internet, by promoting adequate representation of different segments within societies at all levels of their organizational structure.[29]

11. The Durban Programme of Action also urged States to encourage the private sector to promote the development of voluntary ethical codes of conduct and self-regulatory measures, and of policies and practices aimed at:

(a) Combating racism, racial discrimination, xenophobia and related intolerance;

(b) Promoting the fair, balanced and equitable representation of the diversity of their societies, as well as ensuring that this diversity is reflected among their staff;

(c) Combating the proliferation of ideas of racial superiority, justification of racial hatred and discrimination in any form;

(d) Promoting respect, tolerance and understanding among all individuals, peoples, nations and civilizations, for example through assistance in public awareness-raising campaigns;

(e) Avoiding stereotyping in all its forms, and particularly the promotion of false images of migrants, including migrant workers, and refugees, in order to

[29] *Ibid*., para 147.

> prevent the spread of xenophobic sentiments among the public and to encourage the objective and balanced portrayal of people, events and history.[30]

12. One of three mechanisms established to follow-up the Durban Declaration and Programme of Action and serviced by the Anti-Discrimination Unit is the Intergovernmental Working Group (IGWG). Established by the Commission on Human Rights resolution 2002/68, this Group is mandated "to make recommendations for the effective implementation of the Declaration and Programme of Action and to prepare complementary international standards to strengthen and update international legal instruments against racism." The IGWG decided at its first session (21-31 January 2003) to organize its work on a thematic basis, and one of the thematic areas examined by the IGWG at its third session (11 to 22 October 2004) was that of racism and the Internet. The IGWG adopted eight recommendations on this theme which were submitted as part of its report to the 61st session of the Commission. Recommendation 22 provides that the:

> OHCHR should organize a high-level seminar within the next session of the Working Group on the Internet and racism, racial discrimination, xenophobia and related intolerance. The purpose of the seminar would be to consider progress made in the implementation of relevant provisions of the Durban Declaration and Programme of Action; to assess the possibilities of and challenges posed by the use of the Internet to propagate or to counter material which incites racial hatred and acts of violence and propose concrete measures to be taken at the international and national levels to combat the abuse of the Internet for all forms of racist manifestations; and to examine the contribution that the Internet can make in the fostering of social harmony and the fight against racism. OHCHR should endeavour to ensure the participation of all stakeholders, *inter alia* States, WSIS, international and regional organizations, NGOs, the private sector and the media.

13. The OHCHR high-level seminar on racism and the Internet will take place in Geneva, on 16-17 January 2006. This report seeks to provide a timely critical overview of issues central to this debate, focusing on both legal and policy initiatives (self and co-regulatory) to combat racism on the Internet. Significant developments at State level as well as developments within international organisations form part of this analysis.

II. Identifying Key Issues

14. The global, decentralised and borderless nature of the Internet creates a potentially infinite and unbreakable communications complex which cannot be readily bounded by one national government or even several or many acting in concert. The decentralised nature of the Internet means simply that there is no unique solution for effective regulation at the national level. Harmonisation efforts to combat illegal content, even for universally condemned content such as child pornography, have been protracted and are ongoing.[31] Efforts to harmonise laws to combat racist content on the Internet have proved to be even more problematic. While child pornography is

---

30 *Ibid*., para 144.

31 Rights of the Child: Report submitted by Mr. Juan Miguel Petit, Special Rapporteur on the sale of children, child prostitution and child pornography, E/CN.4/2005/78, 23 December 2004. Note also the Addendum to this report: E/CN.4/2005/78/Add.3, 8 March 2005.

often regarded as a clear cut example of "illegal content," racist content has been much more difficult to categorise.[32] So far, differing views of the limits to freedom of expression have resulted in different legal responses to racist discourse in North America (especially in the United States) and in Europe. There are also varied approaches within Europe in terms of what constitutes illegal content. Harm criterion remain distinct within different jurisdictions with individual States deciding what is legal and illegal. Content regarded as harmful or offensive do not always fall within the boundaries of illegality in all States.

15. Achieving a proper balance between the desire to control racist content and to protect freedom of expression has inevitably proved challenging on the Internet. Despite an attempt at regional harmonisation at the Council of Europe level with the Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems, there is no uniformed approach to the dissemination and availability of racist content on the Internet.

16. The European Commission Against Racism and Intolerance ("ECRI") has noted, "the obligation incumbent upon all States to prevent and prohibit discrimination on the basis of race is enshrined in Arts. 55(c) and 56 of the Charter of the United Nations and has been subsequently reiterated in numerous multilateral conventions."[33] The most significant instrument in this context is the International Convention on the Elimination Of All Forms Of Racial Discrimination ("ICERD") The ICERD, through article 4, "condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form." Article 4 of ICERD clearly sets out the obligations of the signing and ratifying States by stating that State parties "undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, *inter alia*:

---

[32] Child pornography is often presented in visual format involving images and videos, while racist content is portrayed often in writings (but often presented together with images) and makes it difficult to categorise.

[33] "Some prohibit racial discrimination either generally, or in respect of all of the exercise and enjoyment of all of the rights enunciated in those conventions: International Covenant on Civil and Political Rights, 1966, Art 2(1); International Covenant on Economic, Social and Cultural Rights, 1966, Art. 2(2); International Convention on the Suppression and Punishment of the Crime of Apartheid, 1973; International Convention against Apartheid in Sports, 1985. Refer in this context also to Arts. 2 and 7 of the Universal Declaration of Human Rights, 1948, which, although it is not a legally binding treaty, is generally considered to be declaratory of binding customary international law. The following treaties prohibit racial discrimination in the specific fields with which they deal: Convention relating to the Status of Refugees, 1951, Art. 3; Convention relating to the Status of Stateless Persons, 1954, Art. 3; ILO Convention No. 111 concerning Discrimination in respect of Employment and Occupation, 1960, Art. 3(b); UNESCO Convention Against Discrimination in Education, 1962, Art. 3; Additional Protocol I to the Geneva Conventions on the Protection of Victims of International Armed Conflicts, 1977, Art. 85(4); Convention Against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment, 1984, Art. 1; Convention on the Rights of the Child, 1989, Art. 2." See European Commission Against Racism and Intolerance (ECRI), *Legal Instruments to Combat Racism on the Internet*, report prepared by the Swiss Institute of Comparative Law (Lausanne), CRI (2000) 27, at <http://youth-against-racism.net/files/youth/ECRI_Combat_Racism_Internet.pdf>, page 65 and footnote 104.

(a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof;

(b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law;

(c) Shall not permit public authorities or public institutions, national or local, to promote or incite racial discrimination.

17. Currently, with 170 ratifications by member states as of December 2005, the ICERD provisions remain the most important normative basis upon which international efforts to eliminate racial discrimination should be built. [34] The Committee on the Elimination of Racial Discrimination ("CERD") in its General Recommendations number VII[35] and XV[36] explained that the provisions of article 4 are of a mandatory character. According to CERD, to satisfy these obligations, States parties need to enact appropriate legislation as well as ensure that such legislation is effectively enforced. CERD believes that

> "the prohibition of the dissemination of all ideas based upon racial superiority or hatred is compatible with the right to freedom of opinion and expression. This right is embodied in article 19 of the Universal Declaration of Human Rights and is recalled in article 5 (d) (viii) of the International Convention on the Elimination of All Forms of Racial Discrimination. Its relevance to article 4 is noted in the article itself. The citizen's exercise of this right carries special duties and responsibilities, specified in article 29, paragraph 2, of the Universal Declaration, among which the obligation not to disseminate racist ideas is of particular importance. The Committee wishes, furthermore, to draw to the attention of States parties article 20 of the International Covenant on Civil and Political Rights, according to which any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law."[37]

18. Nonetheless, harmonisation has not been established and there remain different interpretations and applications of article 4. 19 states have entered reservations and/or interpretative declarations in respect of article 4. A number of States have not fulfilled the requirements of article 4. Most notably, the US Government declared that "the Constitution and laws of the United States contain extensive protections of individual freedom of speech, expression and association. Accordingly, the United States does not accept any obligation under this Convention, in particular under articles 4 and 7,

---

[34] See Report of the Committee on the Elimination of Racial Discrimination, Sixty-fourth session (23 February-12 March 2004) Sixty-fifth session (2-20 August 2004), No: A/59/18, 01 October, 2004.

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

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

[37] Report of the Committee on the Elimination of Racial Discrimination, Sixty-fourth session (23 February-12 March 2004) Sixty-fifth session (2-20 August 2004), No: A/59/18, 01 October, 2004.

to restrict those rights, through the adoption of legislation or any other measures, to the extent that they are protected by the Constitution and laws of the United States."

19. As the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in his 1998 Report "the ambivalence surrounding points related to the principle of the need to balance rights and protections is evident in the positions taken by Governments through the declarations and reservations they have entered to article 4."[38]

20. It could be argued that ICERD provisions are rather limited and fall short of tackling various manifestations of racism and discrimination despite the progressive interpretation of the various provisions of the instrument. Within this context the question arises for example as to whether there is a need for complementary international standards to combat racism on the Internet. While there is an urgent need to review the functioning of ICERD and consider whether it should be updated, "great care must be taken to achieve an appropriate balance between the rights to freedom of opinion and expression and to receive and impart information and the prohibition on speech and/or activities promoting racist views and inciting violence"[39] as noted by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression noted in his 1998 Report. That balance is yet to be reached and agreed.

III. Governance of Racist Content on the Internet

> *"Clearly, there is need for governance, but that does not necessarily mean that it has to be done in the traditional way, for something that is so very different."* (Kofi Annan, 2004)[40]

21. Typically the stance taken by governments is that what is illegal and punishable in an offline form must also be treated equally online. There are, however, several features of the Internet which fundamentally affect approaches to its governance. As stated above, the decentralized nature of the Internet means that there is no unique solution for effective regulation at the national level. The legal and investigative possibilities at the national level are restricted by the global, distributed and decentralised architecture of the Internet. According to the Commission on Global Governance Reforming the United Nations,

> "Global governance is about a varied cast of actors: people acting together in formal and informal ways, in communities and countries, within sectors and across them, in non governmental bodies and citizens' movements, and both nationally and internationally, as a global civil society. And it is through people that other actors play their roles: states and governments of states, regions and alliances in formal or informal garb. But we also noted that a vital and central role in global governance falls to people coming

---

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

[39] *Ibid*, para 8.

[40] Kofi Annan, Global Forum on Internet Governance, 24 March, 2004 (*Internet Governance: A Grand Collaboration*, March 2004).

> together in the United Nations, aspiring to fulfil some of their highest goals through its potential for common action."[41]

22. This emphasises the global nature of governance that cuts across a variety of possible players that may be involved with governance, including non-governmental organisations both at the local, regional, and international levels. Internet governance as it is emerging may include several layers including the National (and the local), Supra National (e.g. European Union), Regional (Council of Europe, OSCE), and international (United Nations). The effect of supranational, regional and international developments on nation-state governance cannot be underestimated and the aligning of strategies and policies may be necessary to find common solutions for Internet related problems. Internet governance may comprise not only regulatory action by governments but also social norms, self-regulation (ISPs), co-regulation (Hotlines) and co-operation with the ISPs (notice & takedown provisions), regulation through code and technical means (such as rating and filtering tools), as well as education and awareness campaigns. The development of international agreements and conventions could also be part of this emerging wide Internet governance model.

23. The following sections of this report provide a critical overview of key developments at national, regional international, and international levels of Internet governance.

IV. The National Approaches to Internet governance and its limitations

24. A number of court cases have targeted the creators of racist content as well as those hosting it, or providing access to such content in a number of jurisdictions. The most significant of these cases will be highlighted here to illustrate the difficulties encountered at a national level to fight racist Internet content.

