5.8 Het EESC blijft erbij dat Verordening 4056/86 moet worden ingetrokken en vervangen door een nieuwe Verordening van de Commissie voor lijnvaartconferences die in een groepsvrijstelling voorziet. Het nieuwe regime dient strikt gebaseerd te zijn op de voorwaarden die in de jurisprudentie van het Gerecht van Eerste Aanleg en van de Commissie zijn geformuleerd (bijv. de TACA-zaak). Het conferencesysteem dient ook gehandhaafd te worden om het concurrentievermogen van communautaire reders in de hele wereld te beschermen. Allianties en andere vormen van samenwerking mogen dan wel geschikt zijn voor grote scheepvaartmaatschappijen, maar kleine en middelgrote ondernemingen kunnen niet zonder conferences om hun marktaandelen te behouden, met name op de routes met ontwikkelingslanden. Intrekking van de vrijstelling kan de concurrentiepositie van deze kleine ondernemingen aantasten en de dominante positie van grotere scheepvaartmaatschappijen verder versterken.

5.9 Deze overgangsperiode zou door de Commissie gebruikt moeten worden om de ontwikkelingen op de lijnvaartmarkt, waaronder consolidatietendensen, in het oog te houden. Bovendien zou de Commissie overleg moeten voeren met andere rechtsgebieden (OESO) om te komen tot een adequaat alternatief systeem dat overal ter wereld toegepast kan worden.

5.10 Het EESC steunt voorstellen in het Witboek inzake de behandeling van de wilde vaart en cabotage, aangezien de overgrote meerderheid van de gevallen in deze sectoren geen problemen op mededingingsgebied zal opleveren. Ter wille van de rechtszekerheid wordt de Commissie echter verzocht te zorgen voor een juridische leidraad met betrekking tot bulkpools en gespecialiseerde vaart, zodat de scheepvaartmaatschappijen zelf kunnen nagaan of hun activiteiten verenigbaar zijn met art. 81 van het EG-Verdrag.

5.11 Het EESC hoopt behulpzaam te kunnen zijn met de follow-up van de brainstorming waartoe de Commissie in dit Witboek de aanzet heeft gegeven.

Brussel, 16 december 2004

De voorzitter
van het Europees Economisch en Sociaal Comité
A.-M. SIGMUND

Advies van het Europees Economisch en Sociaal Comité over het „Voorstel voor een beschikking van het Europees Parlement en de Raad betreffende de vaststelling van een communautair meerjarenprogramma ter bevordering van een veiliger gebruik van het internet en nieuwe online-technologieën"

(COM(2004) 91 def. — 2004/0023 (COD))

(2005/C 157/24)

De Raad heeft op 26 maart 2004 besloten, overeenkomstig de bepalingen van art. 153 van het EG-Verdrag, het Europees Economisch en Sociaal Comité te raadplegen over voornoemd voorstel.

De gespecialiseerde afdeling „Vervoer, energie, infrastructuur, informatiemaatschappij", die met de voorbereidende werkzaamheden was belast, heeft haar advies op 5 oktober 2004 goedgekeurd (rapporteur was de heer RETUREAU, co-rapporteur mevrouw DAVISON).

Het Comité heeft tijdens zijn 413e zitting op 15 en 16 december 2004 (vergadering van 16 december 2004) het volgende advies uitgebracht, dat met 147 stemmen vóór en zonder stemmen tegen, bij 1 onthouding, is goedgekeurd.

1. **Samenvatting van het ontwerpadvies**

1.1 De Commissie stelt voor een nieuw programma „Safer Internet" te lanceren. Dit versterkte programma moet rekening houden met de snelle ontwikkelingen in de informatiemaatschappij op het gebied van de communicatienetwerken. Het programma wordt „Safer internet plus" genoemd (2005-2008).

