5.8 The EESC maintains that Regulation 4056/86 should be repealed and substituted by a new Commission Regulation for liner conferences granting a block exemption. The new regime should strictly follow the yardsticks established under the jurisprudence of the European Court of First Instance and of the Commission (e.g. TACA case). The conference system should also be maintained in order to defend the competitiveness of Community shipowners worldwide. Whilst for the large carriers 'alliances' and other types of cooperation agreements may be appropriate, small and medium size carriers still need conferences in order to maintain their market shares especially in trades with developing countries. The abolition of the exemption may have anticompetitive effects for these small carriers enhancing the dominant position of the larger ones.

5.9 This interim transitional period should be used by the Commission to monitor the liner market developments including trends of consolidation. Moreover, the Commission should undertake consultations with other jurisdictions (OECD) with a view to arriving at a suitable alternative system compatible worldwide.

5.10 The EESC endorses proposals of the White Paper regarding the treatment of tramp and cabotage services since the vast majority of cases in these sectors would not raise competition problems. For the sake of legal certainty, however, the Commission is requested to provide legal guidance regarding the self assessment of bulk pools and specialized trades regarding their compatibility with Article 81 EC.

5.11 The EESC hopes to provide its assistance in the follow-up to the brainstorming exercise launched by the White Paper.

Brussels, 16 December 2004

The President
of the European Economic and Social Committee
Anne-Marie SIGMUND

Opinion of the European Economic and Social Committee on the 'Proposal for a Decision of the European Parliament and of the Council on establishing a multiannual Community programme on promoting safer use of the internet and new online technologies'

(COM(2004) 91 final — 2004/0023 (COD))

(2005/C 157/24)

On 26 March 2004, the Council decided to consult the European Economic and Social Committee, under Article 153 of the Treaty establishing the European Community, on the abovementioned proposal.

The Section for Transport, Energy, Infrastructure and the Information Society, which was responsible for preparing the Committee's work on the subject, adopted its opinion on 5 October 2004. The rapporteur was Mr Retureau and the co-rapporteur, Ms Davison.

At its 413th plenary session on 15 and 16 December 2004 (meeting of 16 December 2004), the European Economic and Social Committee adopted the following opinion by 147 votes in favour with 1 abstention:

1. Summary of the draft opinion

1.1 The Commission proposes to launch a new Safer Internet Programme, which is to be enhanced to reflect the rapid development of the Information Society in terms of communications networks. It has therefore been named the Safer Internet Plus Action Plan (2005-2008).

1.2 Besides the proposal for a Decision of the European Parliament and of the Council submitted by the Commission, the Committee has examined the ex ante evaluation of Safer Internet Plus (2005-2008), set out in a Commission staff working paper (SEC(2004) 148), and in COM(2004) 91 final. It supports broadening the scope of the new action plan and its objectives to reflect the rapid development and diversification of Internet access and the very rapid growth of broadband connections. In its general and specific comments on the subject, the Committee offers some additional proposals for political and regulatory measures, in particular:

— technical and legal standards (compulsory and voluntary);

— education and training of users;

— obligations of Internet service providers and other operators (credit card companies, search engines, etc.);

— the responsibility of software authors and Internet security providers;

— the protection of vulnerable individuals against fraud and information from doubtful sources (various scams, uncontrolled sales of medicines, advice and treatment from persons without any medical authority, etc.).

2. Proposals of the Commission (summary)

2.1 The aim of the proposed programme is to promote safer use of the Internet and online technologies for end users, and in particular for children and young people, at home or at school. To this end, it is planned to co-finance projects put forward by associations and other groups (research teams, software designers, educational institutions, etc.), with the aim of developing means of protection such as hotlines, spam and virus filters, and 'smart' navigation filters.

2.2 The previous Safer Internet Action Plan (1999-2002) was extended to the period 2003-2004.

2.3 The website of the European Commission lists the projects which had already been completed under the Safer Internet Programme by the end of 2003. [1]

2.4 The current proposal (for 2005-2008) also covers new forms of online communication, for which it provides support in combating illegal and harmful content, including viruses and other harmful or unwanted content (e.g. spam).