A. Yahoo Case (France/USA)

25. In May 2000, the League Against Racism and Anti-semitism (LICRA) and the Union of French Jewish Students (UEJF) brought an action against Yahoo! Inc. and Yahoo France. The plaintiffs alleged that Yahoo! Inc hosted an auction website which contained for sale thousands of items of Nazi paraphernalia and that Yahoo France provided a link and access to this content through the Yahoo.com website. The French Court in its initial judgment[42] held that access by French Internet users to the auction website containing Nazi objects constituted a contravention of French law and an offence to the 'collective memory' of the country and that the simple act of displaying such objects (e.g. exhibition of uniforms, insignia or emblems resembling those worn or displayed by the Nazis) in France constitutes a violation of the Penal Code and is therefore considered as a threat to internal public order. On 22 May, 2000, the Tribunal de Grande Instance de Paris ordered Yahoo! Inc. to take all necessary measures to dissuade and make impossible any access via yahoo.com to the auction

---

41 An overview of *Our Global Neighbourhood: the report of the Commission on Global Governance Reforming the United Nations*, at <http://www.cgg.ch/unreform1.htm>. Note particularly chapter five of this report.

42 *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France*, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000.

service for Nazi memorabilia as well as to any other site or service that may be construed as an apology for Nazism or contesting the reality of Nazi crimes.

26. Yahoo! Inc. announced in January 2001 that it would no longer allow Nazi and Ku Klux Klan memorabilia to be displayed on its yahoo.fr websites and that a more proactive approach with a monitoring or filtering system would be in operation. The new policy, which also included a ban on other forms of hate material, took effect on 10 January, 2001. However, Yahoo! Inc. also asked the U.S. District Court in San Jose to declare the French ruling in violation of the First Amendment and to rule that the French court did not have jurisdiction over content produced by a US business. This was followed by LICRA filing a motion with the San Jose Court to dismiss Yahoo Inc.'s case which was denied by the US District Court for the Northern District of California in San Jose in June 2001. A motion for summary judgment was granted for Yahoo! by the San Jose Court[43] which stated that

> "this case is *not* about the moral acceptability of promoting the symbols or propaganda of Nazism. Most would agree that such acts are profoundly offensive. By any reasonable standard of morality, the Nazis were responsible for one of the worst displays of inhumanity in recorded history. This Court is acutely mindful of the emotional pain reminders of the Nazi era cause to Holocaust survivors and deeply respectful of the motivations of the French Republic in enacting the underlying statutes and of the defendant organizations in seeking relief under those statutes. Vigilance is the key to preventing atrocities such as the Holocaust from occurring again."

27. The Court also questioned "whether it is consistent with the Constitution and laws of the United States for another nation to regulate speech by a United States resident within the United States on the basis that such speech can be accessed by Internet users in that nation." This was a crucial point in granting summary judgment in favour of Yahoo! However, La Ligue Contre Le Racisme et L'Antisemitisme and the US Courts of Appeal for the Ninth Circuit reversed the District Court's grant of summary judgment in August 2004.[44] Then in February 2005, the Ninth Circuit Court of Appeals granted a petition filed by Yahoo! to reconsider its earlier decision.[45] In April 2005, an appeals court in Paris upheld a decision that absolved Yahoo! from legal responsibility for auctions of Nazi paraphernalia sold through its Web site.[46]

---

43 *YAHOO!, Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme*, Case Number C-00-21275 JF [Docket No. 17], United States District Court for the Northern District of California, San Jose Division, 169 F. Supp. 2d 1181; 2001 U.S. Dist. LEXIS 18378, November 7, 2001, Decided.

44 *Yahoo! INC., a Delaware corporation, Plaintiff-Appellee, v. La Ligue Contre Le Racisme Et L'antisemitisme, a French association; L'union Des Etudiants Juifs De France, a French association*, Defendants-Appellants, (2004) 379 F.3d 1120; 2004 U.S. App. LEXIS 17869; 32 Media L. Rep. 2185.

45 *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 2005 U.S. App. LEXIS 2166 (9th Cir., Feb. 10, 2005). Oral arguments were heard in late March 2005. See further Bizreport, "Yahoo Sees Small Victory in Nazi Dispute," 11 February, 2005, at <http://www.bizreport.com/news/8669/>, Associated Press Financial Wire, "Yahoo Lawyers Ask Court for Protection," March 28, 2005.

46 Note that Yahoo! was acquitted by a Paris criminal court in February 2003 but the Association of Auschwitz Survivors and the French Movement Against Racism (MRAP) appealed the decision, pursuing a civil legal action as the public prosecutor declined to appeal the Court's decision on the criminal charges. See generally Agence France Presse, "Auschwitz survivors continue challenge of internet sale of Nazi memorabilia," January 19, 2005; The Associated Press, "Appeals court says former Yahoo exec not liable," April 6, 2005; "French Court Says Yahoo Not Responsible For Nazi;

According to the Court, Yahoo! did not seek to "justify war crimes and crimes against humanity" by allowing such sales on its site.

28. The Yahoo! case is an example of nation-state's desire to enforce and apply national laws to a global and multi-national medium. With the advancement of new technologies and the Internet, cultural, moral, and legal differences become more pronounced. While such differences are legitimate and acceptable, enforcement of such local and national standards to a company based in another country remains inherently problematic.

B. Toben case (Australia/Germany)

29. Dr. Frederick Toben, a German-born Australian Holocaust revisionist who denied the existence of the Holocaust maintained the Adelaide Institute website[47] in Australia. A complaint lodged by the Executive Council of Australian Jewry ("ECAJ") against Adelaide Institute's website was heard by the Australian Human Rights and Equal Opportunity Commission (HREOC) in November 1998.[48] The material on the Adelaide Institute website was deemed to be in breach of section 18C of the Australian Racial Discrimination Act 1975 by the Human Rights and Equal Opportunity Commission in October 2000[49] as the content in question denied the existence of the Holocaust and vilified Jewish people. The material posted on the Adelaide Institute website by Toben cast doubt on the Holocaust, and "suggested that homicidal gas chambers at Auschwitz were unlikely and that some Jewish people, for improper purposes including financial gain, had exaggerated the number of Jews killed during World War II."[50] The decision of the Commission was never enforced and in 2002 an Australian Federal Court[51] agreed with the decision of the Commission and ordered Toben to remove the content in question from his website. The Court was satisfied that Toben had published material on the World Wide Web which was reasonably likely, in all of the circumstances, to offend, insult, humiliate and intimidate Jewish Australians or a group of Jewish Australians. Justice Branson was satisfied that it was "more probable than not that the material would engender in Jewish Australians a sense of being treated contemptuously, disrespectfully and offensively".[52] The Court deliberated for some 14 months before making a ruling, and Toben did not file any defence. The Federal Court made orders requiring Toben to remove the offending material, and any other material the content of which was substantially similar to the offending material, from all web sites controlled by him or

---

Sales," National Journal's Technology Daily, April 7, 2005; "Can the Internet Have Borders?" The Washington Post, April 7, 2005.

47 See <http://www.adelaideinstitute.org>.

48 AAP Newsfeed, "Jewish group seeking apology over website material," 2 November, 1998.

49 Human Rights and Equal Opportunity Commission, Case No. H97/120 between Jeremy Jones and members of the Committee of Management of the Executive Council of Australian Jewry and Fredrick Toben on behalf of the Adelaide Institute, 5 October 2000 (decided).

50 See *Racism and the Internet: Review of the operation of Schedule 5, Broadcasting Services Act 1992*, conducted by the Department of Communications, Information Technology and the Arts. Submission by the Australian Race Discrimination Commissioner Human Rights and Equal Opportunity Commission, November 2002 at <http://www.dcita.gov.au/__data/assets/word_doc/10892/Racism_and_the_Internet.doc>.

51 *Jones v Toben*, Federal Court of Australia, [2002] FCA 1150. The decision can be accessed at <http://www.austlii.edu.au/au/cases/cth/federal_ct/2002/1150.html>.

52 *Ibid*.

the Adelaide Institute and not to publish or republish such material again. Toben appealed and the Full Court of the Federal Court of Australia in Toben v Jones[53] in June 2003 held that Part IIA of the Racial Discrimination Act 1975 which deals with prohibiting offensive behaviour based on racial hatred was constitutionally valid as an exercise of the external affairs power. Justice Carr stated that

> "In my opinion it is clearly consistent with the provisions of the [International Convention on the Elimination of all forms of Racial Discrimination] and the ICCPR that a State party should legislate to 'nip in the bud' the doing of offensive, insulting, humiliating or intimidating public acts which are done because of race, colour or national or ethnic origin before such acts can go into incitement or promotion of racial hatred or discrimination. The authorities show that, subject to the requisite connection [with the external affairs power], it is for the legislature to choose the means by which it carries into or gives effect to a treaty".[54]

30. It is worth noting that Toben was prosecuted and imprisoned in Germany by the German Bundesgerichtshof (German Federal High Court) back in December 2000 for publishing the same material in his Adelaide Institute website.[55] He was arrested in Germany[56] while attending a conference and neither his Australian citizenship nor the fact that his web server was run in Australia served as a defence. As long as the material on his website was accessible in Germany, the Court found jurisdiction. He was sentenced to 10 months imprisonment "for the offences of criminal defamation, several counts of disparaging the memory of the dead and of inciting the populace".[57] The German Federal High Court reversed a lower court decision which held that Toben could not be convicted under the law against inciting racial hatred because the inciting material existed on a foreign Web site. However, the *Bundesgerichtshof* concluded that German laws banning the Nazi party and any glorification of it could be applied to Internet content originating outside German borders but accessed from within Germany, and in particular to the content on Toben's Web site.[58] Toben commented that Germany was "trying to rule the world again by saying that the

---

[53] *Toben v Jones* [2003] FCAFC 137 (27 June 2003). See further Australian Human Rights and Equal Opportunity Commission, *Change and Continuity: Review of the Federal Unlawful Discrimination Jurisdiction*, Supplement, September 2002 - August 2003.

[54] *Ibid*.

[55] Gold, S., "German Landmark Nazi Ruling," Newsbytes, December 12, 2000. Note also that in another similar case American neo-Nazi Gary Lauck was jailed for four years in Hamburg after a court convicted him in 1996 of inciting racial hatred for sending anti-Semitic literature to Germany for many years. See The Australian, "History's rewriter faces German jail," 8 July, 1999.

[56] An English copy of the Arrest Warrant for Dr. Frederick Töben (4/9/99) can be seen at <http://www.ihr.org/other/990409warrant.html>. See further Agence France Presse, "Australian historian arrested in Germany for disputing Holocaust," 09 April, 1999.

[57] See Taylor, G., "Casting the Net Too Widely: Racial Hatred on the Internet", *Criminal Law Journal,* October 2001, p. 262. See further section 130 paragraphs 1 and 3 of the German Criminal Code, StGB. For the German decision see Bundesgerichtshof, Urteil vom 12. December 2000 -- 1 StR 184/00.

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

people who access the Internet have no choice. If someone is offended by the material, they can switch off."[59]

C. Zundel Case (Canada/Germany)

31. In 1997, the Canadian Human Rights Tribunal heard a complaint brought against Ernst Zündel, a German citizen living in Canada, and his website entitled *Zundelsite*[60] which was at the time located in a server in the United States. Among the principal issues that the Tribunal was called upon to decide were whether the site, in denying the Holocaust, among other things, promoted hatred and whether Zündel could be said to control the site, given that it existed physically outside Canada.[61] It is alleged that by posting material to the Zundelsite, Ernst Zündel, caused repeated telephonic communication that was likely to expose Jews to hatred or contempt. The Tribunal was asked to determine whether it was a discriminatory practice to post material on a Website if the material is likely to expose a person to hatred or contempt. Further, the Tribunal was asked to consider what limits, if any, are to be applied to repeated communication of hate messages via the Internet? Finally, if applied to the Internet, whether this was a permissible restriction on freedom of speech under the Canadian Charter of Rights and Freedoms? The original complaints were made back in 1996 but the case proceeded very slowly and it took almost 6 years for the Tribunal to bring this case to an end. Finally a decision was published in January 2002.[62]

32. The Tribunal referred to a number of previous cases[63] and studies[64] which found that hate propaganda[65] poses a "serious threat to society". The Tribunal ordered[66] that Ernst Zündel, and any other individuals who act in the name of, or in concert with Ernst Zündel cease the discriminatory practise of communicating telephonically or causing to be communicated telephonically by means of the facilities of a telecommunication undertaking within the legislative authority of Parliament, matters of the type contained on the Zundelsite, or any other messages of a substantially similar form or content that are likely to expose a person or persons to hatred or contempt by reason of the fact that that person or persons are identifiable on the basis of a prohibited ground of discrimination, contrary to s. 13(1) of the *Canadian Human Rights Act*.[67] In the views of the Tribunal, the use of s. 13(1) of the *Act* to deal with

---

[59] The Washington Post, "Neo-Nazis Sheltering Web Sites In the U.S.; German Courts Begin International Pursuit," 21 December, 2000.

[60] See <http://www.zundelsite.org/>.

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

[62] See the full decision for a chronology of the main procedural elements within this case: *Sabina Citron Toronto Mayor's Committee on Community and Race Relations and Canadian Human Rights Commission v Ernst Zündel*, Canadian Human Rights Tribunal, T.D. ½ 2002/01/18, at <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=252&lg=_e&isruling=0>.

[63] See for example *Canada (Human Rights Commission) v. Taylor*, [1990] 3 S.C.R. 892.

[64] Report of the Special Committee on *Hate Propaganda in Canada* (the Cohen Committee), 1966.

[65] See generally Canadian Parliamentary Research Branch, "*Hate Propaganda*," Current Issue Review, 85-6E, 24 January 2000, at <http://www.parl.gc.ca/information/library/PRBpubs/856-e.pdf>.

[66] *Ibid.*

[67] Section 13(1) entitled Hate messages states that "It is a discriminatory practice for a person or a group of persons acting in concert to communicate telephonically or to cause to be so communicated,

hateful telephonic messages on the Internet remains a restriction on the Respondent's freedom of speech which is reasonable and justified in a free and democratic society. In terms of the effect of the Internet to disseminate hatred the Tribunal stated that it was difficult for the Tribunal "to see why the Internet, with its pervasive influence and accessibility, should be available to spread messages that are likely to expose persons to hatred or contempt. One can conceive that this new medium of the Internet is a much more effective and well-suited vehicle for the dissemination of hate propaganda."[68] The message sent out by the Tribunal was clear that hate could not be tolerated on the Internet or elsewhere. However, the Zundelsite continued to transmit through a server in the United States and continues to do so.

33. Ernst Zündel moved to the United States in 2000, but he was deported back to Canada in 2003 for alleged immigration violations. He was declared a national security threat by a Canadian Federal Court and was deported to Germany in February 2005. His trial started in November 2005 and he faces charges of inciting racial hatred, libel and disparaging the dead before the state court in the Southwestern city of Mannheim. He faces a maximum sentence of five years in jail if convicted.[69] In a parallel development, David Irving, a well known British Holocaust Denier, who also publishes his thoughts on this subject was arrested in November 2005 in Austria on a warrant issued in 1989 under Austrian laws that make it a crime to deny the Holocaust and currently is awaiting trial.[70] In terms of Holocaust denial, it should be recalled that a recent United Nations Resolution rejected any denial of the Holocaust as an historical event, either in full or part in October 2005.[71]

34. These examples reflect the complex nature of the Internet as well as the limitations of the application of existing laws to the Internet. The Zündel case took nearly five years to be finalised in Canada, and even after that various trials related to Zündel continued and as of December 2005 he is still awaiting trial in Germany. The website is still up and running despite the court cases. The Toben case was a similarly drawn out affair and Toben's carefully drafted website is still active. At the same time the various cases related to the Yahoo! case both in France and the US were initiated over five years ago and are still not fully resolved. The legal system which is more adapted to deal with one-off traditional publications (such as newspapers and magazines) has been extremely slow in dealing with web based Internet publications. Above all else, these cases illustrate that the emergence of Internet governance entails

---

repeatedly, in whole or in part by means of the facilities of a telecommunication undertaking within the legislative authority of Parliament, any matter that is likely to expose a person or persons to hatred or contempt by reason of the fact that that person or those persons are identifiable on the basis of a prohibited ground of discrimination.

[68] Note also *Mark Schnell V. Machiavelli and Associates Emprize Inc. et al*. (2002) T.D. 11/02, 2002/08/20, at <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=285&lg=_e&isruling=0>; *Warman v. Kyburz* (2003) CHRT 18, 2003/05/09, at <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=453&lg=_e&isruling=0>; and *Warman v. Warman* (2005) CHRT 36, 2005/09/23, at <http://www.chrt-tcdp.gc.ca/search/view_html.asp?doid=639&lg=_e&isruling=0>.

[69] See Associated Press Worldstream, "Trial of Holocaust denier Zundel halted after judge fires defense lawyer," 15 November, 2005.

[70] BBC News, "Irving faces week in Austria cell," 18 November, 2005, at <http://news.bbc.co.uk/go/pr/fr/-/2/hi/europe/4448896.stm>; The New York Times, "Austria Arrests David Irving, Writer Known as a Holocaust Denier," 18 November, 2005.

[71] See UN General Assembly Resolution on Holocaust Remembrance, A/60/L.12, 26 October, 2005, at <http://www.hmd.org.uk/assets/docs/pdfs/misc/un_resolution.pdf>.

a more diverse and fragmented regulatory network with no presumption that these will be anchored primarily in nation-states. A shift from unilateral state regulation into various forms and models of governance will almost inevitably be witnessed in which alternatives to state regulation such as self-regulation, co-regulation, or a mixture of these are considered by states and international organisations.

V. Regional International Initiatives

This section of the report will provide an overview of the initiatives at the Council of Europe (CoE), Organization for Security and Co-operation in Europe (OSCE, and the European Union (EU) levels before addressing the international initiatives at the United Nations (UN) level.

A. Initiatives by the Council of Europe

35. The Council of Europe ("CoE") Cyber-Crime Convention 2001[72] is the first international treaty to address criminal law and procedural aspects of various types of offensive behaviour directed against computer systems, networks or data in addition to content related crimes such as child pornography. In general, the Convention aims to harmonise national legislation in this field, facilitate investigations and allow efficient levels of co-operation between the authorities of different member states of the CoE and other third party states who would be party to the Convention following a ratification process at the national level.

36. A Committee of Experts on Crime in Cyberspace ("PC-CY") was established within the Council of Europe to draw up the Cyber-Crime Convention to fight *inter alia* substantive offences committed through the use of the Internet in 1997.[73] A number of non member states such as the US, Canada, Japan, and South Africa also contributed to the development of the Convention[74] through the PC-CY Committee. Since then several versions have been developed until a final version was published in June 2001[75] following the approval of the European Committee on Crime Problems

---

[72] The text of the Cyber-Crime Convention can be found at <http://conventions.coe.int/treaty/en/projects/cybercrime.htm>. Note Cyber-Rights & Cyber-Liberties, *An Advocacy Handbook for the Non Governmental Organisations: The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems*, December 2003 (revised and updated in December 2005) at <http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf>.

[73] European Commission, Interim report on *Initiatives in EU Member States with respect to Combating Illegal and Harmful Content on the Internet*, Version 7 (June 4, 1997).

[74] The United States was invited to participate as an "observer" for the development of the 1989 and 1995 Recommendations, as well as in the development of the Convention on Cyber-Crime. See Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the US Department of Justice, Frequently Asked Questions and Answers1 About the Council of Europe Convention on Cybercrime, (Final Draft, released June 29, 2001), at <http://www.cybercrime.gov/newCOEFAQs.html>.

[75] European Committee on Crime Problems (2001) 'Committee of Experts on Crime in Cyberspace (PC-CY)', Final Draft Convention on Cyber-crime,' CDPC (2001) 17, Strasbourg, 29 June 2001, at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm>. See also the European Committee on Crime Problems, Explanatory Memorandum to the Cyber-Crime Convention, CDPC

(CDPC).[76] The Council of Europe Ministers' Deputies approved the Convention in September 2001.[77] This was followed by a formal adoption by the Foreign Affairs Ministers meeting and opening up the Convention to signatures in November 2001.

37. As of December 2005, the signing and ratification process for the main Cyber-Crime Convention resulted with 38 member states (plus the external supporters United States, Canada, South Africa, and Japan) signing and 11 countries (Albania, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Hungary, Lithuania, Romania, Slovenia, and the former Yugoslav Republic of Macedonia) ratifying the main convention out of the potential 49 countries (45 CoE member states plus the above mentioned external supporters). Following the first five ratifications, the Cyber-Crime Convention came into force on 1 July, 2004.

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

38. Although action against racism is viewed by the Council of Europe (CoE) as an integral part of the protection and promotion of human rights, the CoE did not develop a specific convention addressing racism. In 1997 a Council of Europe Recommendation on Hate Speech called upon member states "to take appropriate steps to combat hate speech by ensuring that such steps form part of a comprehensive approach to the phenomenon which also targets its social, economic, political, cultural, and other root causes." [78] Parallel to this political call, the Committee drafting the Cyber-Crime Convention discussed the possibility of including content-related offences other than child pornography (article 9) within the Convention such as the distribution of racist propaganda through computer systems. However, provisions involving the criminalisation of acts of a racist and xenophobic nature committed through computer systems were left out of the Cyber-Crime Convention 2001 as there was no consensus on the inclusion of such provisions. While European states such as France and Germany strongly supported inclusion, the United States of America which has been influential in the development of the main Convention opposed the inclusion of speech related provisions apart from child pornography.

39. Noting the complexity of the issue, the Committee drafting the Cyber-Crime Convention decided that the Committee would refer to the European Committee on Crime Problems (CDPC) the issue of drafting an additional Protocol to the Convention.[79] The Parliamentary Assembly, in its Opinion 226(2001) concerning the Convention recommended the immediate development of an additional protocol to the Convention under the title "Broadening the scope of the convention to include new

---

(2001) 17, Strasbourg, 29 June 2001, at <http://www.privacyinternational.org/issues/cybercrime/coe/cybercrimememo-final.html>.

[76] An intergovernmental expert body reporting to the Council of Europe's Committee of Ministers.

[77] CoE press release, First international treaty to combat crime in cyberspace approved by Ministers' Deputies - 646a(2001), Strasbourg, 19.09.2001.

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

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

forms of offence", with the purpose of defining and criminalising, *inter alia*, the dissemination of racist propaganda.[80]

40. The European Committee on Crime Problems (CDPC) and, its Committee of Experts on the Criminalisation of Acts of a Racist and Xenophobic Nature committed through Computer Systems (PC-RX), was handed the task of preparing the additional protocol, dealing in particular with the following issues:

i. the definition and scope of elements for the criminalisation of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms of distribution of materials or messages with such content through computer networks;

ii. the extent of the application of substantive, procedural and international co-operation provisions in the Convention on Cyber-Crime to the investigation and prosecution of the offences to be defined under the additional Protocol.