2.5 For the institutions of the European Union, the main reasons why measures need to be taken in this area are:

— rapid growth in the use of high-speed and broadband connections by individual users, businesses, government administration and private institutions (NGOs);

— diversification of media and methods of access to the Internet and new online content, much of which is unwanted (e-mails, text messages), and increasingly attractive content (multimedia);

— the dramatic increase in unwanted, potentially dangerous or inappropriate content has created new dangers for the general public (viruses: invade memory, abuse or destroy data, make unauthorised use of the victim's communication media; spam: clogs up bandwidth and memory, invades electronic mailboxes, with the result that effective use of the Internet and communication is either blocked or made more difficult, and causes significant costs, borne not by those are responsible but by end users); some significant categories of users, such as children, are at risk from sexually explicit spam, inappropriate messages and invitations by paedophiles to dates in online chat rooms;

— inappropriate content easily accessible to children, due to the limited effectiveness of current filtering systems available to those in charge of children.

2.6 The main objective of the programme is to protect children and support those in charge of them (parents, teachers, educators, etc.) and those defending their interests and their moral health. The programme therefore concerns NGOs dealing with social issues, children's rights, racism, xenophobia [2] and all other forms of discrimination, consumer rights, the defence of civil liberties, etc.

2.7 The programme also concerns governments, legislative, judicial and police bodies, and regulatory authorities. Changes need to be made both to laws and to legal procedures, and training and equipment need to be provided for a sufficient number of staff.

2.8 In addition, the programme concerns the industry, which needs a secure environment in order to boost consumer confidence.

2.9 Universities and researchers can shed light on how children use the new media. The best approach to effective communication on the issue of security is to make the public aware of how criminals make use of the new media, to search for new technological solutions, and to provide an independent perspective on finding a balance between the interests affected by regulatory and self-regulatory procedures.

2.10 There are two dimensions to the programme. On the social front, it focuses on areas where regulation and the market are not sufficient in themselves to guarantee the safety of users. On the economic front, it aims to promote safer use of the Internet and online technologies by creating a climate of confidence.

2.11 About €50 million of funding is planned to develop legal and technological measures, software and information in order to combat invasion or fraudulent use of networks or computers through unwanted content which has the potential to be morally, socially or economically harmful.

[1] http://www.europa.eu.int/information_society/programmes/iap/index_en.htm

[2] Topics covered previously by the Committee

3. **General comments by the Committee**

3.1 The Committee refers to its previous position on protection of children on the Internet and its first action plan. [1] It welcomes the proposal for a new action plan to deal with illegal and harmful content in online communication (see Section 1, Summary, at the beginning of this document), and it supports the objectives and priorities of the Safer Internet Plus Programme, as one of the strategies intended to make Internet use safer. However, the Committee emphasises the enormity of the problem and the need for international measures and legislation to deal with it.

3.2 In the view of the Committee, the Internet and new technologies for online communication (for example, mobile telephones and palmtop computers with Internet and multimedia functions, currently undergoing rapid growth) are of fundamental importance for the development of the knowledge economy, the e-economy and e-government. They are flexible communication tools used for culture, work and free time. Therefore, it is vital to ensure that communications networks can function safely and smoothly, given that they are an essential public service which needs to remain open and accessible, and which needs to inspire the confidence of all users in order to fulfil its various functions in the best possible conditions. Including information on safer Internet use in the various e-Europe programmes, and training activities in particular, is one of the most promising ways forward, as a cost-effective means of reaching the largest possible number of people.

3.3 Conducive to the freedom of expression and communication prevailing on the Internet are the relatively low costs of Internet access, including broadband connections, which provide increasingly fast access to multimedia content. Only a few countries with significant democratic deficits seek to monitor the messages and contents available to their nationals, at the cost of permanent impairment to freedom. In the opinion of the Committee, it is important to guarantee increased security while at the same time preserving and promoting freedom of information, communication and expression.

3.4 However, the Internet, as a global medium of free expression and information, is used for illegal activities such as paedophilia and the dissemination of racist or xenophobic content to an even greater extent than other forms of communication. Some types of content may also be harmful for particular groups of users, especially minors, such as pornography and gambling (which are actually prohibited in some countries) or those related to various criminal activities (abuse of bandwidth, or fraudulent use of data or servers). The Committee is therefore in favour of broadening the scope of the action plan to cover all forms of electronic communication which are capable of being used for unwanted or hostile external access.

3.5 Regulation of this new and rapidly growing area has become complex due to the fact that the Internet is an international, open network accessible to everyone through any server or any personal computer, with unrestricted access from practically any country in the world. However, many countries still have weak or insufficient legislation permitting the operation of websites which are banned in the European Union. It is very important for the European Union, in cooperation with the main North American and Asian countries where broadband Internet use is widespread, to speak out and to campaign for international measures to protect those who are most vulnerable, to take more effective action against unsolicited messages (spam), which threaten the development of electronic mail, and against the proliferation of computer viruses, which undermine the digital economy. Necessary though such action is within the European Union, the measures need to be implemented as part of a global approach.