41. The Parliamentary Assembly considered racism "not as an opinion but as a crime" in its Recommendation 1543 (2001)[81] on Racism and Xenophobia in Cyberspace. The Parliamentary Assembly also noted that the protocol will "have no effect unless every state hosting racist sites or messages is a party to it."[82]

42. The Additional Protocol Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems[83] aims to harmonise substantive criminal law in the fight against racism and xenophobia on the Internet and to improve international co-operation in this area. The Council of Europe believes that a harmonised approach in domestic laws may prevent misuse of computer systems for a racist purpose. The Explanatory Memorandum to the Additional Protocol states that "this kind of harmonisation alleviates the fight against such crimes on the national and on the international level,"[84] and that "corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by Parties

---

[80] *Ibid*., para 5.

[81] Text adopted by the Standing Committee, acting on behalf of the Assembly, on 8 November 2001.

[82] Para 4 of the Recommendation 1543 (2001).

[83] The drafters of this Protocol took account in particular of (i) the International Convention on the Elimination of All Forms of Racial Discrimination (CERD), (ii) Protocol No. 12 (ETS 177) to the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (iii) the Joint Action of 15 July 1996 of the European Union adopted by the Council on the basis of Article K.3 of the Treaty on the European Union, concerning action to combat racism and xenophobia, (iv) the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance (Durban, 31 August-8 September 2001), (v) the conclusions of the European Conference against racism (Strasbourg, 13 October 2000) (vi) the comprehensive study published by the Council of Europe Commission against Racism and Xenophobia (ECRI) published in August 2000 (CRI(2000)27) and (vii) the November 2001 Proposal by the European Commission for a Council Framework Decision on combating racism and xenophobia (in the framework of the European Union). See para 10 of the Explanatory Report of the Additional Protocol to the Convention on Cyber-Crime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, as adopted by the Committee of Ministers on 7 November 2002, at<http://conventions.coe.int/Treaty/en/Reports/Html/189.htm>.

[84] *Ibid*., para 3.

whose laws in this area are less well defined".[85] The Additional Protocol entails an extension of the Cyber-Crime Convention's scope, "including its substantive, procedural and international co-operation provisions, so as to cover also offences of racist and xenophobic propaganda."[86] Thus, apart from harmonising the substantive law elements of such behaviour, the Protocol aims at "improving the ability of the Parties to make use of the procedural provisions of the Cyber-Crime Convention including international co-operation and mutual legal assistance".[87]

43. The definition of "racist and xenophobic material" contained in Article 2 of the Additional Protocol refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors in such a format that it can be stored, processed and transmitted by means of a computer system.[88]

44. Measures to be taken at national level are explained in chapter II of the Additional Protocol. Article 3 entitled dissemination of racist and xenophobic material through computer systems requires parties to adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the distribution, or otherwise making available, racist and xenophobic material to the public through a computer system.[89] Such conduct needs to be committed intentionally and without right.[90] The "intention" requirement would limit the liability of Internet Service Providers as long as they act as a conduit. But this would not for example exclude "notice based liability" as introduced by the EU Directive on Electronic Commerce which will be discussed later in this report.

45. Article 4 requires parties to criminalise racist and xenophobic motivated threats through a computer systems and as in article 3 such conduct needs to be committed intentionally and without right.[91] Article 5 requires parties to criminalise racist and xenophobic motivated insults made in public[92] through computer systems.[93] Article 6

---

85 *Ibid.*

86 *Ibid.*, para 7.

87 *Ibid.*

88 Para 12 of the Expl. Rep.

89 Note that article 7 requires parties to criminalise the intentional aiding or abetting of the commission of any of the offences established in accordance with the Additional Protocol.

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

91 Note that unlike in article 3, no exceptions are provided for this offence and parties may not reserve the right not to attach criminal liability to such conduct.

92 Unlike in the case of threat, an insult expressed in private communications is not covered by this provision.

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

requires the criminalisation of expressions which deny, grossly minimise, approve or justify acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945.[94] This is supported by the European Court of Human Rights which made it clear in its judgment in *Lehideux and Isorni*[95] that the denial or revision of "clearly established historical facts – such as the Holocaust (whose negation or revision) would be removed from the protection of Article 10 by Article 17" of the European Convention on Human Rights. The Court stated that "there is no doubt that, like any other remark directed against the Convention's underlying values,[96] the justification of a pro-Nazi policy could not be allowed to enjoy the protection afforded by Article 10."

46. The Additional Protocol was opened for signature in Strasbourg, on 28 January 2003. Since then 30 member states have signed the additional protocol (including the external supporter Canada).[97] Out of the 30 signing states, Albania, Cyprus, Denmark, Slovenia, and the former Yugoslav Republic of Macedonia are the only member states which have ratified the Additional Protocol as of December 2005. The Protocol will enter into force following these five ratifications on 1 March, 2006. More recently, a Recommendation of the Parliamentary Assembly of the Council of Europe on Media and Terrorism[98] recommended that the Committee of Ministers ask member and observer states to apply the Additional Protocol to terrorist content in so far as the latter advocates, promotes or incites hatred or violence against any individual or group of individuals based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

B. Initiatives by the Organization for Security and Co-operation in Europe

47. During the past few years there have been increasing demands within the Organization for Security and Co-operation in Europe ("OSCE") to enhance the work of the Organisation in the area of action against racism, xenophobia, discrimination, and anti-Semitism.[99] The 11th Ministerial Council, meeting in December 2003 in

---

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

[95] judgment of 23 September 1998.

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

[97] These are Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Poland, Portugal, Romania, Serbia and Montenegro, Slovenia, Sweden, Switzerland, Ukraine. Note that Canada also signed the Additional Protocol.

[98] CoE Recommendation 1706 (2005) on Media and Terrorism, at <http://assembly.coe.int/Documents/AdoptedText/ta05/EREC1706.htm>. Note also Josef Jarab's report for the Parliamentary Assembly on Media and Terrorism, Doc. 10557, 20 May, 2005, at <http://assembly.coe.int/Documents/WorkingDocs/Doc05/EDOC10557.htm>.

[99] See generally OSCE Office for Democratic Institutions and Human Rights (ODIHR) report, *International Action Against Racism, Xenophobia, Anti-Semitism and Tolerance in the OSCE Region: A Comparative Study*, September 2004, at <http://www.osce.org/publications/odihr/2004/09/12362_143_en.pdf>. Note also the ODIHR report,

Maastricht encouraged the participating States to collect and keep records and statistics on hate crimes, including on forms of violent manifestations of racism, xenophobia, discrimination, and anti-Semitism. The Ministerial Council also gave concrete responsibilities to the OSCE institutions, including the Office for Democratic Institutions and Human Rights which was tasked, in full co-operation, *inter alia*, with the CERD, the European Commission against Racism and Intolerance (ECRI), and the European Monitoring Centre on Racism and Xenophobia (EUMC), as well as with relevant Non-Governmental Organizations (NGOs), with serving as a collection point for information and statistics collected by participating States.

48. The OSCE, has organised a number of high level conferences and meetings in recent years to address the problem of racism, xenophobia, discrimination, and anti-Semitism.[100] The need to combat hate crimes, which can be fuelled by racist, xenophobic, and anti-Semitic propaganda on the internet was explicitly recognised by a decision [101] during the 2003 Maastricht Ministerial Council. This was reinforced by the OSCE Permanent Council Decisions on Combating anti-Semitism (PC.DEC/607),[102] and on Tolerance and the Fight against Racism, Xenophobia and Discrimination (PC.DEC/621) [103] during 2004. In November 2004, the OSCE published a Council Decision on Promoting Tolerance and Media Freedom on the Internet (PC.DEC/633).[104]

49. The November 2004 Council Decision stated that participating States should investigate and, where applicable, fully prosecute violence and criminal threats of violence, motivated by racist, xenophobic, anti-Semitic or other related bias on the Internet.[105] Alongside the decision the OSCE Representative on Freedom of the Media was given the task to actively promote both freedom of expression and access to the Internet and will continue to observe relevant developments in all the participating States. This will involve monitoring and issuing early warnings when laws or other measures prohibiting speech motivated by racist, xenophobic, anti-Semitic or other related bias are enforced in a discriminatory or selective manner for political purposes which can lead to impeding the expression of alternative opinions and views.[106] The Council also decided that participating States should study the effectiveness of laws and other measures regulating Internet content, specifically with

---

Combating Hate Crimes in the OSCE Region: An Overview of statistics, legislation, and national initiatives, June 2005, at <http://www.osce.org/publications/odihr/2005/09/16251_452_en.pdf>.

[100] Note Conference on Anti-Semitism on 19-20 June 2003 in Vienna; Conference on Racism, Xenophobia and Discrimination on 4-5 September 2003 in Vienna; Conference on Anti-Semitism on 28-29 April 2004 in Berlin; Meeting on the Relationship between Racist, Xenophobic and Anti-Semitic Propaganda on the Internet and Hate Crimes on 16-17 June 2004 in Paris; and Conference on Tolerance and the Fight Against Racism, Xenophobia and Discrimination on 13-14 September 2004 in Brussels, Conference on Anti-Semitism, and other forms of Intolerance on 8-9 June, 2005 in Cordoba.

[101] See para 8 of the Decision No. 4/03 on Tolerance and Non-Discrimination by the 2003 Maastricht Ministerial Council (MC.DEC/4/03).

[102] See <http://www.osce.org/documents/pc/2004/04/2771_en.pdf>.

[103] See <http://www.osce.org/documents/pc/2004/07/3374_en.pdf>.

[104] See <http://www.osce.org/documents/pc/2004/11/3805_en.pdf>. Note also the Ministerial Council Decision No. 12/04 on Tolerance and Non-Discrimination, December 2004, at <http://www.osce.org/documents/mcs/2004/12/3915_en.pdf>, as well as the Cordoba Declaration, CIO.GAL/76/05/Rev.2, 9 June 2005, at <http://www.osce.org/documents/cio/2005/06/15109_en.pdf>.

[105] *Ibid*., decision no. 2.

[106] *Ibid*., decision no. 4.

regard to their effect on the rate of racist, xenophobic and anti-Semitic crimes,[107] as well as encourage and support analytically rigorous studies on the possible relationship between racist, xenophobic and anti-Semitic speech on the Internet and the commission of crimes motivated by such speech.[108]

C. Initiatives by the European Union

50. In addition to being concerned with telecommunications liberalisation, the creation of a European Information Society, [109] the development of electronic commerce, data protection and privacy, the European Union is also committed to *inter alia* steer co-operation for fighting crime within the Member States in relation to exploitation of women, sexual exploitation of children, and high-tech crime. [110] Tolerance, anti-discrimination and the fight against racism are concepts which are strongly embedded within the institutional framework of the European Union.[111] The EU has always been very active in the field of racism and xenophobia[112] as well as in relation to the safer use of the Internet.

51. In November 2001, the European Commission proposed a Framework Decision on combating racism and xenophobia designed to ensure that racism and xenophobia are punishable in all member states by effective, proportionate and dissuasive criminal penalties. [113] The draft Framework Decision addresses every form of racism and xenophobia irrespective of its motivation or grounds, and intends to improve judicial co-operation between the Member States. However, the Framework Decision has not been yet finalised. Discussions in the Council of the European Union on the proposed Framework Decision on combating racism and xenophobia continued under the

---

107 *Ibid*., decision no. 5.

108 *Ibid*., decision no. 6.

109 European Commission, *eEurope- An Information Society for all*, Progress report for the Special European Council on Employment, Economic reforms and social cohesion towards a Europe based on innovation and knowledge Lisbon, 23 and 24 March 2000, COM/2000/0130 final, March 08, 2000. European Commission, *eEurope 2002 - An Information society for all - Draft Action Plan* prepared by the European Commission for the European Council in Feira - 19-20 June 2000, COM/2000/0330 final. European Commission, Communication from the Commission to the Council and European Parliament - *The eEurope 2002 update* prepared by the European Commission for the European Council in Nice, 7th and 8th December 2000, COM/2000/0783 final. Communication from the Commission to the Council and the European Parliament - *eEurope 2002: Impact and Priorities A communication to the Spring European Council in Stockholm*, 23-24 March 2001, COM/2001/0140 final. Opinion of the Economic and Social Committee on "eEurope 2002 An information society for all Draft Action Plan," Official Journal C 123 , 25/04/2001 P. 0036 – 0046, April 25, 2001.

110 Conclusions of the Tampere European Council: Bull. 10-1999, point I.14: The Council of the European Union at its Tampere meeting in October 1999 stated that the fight against cybercrime is a priority in developing the Union as an area of freedom, security and justice (Article 2 of the EU Treaty). See furthermore Joint Action 97/154/JHA concerning action to combat trafficking in human beings and sexual exploitation of children: OJ L 63, 4.3.1997.

111 Note the EU Annual Report on Human Rights – 2005, 12416/05, Brussels, 28 September 2005.

112 Note the Declaration by the Council and the Representatives of the Governments of the Member States, meeting within the Council on combating racism and xenophobia on the Internet by intensifying work with young people, 9330/01, Brussels, 6 June 2001.

113 Note also the Declaration by the Council and the Representatives of the Governments of the Member States, meeting within the Council on combating racism and xenophobia on the Internet by intensifying work with young people, 9330/01, Brussels, 6 June 2001.

Luxembourg Presidency in 2005, but without conclusion[114] largely due to different approaches to limitations in the exercise of freedom of expression within the Member States of the EU. Even if an agreement had been reached in the course of 2005 the implementation of the Framework Decision within the Member States would not have taken place before June 2007.

52. More specifically, in relation to the safer use of the Internet, the European Union through the European Commission developed an Action Plan[115] in 1998 which encouraged self-regulatory initiatives to deal with illegal and harmful Internet content including the creation of a European network of hotlines for Internet users to report illegal content such as child pornography; the development of self-regulatory and content-monitoring schemes by access and content providers; and the development of internationally compatible and inter-operable rating and filtering schemes to protect users. Furthermore, the EU Action Plan advocated measures to increase awareness of available possibilities among parents, teachers, children and other consumers to help these groups to use the networks whilst choosing the appropriate content and exercising a reasonable amount of parental control. Although originally planned as a three year Action Plan, in 2002[116] the European Commission prolonged the work in this field for another two years expanding the Action Plan related work and projects to cover the EU candidate countries.[117] One of the main reasons for expanding the Action Plan programme was the fact that illegal and harmful content on the Internet remained as a continuing concern for lawmakers, the private sector, and parents. The coverage of the Action Plan was extended to new online technologies:

> "including mobile and broadband content, online games, peer-to-peer file transfer, and all forms of real-time communications such as chat rooms and instant messages. Action will be taken to ensure that a broader range of areas of illegal and harmful content and conduct of concern are covered, including racism and violence."

53. In May 2005, the European Union extended the Action Plan on " Safer Internet Plus" for the period of 2005-2008 to continue to promote safer use of the Internet and new online technologies, particularly to fight against illegal content such as child pornography and racist material and content which are potentially harmful to children or content unwanted by the end-user. It is suggested by the Safer Internet Plus that "practical measures are still needed to encourage reporting of illegal content to those in a position to deal with it, to encourage assessment of the performance of filter technologies and the benchmarking of those technologies, to spread best practice for codes of conduct embodying generally agreed canons of behaviour, and to inform and educate parents and children on the best way to benefit from the potential of new

---

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

[115] Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998.

[116] European Commission Communication, Follow-up to the Multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks: Proposal for a decision of the European Parliament and of the Council amending Decision No 276/1999/EC adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, COM 2002 152, Brussels, 22.03.2002, INFSO/D/5.

[117] *Ibid*, see para 3.1.2. Interface to candidate countries.

online technologies in a safe way."[118] The four year programme will have a budget of EUR 45 million and it will focus more closely on end-users: parents, educators and children. The Safer Internet Plus Plan will also cover EU candidate countries. The indicative breakdown of the budget suggests that almost half of the available budget will be spent on awareness raising (47-51%). Fighting against illegal content will receive 25-30%, tackling unwanted and harmful content 10-17%, and promoting a safer environment 8-12% of the budget.[119]

VI. International Initiatives through the United Nations

54. A call for a study of the use of new technologies (including video games, computer networks) for the propagation of racial hatred and the urgent proposal of a set of internal and international measures to end such abuses were issued following the first European meeting of national institutions for the promotion and protection of human rights in November 1994.[120] This call was to be considered by the United Nations and the Member States of the Council of Europe. Further calls for research to consider whether international measures be taken to control information transmitted over the Internet were made during 1996[121] with the recognition that "no national legislation has any power over this worldwide network".[122]

55. The availability of racist and xenophobic propaganda through computer and electronic networks and measures to be taken at the national and international levels were considered during a United Nations seminar to assess the implementation of the ICERD in Geneva in September 1996.[123] During the seminar Rabbi Abraham Cooper stated that "online discussion or chat groups provided an opportunity to denigrate minorities, promote xenophobia and identify potential recruits for the racist groups." The participants to the seminar felt that the United Nations was responsible for ensuring that modern communications technologies were not used to spread racism. It was thought by the participants that an international approach would help to overcome the problem posed by the differences in national legislations that made it possible for

---

[118] See para 7 of Decision No 854/2005/EC of the European Parliament and of the Council establishing a Multiannual Community Programme on promoting safer use of the internet and new online technologies, PE-CONS 3688/1/04 REV1, Strasbourg, 11 May 2005.

[119] Within this context an EU Proposal for a Recommendation of the European Parliament and of the Council on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry which is currently under consideration at the European Parliament should also be noted.

[120] Implementation Of The Programme Of Action For The Second Decade To Combat Racism And Racial Discrimination, Report by Mr. Maurice Glélé-Ahanhanzo, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, submitted pursuant to Commission on Human Rights resolution 1994/64, E/CN.4/1995/78, 19 January 1995.

[121] Elimination Of Racism And Racial Discrimination: Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Note by the Secretary-General, A/51/301, 20 August 1996.

[122] *Ibid*., para 46.

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

racist material to be produced in countries where there were no legal sanctions against incitement to racial hatred and made available through the Internet in countries where legal restrictions existed. Co-operation with the Internet industry especially with the Internet Service Providers was also mentioned. The participants also recalled that article 4, paragraphs (a) and (b) of the ICERD contained all the provisions on the basis of which States parties could take legal measures to prohibit organizations which were involved in racist propaganda over the Internet. The recommendations adopted by the seminar recommended that the United Nations, in particular its Legal Office, and other international and regional organizations should undertake a systematic review of existing international instruments, with the view to their applicability/adaptability to the parallel forms of communication on the Internet.

56. The Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance noted in his 1997 report that "emphasis should be placed on the use of modern communications technology, including the Internet, as a vehicle for incitement to racial hatred and xenophobia."[124] The Special Rapporteur recommended the consideration for joint action, research, and beginning of such studies at an international level over the use of the Internet as a vehicle for racist propaganda.[125] The Special Rapporteur also welcomed the initiative taken by the General Assembly in its resolution 51/81,[126] whereby the Assembly recommended that a seminar be organized by the United Nations Centre for Human Rights (presently, the United Nations Office of the High Commissioner for Human Rights), in cooperation with the CERD, the United Nations Educational, Scientific and Cultural Organization (UNESCO), the International Telecommunication Union (ITU) and other relevant United Nations bodies, non-governmental organizations and Internet service providers, with a view to assessing the role of the Internet in the light of the provisions of the ICERD.[127]

57. The Office of the High Commissioner for Human Rights organized a seminar on "The role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination" in Geneva, in November 1997.[128] The seminar concluded by strongly condemning the Internet's use by some groups and persons to promote racist and hate speech in violation of international law.[129] The seminar further recommended that the Internet should be used as an

---

[124] Implementation Of The Programme Of Action For The Second Decade To Combat Racism And Racial Discrimination, Report by Mr. Maurice Glélé-Ahanhanzo, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, submitted pursuant to Commission on Human Rights resolution 1996/21, E/CN.4/1997/71, 16 January 1997, para 8.

[125] *Ibid*., para 132.

[126] See para.10 of the Resolution 51/81.

[127] See generally Elimination Of Racism And Racial Discrimination: Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Note by the Secretary-General, A/52/471, 16 October 1997.

[128] Racism. Racial discrimination, xenophobia and related intolerance: Report by Mr. Glélé-Ahanhanzo, Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, submitted pursuant to Commission on Human Rights resolution 1997/73, E/CN.4/1998/79, 14 January 1998, para 23.

[129] Racism, Racial Discrimination, Xenophobia and Related Intolerance: Report of the expert seminar on the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination (Geneva, 10-14 November 1997), E/CN.4/1998/77/Add.2, 6 January 1998.

educative tool to combat racist propaganda, prevent racist doctrines and practices and promote mutual understanding. The seminar also recommended that Member States of the United Nations continue their cooperation and establish international juridical measures in compliance with the ICERD to prohibit racism on the Internet while respecting individual rights, especially freedom of expression.

58. The Special Rapporteur in his 1998 report noted that "although the States have now become aware of the dangers these acts represent, very few efforts have been made to combat the phenomenon,"[130] and that "only globally concerted action will be effective enough to halt the tendency to use the Internet for racist and xenophobic purposes, in view of the global, cross-frontier nature of that type of activity."[131] The Special Rapporteur questioned whether it would not be possible in conformity with articles 4 and 5 of the ICERD to adopt appropriate legislation, on a country-by-country basis, against incitement to hatred and racial discrimination? In addition to taking possible legislative action he also called upon the international community to undertake positive action to combat the abusive exploitation of the Internet on its own ground, that is, "by using the Internet itself to broadcast anti-racist and anti-xenophobic messages, and even to spread human rights education against racism."[132] In this respect, the Council of Europe's efforts were noted with the launch of the European Commission against Racism and Intolerance website. The Special Rapporteur in the same report recommended, as in previous reports, to envisage the possibility of action at the international level by immediately beginning studies, research and consultations on the use of the Internet for purposes of incitement to hatred, racist propaganda and xenophobia, and also to draw up a programme of human rights education and exchanges over the Internet on experience in the struggle against racism, xenophobia and anti-Semitism.

59. In 1999, the Commission on Human Rights, while noting with concern the increase in the use of new communications technologies, in particular the Internet, to disseminate racist ideas and incite racial hatred, stated that the use of Internet technologies could contribute to combating racism, racial discrimination, xenophobia and related intolerance, for example through the creation of Internet sites to disseminate anti-racist and anti-xenophobic messages.[133] The Commission requested the United Nations High Commissioner for Human Rights to undertake research and consultations on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, to study ways of promoting international cooperation in that area, and to draw up a programme of human rights education and exchanges over the Internet on experience in the struggle against racism, xenophobia and anti-Semitism. The Special Rapporteur suggested that the question of use of the Internet to disseminate racism and xenophobia should be included in the agenda of the World Conference on Racism and Racial Discrimination, Xenophobia and Related Intolerance.

---

130 Racism. Racial discrimination, xenophobia and related intolerance: Report by Mr. Glélé-Ahanhanzo, Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, submitted pursuant to Commission on Human Rights resolution 1997/73, E/CN.4/1998/79, 14 January 1998, para 50.