3.6 Given the lack of international agreements, prohibition of certain types of content by some countries may even be contested by complaints lodged with the WTO concerning TBTs [2]; this is an issue which needs to be discussed during the current round of negotiations.

3.7 The territoriality of law and the diversity of national legislation make it difficult to deal with the problem. The current state of technology also permits individuals to send each other all kinds of files directly (P2P, peer-to-peer), including encoded files whose contents cannot be checked; any computer or online network can be used to store or send increasingly sophisticated content, and it is possible to connect to any server without revealing one's identity or leaving a trail, and to use encryption technologies which are very resistant or even impossible to crack.

3.8 As a result of the fashion for personal websites and blogs, the development of online shopping and financial services, the multitude of educational, informative, scientific and technical websites, and also online pornography and gambling, there are hundreds of millions of websites all over the world. However, to some extent these can be checked during the compilation of key words by search engines. Internet service providers can also monitor direct connections and websites which automatically forward contents such as spam; advertising and other unwanted messages which these are used for can be generally harmful (clogging up bandwidth, viruses) or can affect particular users such as children (moral or psychological ill-effects).

[1] EESC opinions on *A programme for child protection on the Internet*, rapporteur: **Ms Davison**, O.J. C48, 21/02/2002, on the *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach*, rapporteur: **Mr Retureau**, O.J. C48 of 21/02/2002 and the *Green Paper on the protection of minors and human dignity in audiovisual and information services*, rapporteur: **Ms Barrow**, O.J. C 287, 22/09/1997.

[2] 'Technical Barriers to Trade'. Agreements on technical barriers to the exchange and provision of services. See e.g. USA vs. Antigua and Barbuda - offshore gambling; appeal against the WTO panel decision (http://www.wto.org/english/tratop_e/dispu_e/distabase_wto_members1_e.htm), Document 03-4429, page WT/DS285/3, 26/08/2003. Case pending.

3.9 The Internet is used by gangs, racketeers, virus authors, those engaged in piracy and industrial espionage, and other criminals. Stamping out this kind of crime is difficult, even though many countries have specialised police departments to identify, track and stop such activities, and it usually requires international cooperation, which should be encouraged more strongly.

3.10 How can criminal activities such as paedophile websites be dealt with? Although prohibiting such activities is unlikely to pose a legal problem, it is important to put in place the resources for tracking down criminal networks. It is also important to protect children from paedophiles searching for dates in online chat rooms, which are especially popular with young people. The question that needs to be answered here is not whether it is legitimate to prohibit and prosecute such activities, but what resources are needed to do so.

3.11 Internet service providers (ISPs) are unable to monitor and check all the websites hosted by them or messages between users (which are private correspondence). However, if they are called on to do so by an authorised judge, police department, or authority responsible for protecting children, ISPs are required to immediately respond to requests or rulings concerning closure of such websites and identification of the persons using them, which necessitates preserving publication details of websites and information about visits to websites for a certain period.

3.12 However, credit card companies, search engines and Internet service providers should, for example, carry out sample audits to track down websites offering paedophile or other criminal content, using clues such as key words and geographical areas. They could then report these to the police. The same techniques should be used to identify ‘customers’ ordering ‘customised’ child pornography and snuff movies [1] by credit card. If necessary, legislation should require such audits. Internet search engines should also make it harder for surfers to find child pornography and other criminal content through the use of key words and phrases.

3.13 For this to happen, there is a need for public authorities to be provided with appropriate resources and trained staff, for wide-ranging international cooperation, and for regulation at national, European and international levels which strikes a balance between, on the one hand, preserving the rights of Internet users and, on the other, preventing individuals and groups from using the Internet to send illegal content, and enabling recipients to opt to block inappropriate or harmful content.

3.14 In addition, to be effective, this programme should directly involve all Internet users, who need to be trained and informed of the precautions to take and the resources to use in order to protect themselves from being sent harmful or unwanted content, or from being used to forward such content. In the view of the Committee, one of the priorities of the action plan in regard to information and training should be to gain the support of users and to make them responsible for themselves and their dependants. A problem is presented by unregulated health sites for example. To protect themselves, companies should also focus on staff training and making e-commerce networks and websites secure. In addition, government administration and private and state institutions should apply similar security policies to ensure absolute confidentiality of data, and personal data in particular. Awareness raising should be accompanied by promotion of quality online content, and also encouragement of offline activities as alternatives to prolonged surfing or certain role-playing games which can have long-term effects on immature individuals.