131 *Ibid*.

132 *Ibid*, para 51.

133 See Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance, Note by the Secretary-General, A/54/347, 8 September 1999.

60. In his 2000 report, the Special Rapporteur strongly recommended the holding of international consultations at the governmental level with a view to regulating the use of the Internet and harmonizing criminal legislation on use of the Internet for racist purposes.[134]

61. In his 2002 report,[135] the Special Rapporteur said he hoped that the States concerned and the international community will succeed in developing measures to nip this increasingly alarming phenomenon in the bud pursuant to the provisions of the Durban Programme of Action.[136]

62. Condemnation of the misuse of print, audio-visual and electronic media and new communications technologies, including the Internet, to incite violence motivated by racial hatred by the UN General Assembly continued in 2003 with a call for States to take all necessary measures to combat this form of racism in accordance with the commitments that they have undertaken under the Durban Declaration and Programme of Action,[137] in particular paragraph 147 of the Programme of Action, in accordance with existing international and regional standards of freedom of expression and taking all necessary measures to guarantee the right to freedom of opinion and expression.

63. In his 2003 report, the Special Rapporteur[138] commended the adoption in November 2002 of the Additional Protocol to the Convention on Cyber-Crime concerning the Criminalization of Acts of a Racist or Xenophobic Nature Committed Through Computer Systems by the Committee of Ministers of the Council of Europe.[139] The Special Rapporteur said in his report that he hoped that a similar document will emerge at the international level in the form of an additional protocol to the ICERD so that more States can adopt legal measures to combat the use of the Internet for racist or xenophobic purposes.[140] There was support for such a consideration from the General Assembly of the United Nations during 2004.[141] However, as mentioned previously in this report, disagreements on the most appropriate strategy (especially between the United States and certain European countries) for preventing dissemination of racist content on the Internet, including the

---

134 Report of the Special Rapporteur of the Commission on Human Rights on contemporary forms of racism, racial discrimination, xenophobia and related intolerance Note by the Secretary-General, A/55/304, 19 August 2000.

135 Measures to combat contemporary forms of racism, racial discrimination, xenophobia and related intolerance Note by the Secretary-General, A/57/204, 11 July 2002.

136 See Report of the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance, Durban, 31 August - 8 September 2001, A/CONF.189/12, 25 January, 2002, chap. I, Programme of Action, paras. 143-147.

137 The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/58/313, 22 August 2003.

138 Note change in Special Rapporteur:Mr. Doudou Diène (Senegal), replaced Mr. Maurice Glèlè-Ahanhanzo (Benin) (1993-2002) as of August 2002 (E/CN.4/RES/2002/68). The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/58/313, 22 August 2003.

139 *Ibid.*

140 *Ibid.*

141 The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/59/329, 7 September 2004.

need to adopt regulatory measures to that end remains and these were highlighted by the Secretary-General report in September 2004.[142] In the absence of global consensus and agreement on the limits of interference with freedom of expression, such an international instrument will be difficult to develop and implement.

VII. Effectiveness of Regional and International Regulatory Efforts & Alternatives to State Legislation

64. Substantial international efforts such as the CoE's Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems carry political significance but will such legislative initiatives have an impact upon reducing the problem of racist content on the Internet? Although state legislation is still a strong option and may be preferred in most instances, problems associated with the Internet may require the careful consideration of alternatives to state regulation. Due to the global and decentralised nature of the Internet, government regulation and even prosecutions may have limited effect and application especially if the racist content is transmitted from outside the jurisdiction in which it is considered illegal. As shown in this report, the Courts' reaction to cases involving the prosecution of racist content has been slow and problematic. Hence the need to consider alternative and/or additional forms of regulation to fight racist content on the Internet.

65. The steps taken by a number of governments at the national level have shown their limitations as this report has tried to highlight, and a regional international regulatory initiative such as the CoE Additional Protocol aimed at punishing racism on the Internet will have no effect unless every state hosting racist sites or messages is a party to it as rightly stated by a CoE Recommendation 1543(2001) on Racism and xenophobia in cyberspace.[143] The ratification process is a drawn out affair and it is taking over three years to bring the Protocol into force in March 2006 with only five States ratifying it since January 2003. A considerable amount of time will be required to reach a substantial number of ratifications. This is not necessarily unusual as the ratification of such instruments is a very long process at the Member States level, and even the main supporters of the Additional Protocol such as Germany and France are yet to ratify.

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

---

142 *Ibid*, para 31.

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

criminalisation of expressions which deny, grossly minimise, approve or justify acts constituting genocide or crimes against humanity may not be all supported by the non signing and non ratifying Member States.

67. The reservations present in articles 3, 5, and 6 could also result in disparities between the parties to the Additional Protocol and harmonisation may never take place in relation to "racist and xenophobic motivated insults" (article 5), and "denial, gross minimisation, approval or justification of genocide or crimes against humanity" (article 6) as these two articles allow the parties to the Protocol to reserve the right not to apply, in whole or in part the offences provided within these articles. For example, within the Council of Europe, only France, Germany, Belgium, Switzerland, and Austria have laws criminalising the denial of crimes against humanity, and in the case of Germany, Belgium, and Austria this is only limited to the denial of genocide committed by the Nazis.[144] A similar reservation is also provided in relation to the "dissemination of racist and xenophobic material through computer systems" (article 3) but only so far as the dissemination is related to material which advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. It is also provided that a Party may reserve the right not to apply the dissemination offence provided in article 3 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies.

68. It is difficult to speculate how effective a regional international effort such as the CoE Additional Protocol will be. Even if all member states of the CoE sign and ratify the Additional Protocol, the problems associated with racist Internet content will not disappear. Certain websites will continue to be hosted in the United States and elsewhere in which the transmission of racist content is not criminalised. This, in a sense, reflects the true nature of the Internet which carries inherent risks. The key question is how to manage these risks.

69. The "one for all" rules advocated by the likes of the CoE Additional Protocol remain problematic and States with strong constitutional protection for freedom of expression such as the USA will not rush to sign and ratify such international agreements and conventions. In other words, there will always be safe havens to host and carry content deemed to be illegal under the terms of international agreements, protocols, and conventions.

70. It is not of course suggested that nothing should be done to tackle the problem of racist content on the Internet. There are, however, other options available to tackle such risks and problems in a global society. This should not be limited to developing international conventions, and adopting laws. The development of international conventions and agreements and the implementation of such conventions including the signing, ratification, and effective implementation by the States at a national level is an incredibly slow and problematic process as witnessed by the limited implementation of CERD, the CoE's Cyber-Crime Convention as well as that of the Additional Protocol to the Cyber-Crime Convention, and the UN Optional Protocol to

---

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

the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.

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

72. Within the context of racism and xenophobia on the Internet, "doing nothing" is not a viable option given the extent and expanding nature of the problem. It was growing concerns over the availability of such content over the Internet that triggered the Council of Europe to develop the Additional Protocol to the Cyber-Crime Convention, and the United Nations World Conference Against Racism, Racial Discrimination, Xenophobia and Related Intolerance to adopt the Durban Declaration and Programme of Action. At the same time relying on social norms, customs and netiquette (set of custom Internet rules) is also not a viable option as these will not be enforceable nor effective in a borderless and multi national, and multi cultural environment.[145]

73. The Declaration on Freedom of Communication on the Internet adopted by the Committee of Ministers of the Council of Europe on 28 May 2003 encouraged self-regulation and co-regulatory initiatives regarding Internet content. Similar recommendations were also made in a CoE Recommendation (2001)8 on self-regulation concerning cyber-content.[146] Within this context the no rush to legislation approach adopted by the European Commission with its Action Plan on promoting safer use of the Internet should be noted which is now extended to cover EU candidate countries.

74. With self and co-regulatory initiatives the states and international organisations can also co-operate with the NGOs and the private sector, and a "socially responsible private sector can help realize an Information Society that respects human rights."[147] This multi-actor approach is also supported by the Durban Programme of Action which encouraged the private sector to promote the development of self-regulatory measures, and policies and practices aimed at combating racism, racial discrimination, xenophobia and related intolerance.[148]

75. The following part of this report will provide a critical analysis of the additional and alternative means of combating racist Internet content including self-regulation by the Internet Service Providers, development of co-regulatory initiatives by Internet Hotlines, as well as regulation through code, and technical means.

---

[145] During the early days of the Internet, such norms and netiquette were observed by the Internet community through peer pressure. But the growth of the Internet made such custom made rules largely inefficient. See Gelbstein, E., and Kurbalija, J., *Internet Governance: Issues, Actors, and Divide*, DIPLO report, 2005, at <http://www.diplomacy.edu/isl/ig/>, p. 71.

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

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

[148] See paragraph 144 of the Durban Programme of Action.

VIII. Self-Regulation and Co-Regulation: Internet Service Providers & Hotlines

76. Illegal content must be dealt with at source by law-enforcement agencies, and their activities are covered by the rules of national law and agreements of judicial co-operation. Nevertheless, Internet Service Providers ("ISPs") can help in reducing circulation of illegal content through properly-functioning systems of self-regulation (such as codes of conduct and establishment of hot-lines) in compliance with and supported by the legal system.

77. Technically it is not possible to access the Internet without the services of an ISP, and therefore the role of the ISPs is pivotal. Content regulation has been to date the most politically prominent aspect of Internet regulation in relation to ISPs. Although no ISP controls third party content or all of the backbones of the Internet, the crucial role they play in providing access to the Internet makes them visible targets for the control of "content regulation" on the Internet.

78. In broad terms ISPs are not guardians or guarantors of Internet content and therefore are not liable to assess, classify or filter all content provided by third parties before its transmission. There are also technical factors that prevent an ISP from blocking the free flow of information on the Internet. First, an Internet service provider cannot easily stop the incoming flow of material to its servers (for example through newsgroups). No one can monitor the enormous quantity of network traffic, which may consist of hundreds of thousands of e-mails, newsgroup messages, files, and Web pages that pass through in dozens of text and binary formats, some of them readable only by particular proprietary tools, through the servers of an ISP. ISPs do have a limited technical ability to detect and control content, but in most cases it would be impossible for a single ISP to judge whether this enormous amount of Internet content contains illegal content according to the laws of the country of service. In fact, the EU Directive on Electronic Commerce[149] which was finalised during the summer of 2000,[150] through article 15, prevents member states from imposing a general monitoring obligation on service providers for actively seeking facts or circumstances indicating illegal activity on their servers.[151]

79. While a general monitoring obligation cannot be imposed upon ISPs this does not stop states issuing blocking orders. During 2002, North Rhine Westphalia, Germany's most populous state issued a blocking-order to prevent German-based ISPs from providing access to Web sites based outside Germany (mainly in the US) if those sites

---

149 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Communities, vol 43, OJ L 178 17 July 2000 p.1. Note also Common Position (EC) No 22/2000 of 28 February 2000 adopted by the Council, acting in accordance with the procedure referred to in Article 251 of the Treaty establishing the European Community, with a view to adopting a Directive on electronic commerce, Official Journal C 128 , 08/05/2000 p. 0032 – 0050.

150 Member States had time until January 2002 to implement the Directive into national law. See generally First Report on the application of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), COM(2003) 702 final, Brussels, 21.11.2003.

151 However, article 15, does not prevent public authorities from imposing a monitoring obligation in a specific and clearly defined individual case.

host racist and neo-Nazi content.[152] The blocking-order affected approximately 76 ISPs within that region.[153] Although there have been legal cases and appeals surrounding the blocking-orders, a number of Administrative courts have ruled that German authorities can continue to ask ISPs to block such pages. Prior to the issuing of the blocking-order, the Dusseldorf District Authority President Jurgen Bussow wrote to four US ISPs in August 2000 requesting that they prevent access to four websites containing racist neo-Nazi material. As this action was unsuccessful Bussow issued the blocking-order to German ISPs within the North Rhine Westphalia region.[154] The utility and effectiveness of such a "blocking regime" remains to be seen but ISPs may be asked to block access to certain websites and content in the future.