3.15 Facilities should be in place to make it easy for users to report illegal content which they find on networks to specialised emergency call centres, recognised organisations or specialised police departments, in order to alert the authorities and enable them to take suitable measures when necessary. Parents should be alerted in countries where children are frequently abused for pornographic purposes, whether online or through other media, for example on the external borders of the European Union; such measures could be included in some RELEX cooperation programmes.

3.16 While lending its support to the specific objectives of the programme, i.e. to enable users to report illegal content (hotlines), to develop technologies for filtering out unwanted content, to classify content, to combat spam, to encourage self-regulation of the sector, and raise awareness of safe Internet use, the Committee suggests in its specific comments some additional objectives which are worth considering.

4. **Specific comments by the Committee**

4.1 In the past, the Committee has already urged the Commission to cut red tape in EU-funded programmes, so that micro-projects and local NGOs have easier access to funding. The Committee supports monitoring which focuses on the tangible results achieved under the programme and the effectiveness of the proposed solutions. Solutions should be disseminated in a less confidential manner.

4.2 The Committee believes that it is worth considering legislative measures contributing to the protection of end users, if possible within the framework of the programme, or otherwise through a new initiative by the Commission.

[1] Films in which actual violence, torture and murders are recorded.

4.3 Authors of Internet access software, server operating systems and firewall programmes should bear full responsibility for their products; it should be guaranteed to users that authors of such software make use of state-of-the-art technology and regularly update their products. Customer guarantees should be backed up by self-regulation, or, in the absence of this, legislation at European level.

4.4 Internet access providers should offer (as many of them already do) easy-to-use anti-virus and spam filtering facilities for e-mail and attached files. This could confer a commercial advantage on providers who take protection of their customers seriously. Given that children are often more knowledgeable about Internet use than their parents, spam filters, virus screens, firewalls and parental control systems should be pre-installed, and sufficiently user-friendly not to require any specialised knowledge.

4.5 The programme should also promote research into specialised software and other means of checking how attack-resistant the code of various filtering and blocking software is, as well as encouraging or possibly requiring producers to promptly supply patches for all security flaws which have been identified or reported, and to develop the effectiveness of firewall hardware and software, and methods for filtering and identifying the actual origin of content.

4.6 The Committee would have liked to see the evaluation of the effectiveness and results achieved by the previous Safer Internet Programme, classed according to the type of problems which the projects dealt with, disseminated more widely. All links to funded projects should be kept active, and those concerned should be made aware of them. The Commission website should also include information on initiatives in Member States and third countries in order to promote the transfer and exchange of knowledge and effective cooperation.

4.7 It is perfectly possible to take legal measures. Internet service providers, credit card companies and search engines are all capable of being regulated, and some have already introduced self-regulation. Rigorous criminal sanctions should act as an effective deterrent against websites promoting terrorism, racism, suicide or child pornography. International action should be undertaken on as wide a scale as possible to identify and trace such websites so that whenever possible they can be closed down; failing this, negotiations on closure can be initiated with host countries.

5. **Conclusions**

While supporting extension of the Safer Internet Plus Programme, and having initially called for its introduction, the Committee believes that the extent to which especially children are threatened with abuse, and the gravity of such threats, urgently necessitate additional legislative measures and appropriate practical steps in the following areas:

— there should be a general obligation incumbent on all operators to protect children and users in general, particularly those who are most at risk;

— filter systems should be installed by default;

— safety warnings should be clearly displayed on all home pages and portals providing access to chat rooms;

— there should be support for organisations setting up hot lines for reporting websites and online activities which are harmful to children;

— the use of credit cards for ordering child pornography and other criminal content on the Internet and for money laundering operations should be prevented;

— parents, educators and authorities in countries where abuse of children for pornographic purposes has become a cause for concern should be alerted through targeted measures;

— more action is needed to tackle the links between exploitation of children for pornographic purposes and organised crime;

— systems should be set up to identify and provide information on harmful content, and to remove racist content; online scams and sales of substances which pose a health risk should be publicised in order to protect vulnerable or ill-informed individuals;

— there should be international cooperation and joint regulation to combat spam more effectively;

— there is a need for international cooperation (improving the early warning system) and deterrent criminal sanctions for creators of computer viruses and for illegal use of private and public networks for criminal purposes (intrusion with a view to using networks for industrial espionage, abuse of bandwidth, and other forms of abuse).

Brussels, 16 December 2004.

The President
of the European Economic and Social Committee
Anne-Marie SIGMUND