A. Notice and Take Down Procedures

80. While ISPs ought to provide law enforcement with reasonable assistance in investigating criminal activity, it is incumbent on law enforcement bodies to initiate and pursue policing action not ISPs. ISPs should ensure that proper authorisation (such as by judicial warrant) is obtained for policing interventions. The above mentioned EU Directive on Electronic Commerce provides a limited and notice based liability with takedown procedures for illegal content. The Directive also required member states and the Commission to encourage the development of codes of conduct,[155] and most of the member states of the EU have left this issue to self-regulation. The service providers need to act expeditiously "upon obtaining actual knowledge" of illegal activity or content "to remove or to disable access to the information concerned."[156] Such removal or disabling of access "has to be undertaken in the observance of the principle of freedom of expression and of procedures established for this purpose at national level"[157] according to the Directive.

81. In terms of the "notice", this has to be specific and may come from an individual complainant or through a self-regulatory hotline and in some countries this may be provided through the law enforcement agencies or courts.

---

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

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

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

[155] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal of the European Communities, vol 43, OJ L 178 17 July 2000 p.1, paragraph 49.

[156] *Ibid*, paragraph 46.

[157] *Ibid*.

B. Hotlines for reporting illegal activity

82. Some ISPs and/or their trade associations, especially in the Western world have developed hotlines to report illegal Internet content. Most of the current Internet hotlines are run privately by industry based organisations and in many countries they are funded by Internet Service Providers. They may constitute centres of expertise providing guidance to ISPs as to what content might be illegal.[158]

83. Internet Hotlines usually allow members of the public and online users to report illegal Internet content to these hotlines. Usually this involves reporting child pornography but some hotlines deal with other types of illegality including racist material.[159] In most cases the hotlines will make an assessment of the report and if the reported content is deemed illegal by the hotline operators, then the content in question will be reported to the appropriate bodies for action including the police, the Internet Service Providers, or if the content in question resides outside the jurisdiction to a correspondent hotline (if exists). Usually upon the receipt of the notice, the ISPs will remove the reported illegal content in question from their servers.

84. There has been international co-operation between various hotlines and the Association of Internet Hotline Providers (INHOPE) has been set up to facilitate and co-ordinate the work of internet hotlines in responding to illegal content on the Internet.[160] Currently it has 18 hotlines[161] as full members,[162] and 7 provisional members.[163]

85. While most hotlines do have expertise in terms of content involving indecent photographs of children under the age of 18 (child pornography), the same may not be said for content involving racist content on the Internet. This type of content could include words, and written material in addition to images, or in some instance just words. Hotlines may not be in a position to judge the suitability or illegality of this type of Internet content. Hotlines are in fact often criticised as there remains serious concerns for the policing role that can be played by such organisations. Many maintain that decisions involving illegality should remain as a matter for the courts of law rather than hotline operators. It has been argued that "these hotlines violate due

---

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

159 During 2004, the Austrian Ministry of the Interior's Internet hotline for reporting National Socialist activity received 140 reports of right-wing extremist activity, particularly in connection with the Internet. See US Bureau of Democracy, Human Rights, and Labor, Report on Global Anti-Semitism, January 2005, at <http://www.state.gov/g/drl/rls/40258.htm>.

160 INHOPE - Internet Hotline Providers in Europe is a project under the EC Daphne Programme to encourage co-operation between European Internet Hotline providers to reduce the level of child pornography on the Internet. For details see <http://www.inhope.org/>.

161 Some but not all of the members of Inhope deal with racist Internet content. See the hotlines from Austria, France, Germany, Greece, Ireland, UK, and Spain in relation to reporting racist Internet content.

162 Full member hotlines are from Australia, Austria, Belgium, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Netherlands, South Korea, Spain, Taiwan, United Kingdom and the United States.

163 Provisional members are from Brazil, Canada, Cyprus, Greece, Hungary, Lithuania, and Poland.

process concepts that are also enshrined in international, regional, and national guarantees around the world." [164]

86. While it may be tempting to identify and attempt to block content posted to particular newsgroups, Web sites, or other Internet forums that seem devoted to illegal material such measures could set dangerous precedents if hotlines assume the role of the courts. Such an approach could result in an act of privatised censorship that would come to be applied too broadly over time. Although hotlines could play an important role in relation to illegal Internet content there remain significant question marks in terms of their operation.

C. Self-Regulation through Code: Rating & Filtering Systems

87. The development of rating and filtering systems has been encouraged since the mid 1990s to deal with harmful Internet content as a means of user empowerment. Such tools are "promoted in order to enable users to make their own decisions on how to deal with unwanted and harmful content".[165] Rating systems, such as the Platform for Internet Content Selections (PICS),[166] works by embedding electronic labels in web documents to vet their content before a computer displays them.[167] The vetting system could include political, religious, advertising or commercial topics. These can be added by the publisher of the material, or by a third party (e.g. by an ISP, or by an independent vetting body). In addition to the rating systems, several filtering software packages are also available to be used at homes intended to respond to the wishes of parents who are making decisions for their children. The type of harmful/offensive/disturbing/shocking/unwanted or undesirable content that is blocked by various filtering software usually include the following:

- Sexually explicit material
- Graphically violent material
- Content advocating hate
- Content advocating illegal activity, such as drug use, bomb making, or underage drinking and gambling

88. There are currently around 50 filtering products (mainly US-based), [168] and approximately 40 of these block content that advocate or promote hatred and discrimination. For a long time filtering software were seen as preferable alternatives to government legislation including at the US Supreme Court level,[169] and it has been

---

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

[165] The EU Safer Internet Plus Plan 2005, Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005, at <http://europa.eu.int/information_society/activities/sip/programme/index_en.htm>.

[166] Note also the ICRA (Internet Content Rating Association) system which follows from the RSACi system. See <http://www.icra.org/> for further information.

[167] See Computer Professionals for Social Responsibility, "Filtering FAQ" <http://quark.cpsr.org/~harryh/faq.html>. Note that most filtering systems based on third-party rating, such as CyberPatrol, are compliant with the PICS labelling system.

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

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

stated that "promoting filter use does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished."[170] It was argued that filters might well be more effective than certain legislation and impose selective restrictions on speech at the receiving end, and would prevent universal restrictions at the source level. It was, however, acknowledged by the Supreme Court that "filtering software is not a perfect solution because it may block some materials not harmful to minors and fail to catch some that are."[171]

89. It is therefore important to note the limitations and criticisms related to rating and filtering systems. Neither system offers total protection to citizens or addresses content-related problems in full. Key limitations are highlighted below.

1. Limited Functionality of Rating Systems

90. Although various governments welcome the use and development of rating systems, the capacity of these tools is limited to certain parts of the Internet. Rating systems are designed for World Wide Web sites while excluding other Internet-related communication systems such as chat environments,[172] file transfer protocol servers (ftp),[173] peer-to-peer networks (P2P), Usenet discussion groups, real-audio and real-video systems which can include live sound and image transmissions, and finally the ubiquitous e-mail communications. These cannot be rated with the systems that are currently available and therefore the assumption that rating systems would make the Internet a "safer environment" is false as WWW content represents only a fraction of the whole of the Internet. Although it may be argued that the World Wide Web represents the more fanciful and most rapidly growing side of the Internet, problems such as racism are not specific to the World Wide Web. So, in terms of rating systems, their development has been only gradual and it does not seem a realistic expectation that these will ever be widely used.

2. Third Party Systems and Problems with Accountability

91. If the duty of rating is handed to third parties, this could cause problems for freedom of speech and with few third-party rating products currently available, the potential for arbitrary censorship increases. This would leave no scope for argument and dissent because the ratings would be done by private bodies without "direct" government involvement. So far this has not been the case but at the same time self-rating is not booming and from time to time third party rating systems are considered.

---

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

171 *Ibid*.

172 Interactive environments like chat channels cannot be rated as the exchange and transmission of information takes place live and spontaneously.

173 Estimated amount of ftp servers on the Internet is about a million. Some of these online libraries may have offensive content or legal content that may be considered harmful for children.

3. Defective Systems

92. Another downside of relying on such technologies is that these systems[174] are used for the exclusion of socially useful websites and information.[175] It has been reported many times that filtering systems and software are over-inclusive and over-block limiting access and censoring inconvenient websites, or filtering potentially educational materials regarding AIDS, drug abuse prevention, or teenage pregnancy. Filtering software and rating systems are being used to exclude minority views and socially useful sites rather than to protect children.[176] According to the report on Internet Filters by the National Coalition Against Censorship:[177]

- I-Gear blocked an essay on "Indecency on the Internet: Lessons from the Art World", the United Nations report "HIV/AIDS: The Global Epidemic", and the home pages of four photography galleries.

- Net Nanny, SurfWatch, Cybersitter, and Bess, among other products, blocked House Majority Leader Richard "Dick" Armey's official website upon detecting the word "dick".

- SmartFilter blocked the Declaration of Independence, Shakespeare's complete plays, *Moby Dick*, and *Marijuana: Facts for Teens*, a brochure published by the National Institute on Drug Abuse (a division of the National Institutes of Health).

- SurfWatch blocked human-rights sites like the Commissioner of the Council of the Baltic Sea States and Algeria Watch, as well as the University of Kansas's Archie R. Dykes Medical Library (upon detecting the word "dykes").

- X-Stop blocked the National Journal of Sexual Orientation Law, Carnegie Mellon University's Banned Books page, "Let's Have an Affair" catering company, and, through its "foul word" function, searches for *Bastard Out of Carolina* and "The Owl and the Pussy Cat".

93. At the same time some filtering software have been criticized for under-blocking.[178] In general, there is too much reliance on mindless mechanical blocking through identification of key words and phrases. Moreover, this is usually based on the morality that an individual company/organization is committed to while developing their filtering criteria and databases. Broad and varying concepts of

---

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

[175] See generally the PeaceFire.Org's pages at <http://www.peacefire.org> as well as Seth Finkelstein's excellent Anticensorware Investigtations – Censorware Exposed pages at <http://sethf.com/anticensorware/>.

[176] Gay & Lesbian Alliance Against Defamation report, *Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community*, New York, December 1997, at <http://www.glaad.org/glaad/access_denied/index.html>.

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

[178] WebSense, at some stage, published daily list of sexually explicit websites on its own website to show the websites that its competitors did not block. However, anybody -- including students from schools that were using SmartFilter and SurfControl -- could access the list, simply by clicking a button on the WebSense site agreeing that they were over 18. See Peacefire's report on Websense at <http://peacefire.org/censorware/WebSENSE/>.

offensiveness, inappropriateness, or disagreement with the political viewpoint of the manufacturer are witnessed with the development of such tools. Most of the companies creating this kind of software provide no appeal system[179] to content providers who are "banned or blocked", thereby "subverting the self-regulating exchange of information that has been a hallmark of the Internet community."[180]

4. Circumvention is Possible

94. Apart from the worrying defects explained above, circumvention of such tools is relatively easy. There is not only the often-cited example of children uninstalling or removing such software from their computers, but also a software known as Circumventor developed by Peacefire.Org which bypasses any content blocking attempts, including those by the likes of CyberSitter and NetNanny.[181] One of the main motivations behind developing Circumventor was Peacefire.Org's desire to bypass censorship of political websites. It is a well-known fact that almost all Internet users in China[182] and the Middle East[183] are blocked from accessing a considerable number of political websites. Technologies like Circumventor can help Internet users in censored countries to access such websites. In addition to Peacefire.Org's Circumventor, websites providing anonymous proxy services and anonymous web surfing, such as anonymizer.com, as well as the Electronic Frontier Foundation's (EFF) TOR network[184] and onion routers can also be used to bypass filtering. It is, however, often the case that the filters block such well-known websites and proxy servers. That is why Peacefire.Org's Circumventor, accessed through an unknown IP address (or known to a limited number of users), provides better success in circumvention and avoids possible unintended risks associated with circumvention technologies.[185]

5. Freedom of Expression & Censorship

95. Problems associated with rating and filtering systems were also acknowledged at the European Union level. As the Economic and Social Committee of the European Commission pointed out in its report[186] on the European Commission's Action Plan

---

[179] Some companies provide a review mechanism and other let their databases searched online. But in most cases an online content provider would not know if their web pages are blocked or not by a filtering software unless that software is tested by the content provider. Considering the number of such software, it is an impossible task to find whether a certain software blocks or not a certain website and for what reason.

[180] See CPSR letter dated 18 December 1996 sent to Solid Oak, the makers of CyberSitter at <http://www.cpsr.org/cpsr/nii/cyber-rights/>.

[181] For further information about PeaceFire.Org's Circumventor, see <http://www.peacefire.org/circumventor/simple-circumventor-instructions.html>.

[182] Note OpenNet Initiative report, *Probing Chinese search engine filtering*, August 2004, at <http://www.opennetinitiative.net/bulletins/005/>.

[183] See generally the Documentation of Internet Filtering Worldwide pages of the Berkman Center for Internet & Society, Harvard Law School, at <http://cyber.law.harvard.edu/filtering/>.

[184] See <http://tor.eff.org/>.

[185] See in detail the OpenNet Initiative report, *Unintended Risks and Consequences of Circumvention Technologies: The IBB's Anonymizer Service in Iran*, May 2004, at <http://www.opennetinitiative.net/advisories/001/>.

[186] Economic and Social Committee of the European Commission, Opinion on the Proposal for a

on promoting safe use of the Internet, it is highly unlikely that the proposed measures will in the long term result in a safe Internet with the rating and classification of all information on the Internet being "impracticable". [187] More importantly, the Committee was worried that the possibility of Internet service providers using filtering and rating systems at the level of entry would render these systems, dubbed as "user empowering", an instrument of control, "actually taking choice out of citizens' hands." The Committee concluded that there is "little future in the active promotion of filtering systems based on rating."[188]

6. Blocking rather than removal

96. As highlighted in this report, racist Internet content is often difficult to categorise and is not always categorised as "illegal content". If such content does not pass the illegality threshold then it must always be recognised that such speech or content are not to be prohibited at source. Although they could be regarded as harmful and offensive to some audiences, it is a matter for the audiences to decide whether they want to access the expression. Filtering software can help audiences to make that decision and block access to certain types of Internet content. However, removal of such legal content from public networks would not be consistent with fundamental human rights such as freedom of expression.

D. Information, Education, and Awareness Campaigns

97. The Internet itself can be an effective tool in the fight against racism.[189] The need to promote the use of new information and communication technologies, including the Internet, to contribute to the fight against racism, racial discrimination, xenophobia and related intolerance[190] is recognised by the Durban Declaration. According to the Declaration "new technologies can assist the promotion of tolerance and respect for human dignity, and the principles of equality and non-discrimination."[191] As noted by an April 2000 UN report leading into the Durban World Conference "governments, intergovernmental organizations, national human rights institutions and non-governmental organizations are using the Internet to inform the public about their work and to spread positive messages of equality and non-discrimination." [192] A number of initiatives aim to assist parents and teachers in preparing children for safer

---

Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet, (OJEC, 98/C 214/08, Brussels-Luxembourg, 10 July, 1998) pp.29-32.

187 *Ibid* para 4.1.

188 See *ibid*. See further Akdeniz, Y., "The Regulation of Internet Content in Europe: Governmental Control versus Self-Responsibility," (1999) *Swiss Political Science Review* 5(2), Summer, 123-131.

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

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

191 *Ibid*.

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

use of the Internet,[193] and within this context a recent Partners Against Hate initiative report highlights critical thinking skills as "one of the most effective tools to provide young people with protection against hate on the Internet."[194]

98. The same approach has been adopted at the OSCE level with recommendations that

> "Internet users should be educated about tolerance and that cooperation should be promoted among all actors, particularly nongovernmental organizations and associations working to combat racist, anti-Semitic and xenophobic propaganda on the Internet."[195]

99. States and international organisations should continue to invest in education[196] and awareness raising[197] campaigns to "provide users, particularly young people, with accurate information on the dangers of racism and anti-Semitism so as to counter the influence of racist organizations." [198] Information, education, and awareness campaigns should be a "crucial component in any initiative or programme to combat racism."[199]

100. In summary, there are currently no specific self and co-regulatory measures, including codes of conduct aimed at combating racist Internet content as recommended by the Durban Programme of Action.[200] There remain significant question marks[201] over the effectiveness and efficacy of the various mechanisms and tools currently offered by the private sector. Self and co-regulatory measures may yet play an important role in the fight against racist Internet content. This will however be

---

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

[194] *Ibid*., at page 30. The report cites John Dewey describing critical thinking skills as "active, persistent, and careful consideration of any belief or supposed form of knowledge in the light of the grounds that support it and the further conclusion to which it tends." See Dewey, J. (1938). *Experience and Education.* New York: Macmillan Publishers.

[195] The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/59/329, 7 September 2004.

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

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

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

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

[200] See paragraph 144 of the Durban Programme of Action.

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

dependent upon substantial improvement of existing systems or the devising of less problematic alternatives.

IX. Conclusion

1. In line with Recommendation 22 of the IGWG, this report has sought to assess the possibilities of and challenges posed by the use of the Internet to propagate or to counter material of a racist nature. Measures taken at the international and national levels as well as by the private sector to combat racist Internet content have been highlighted.

2. A number of themes surfaced from this analysis with the most prominent being the fact that "States have yet to reach a political agreement on how to prevent the Internet being used for racist purposes and on how to promote its use to combat the scourge of racism."[202] Some regard harmonised national legislation and international agreements as the way forward. For example, the European Commission against Racism and Intolerance (ECRI) believes, "national legislation against racism and racial discrimination is necessary to combat these phenomena effectively."[203] Others strenuously oppose this position, citing objections on grounds of freedom of expression. It has been noted, for example, at the OSCE level that "the United States opposes any regulation, on freedom of expression, while the European countries are more in favour of a policy of monitoring and sanctions."[204] Hence, fundamental "disagreements remain on the most appropriate strategy for preventing dissemination of racist messages on the Internet, including the need to adopt regulatory measures to that end".[205] This lack of consensus threatens the implementation of legal sanctions in accordance with relevant international human rights legal instruments, in particular the ICERD as recommended by paragraph 147 of the Durban Programme of Action. It is possible that the strengthening and updating of international instruments, most notably, the ICERD, may result in wider agreement. At the same time, the absence of a global consensus on the limits of freedom of expression may remain an obstacle to regulatory harmonisation through the CoE Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems or any other future international agreement or convention.

3. Another associated factor to emerge from this report is the extent of duplication of efforts at the supranational, and international levels of governance. This duplication

---

202 Racism, Racial Discrimination, Xenophobia And All Forms Of Discrimination Report submitted by Mr. Doudou Diène, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E/CN.4/2005/18, 13 December 2004.

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

204 The fight against racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Note by the Secretary-General, A/59/329, 7 September 2004.

205 The meeting on the relationship between racist, xenophobic and anti-Semitic propaganda on the Internet and hate crimes held by the Organization for Security and Cooperation in Europe (OSCE) in Paris on 16-17 June 2004.

has resulted in delays in finalising policies within relevant organisations, and in its subsequent implementation at the national level to address Internet related problems. Governments and international organisations are, however, reacting more positively against the dissemination of racist content through the Internet,[206] and there is more awareness of the nature of the problem including the use of the Internet by terrorist organisations for terrorist propaganda and inciting terrorist violence,[207] as well as the resurrection of Nazi ideology in Europe.[208]

1. Future Directions

4. Looking to the future, one can expect a trend towards "governance" rather than "government", where the role of the nation state is not exclusive and where more varied forms of regulation, many in the private sector, come into play. The governance of the Internet will continue to evolve at the national, and international levels[209] "regardless of frontiers",[210] and policy initiatives will continue to reflect the decentralised nature of the Internet. As this report has sought to demonstrate, in the fight against racist Internet content no one approach promises to be entirely effective. The emergence of Internet governance entails a more diverse and fragmented regulatory network with no presumption that these are anchored primarily in the nation-states. Although legal regulation will doubtless form an important part of future efforts to tackle the problem of online racism it will only ever form part of the solution. Ultimately, it will prove necessary to rely on additional measures in the form of self and co-regulatory initiatives. The success of these measures will, in turn, depend upon substantial improvement of existing systems including the development of codes of conduct aimed at combating racist Internet content as recommended by

---

206 Global efforts for the total elimination of racism, racial discrimination, xenophobia and related intolerance and the comprehensive implementation of and follow-up to the Durban Declaration and Programme of Action, Report of the Secretary-General, A/60/307, 29 August 2005.

207 Note the UN Resolution 1617 (2005) Adopted by the Security Council at its 5244th meeting, on 29 July 2005. Note also the ADL report, *JIHAD Online: Islamic Terrorists and the Internet*, 2002, at <http://www.adl.org/internet/jihad_online.pdf>, Weimann, G., *www.terror.net: How Modern Terrorism Uses the Internet*, United States Institute of Peace, March 2004, at <http://www.usip.org/pubs/specialreports/sr116.pdf>.

208 Parliamentary Assembly of the Council of Europe, *Combating the resurrection of Nazi ideology*, Report by the Political Affairs Committee (Rapporteur: Mr Mikhail Margelov, Russian Federation, European Democrat Group), Doc. 10766, 19 December 2005, at <http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc05/EDOC10766.htm>. Note also Parliamentary Assembly of the Council of Europe, Resolution 1345 (2003) on Racist, xenophobic and intolerant discourse in politics, at <http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/AdoptedText/ta03/ERES1345.htm>. Assembly debate on 29 September 2003 (26th Sitting). See further Doc. 9904, report of the Committee on Legal Affairs and Human Rights, Rapporteur: Mr McNamara at <http://assembly.coe.int/Main.asp?link=http://assembly.coe.int/Documents/WorkingDocs/doc03/EDOC9904.htm>). Text adopted by the Assembly on 29 September 2003 (26th Sitting).

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

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

the Durban Programme of Action.[211] If successful these measures would potentially be more flexible and more effective than prescriptive government legislation.

5. Consistent with recommendation 141 of the Durban Programme of Action, education about racist content on the Internet and how to foster tolerance, is arguably the single most effective way of combating racist content.[212] To this end, it is crucial that States provide more data and annual reports to various monitoring bodies which would help to better understand the nature of the problem on the Internet. Failure to report and failure to provide up to date reliable data on policy initiatives and measures undertaken by States at the domestic level to address the problem of racism will undoubtedly delay progress which could be achieved at the international level.

6. Equally significant is the continued participation of all stakeholders, *inter alia* States, WSIS, international and regional organizations, NGOs, the private sector and the media, in ongoing discussions and the fostering of a wider public debate. In this regard the high level seminar on racism and the Internet to be held in Geneva on 16-17 January, 2006 offers important opportunities for the exchange of ideas and the formulation of effective future strategies.

---

[211] See paragraph 144 of the Durban Programme of Action.

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