1.2 Behalve het door de Commissie ingediende voorstel voor een beschikking van het Europees Parlement en de Raad heeft het Comité zich gebogen over het *werkdocument van de Commissiediensten* over de evaluatie ex ante van *Safer internet plus* (2005-2008) (SEC(2004)148 en COM(2004) 91 def.). Het stemt in met de uitbreiding van het toepassingsgebied van het nieuwe actieplan en de doelstellingen daarvan, waarbij rekening wordt gehouden met de snelle ontwikkelingen en de diversifiëring van de mogelijkheden voor online-toegang, en de explosieve groei van het aantal hogesnelheids- en permanente verbindingen. In de algemene en bijzondere opmerkingen formuleert het EESC enkele aanvullende voorstellen voor beleids- en wetgevende maatregelen, met name:

— technische en juridische voorschriften (verplicht en vrijwillig);

— educatie/opleiding van gebruikers;

— verplichtingen voor aanbieders van toegang en ruimte, en voor andere exploitanten (kredietkaartmaatschappijen, zoekmotoren, enz.);

— de verantwoordelijkheid van auteurs van software en leveranciers van beveiligingsmiddelen;

— de bescherming van kwetsbare personen tegen fraude of twijfelachtige informatie (verschillende soorten oplichterij, „vrije" verkoop van geneesmiddelen, gezondheidsadviezen of behandelingen door personen zonder medische bevoegdheid, enz.).

2. **Voorstellen van de Commissie (samenvatting)**

2.1 Het voorgestelde programma is gericht op de bevordering van een veiliger gebruik van het internet en van online-technologieën door de eindgebruiker, met name voor kinderen en jongeren, zowel thuis als op school. Hiervoor zullen projecten van verenigingen en andere groepen (onderzoekteams, ontwerpers van software, onderwijsinstellingen, enz.) worden gecofinancierd, om hen te helpen beschermende middelen te ontwikkelen, zoals „hotlines", anti-spam en antivirusprogramma's, en intelligente filtertechnologieën.

2.2 Het vorige plan voor een veilig internet (1999-2002) is verlengd voor de periode 2003-2004.

2.3 Op de website van de Commissie staan de projecten die, tot eind 2003, reeds werden gerealiseerd in het kader van het programma *Safer Internet*. ([1])

2.4 Het onderhavige voorstel (voor de periode 2005-2008) heeft tevens betrekking op de nieuwe online-communicatiemiddelen; de Commissie wil de strijd tegen illegale en schadelijke inhoud opvoeren, met inbegrip van virussen en andere schadelijke of ongevraagde inhoud (*spam*).

2.5 Er zijn verschillende redenen voor de EU-instellingen om deze strijd op te voeren, maar de belangrijkste zijn:

— de snelle ontwikkeling van langdurige of permanente hogesnelheidsverbindingen van particulieren, ondernemingen, overheden en particuliere organisaties (NGO's);

— de diversifiëring van de mogelijkheden voor de toegang tot internet en nieuwe online-inhoud, vaak ongevraagd (*mails, SMS*), en een aantrekkelijker inhoud (multimedia);

— de enorme explosie van ongevraagde en potentieel gevaarlijke of ongeschikte inhoud brengt nieuwe gevaren met zich mee voor het grote publiek (virussen: het binnendringen van het geheugen, misbruik of vernietiging van gegevens, een ongeautoriseerd gebruik van de communicatiemiddelen van het slachtoffer; *spam-mails*: misbruik van de breedband en het geheugen, binnendringing van de elektronische mailbox, waardoor het gebruik van internet en de communicatie worden geblokkeerd of bemoeilijkt, vaak met aanzienlijke kosten (waarvoor niet de „vervuiler", maar de eindgebruiker opdraait); soms zijn deze gericht op bepaalde grote groepen gebruikers, zoals kinderen (expliciet seksueel getinte *spams*, ongeschikte boodschappen en pedofielen die via *chatrooms* met kinderen afspraakjes proberen te maken);

— inhoud die ongeschikt maar gemakkelijk toegankelijk is voor kinderen, omdat de filtermethoden waarover de voor kinderen verantwoordelijke personen momenteel de beschikking hebben, niet erg doeltreffend zijn.

2.6 Hoofddoelstelling van het programma is de bescherming van kinderen en de ondersteuning van de personen die verantwoordelijk voor hen zijn (ouders, onderwijzers, opvoeders, enz.) of die opkomen voor hun morele belangen en welzijn. Zo is het programma relevant voor NGO's die actief zijn in de sociale sector, op het gebied van kinderrechten, de bestrijding van racisme en vreemdelingenhaat ([2]) en iedere andere vorm van discriminatie, consumentenbescherming en de bescherming van de burgerlijke vrijheden, enz.

2.7 Het programma is eveneens van belang voor regeringen, wetgevers, justitie en politie, en de regelgevingsorganen. Het materiële en procedurele recht moet worden aangepast, en er moet voldoende personeel worden opgeleid en van de benodigde apparatuur worden voorzien.

2.8 Het programma is tevens relevant voor het bedrijfsleven, dat behoefte heeft aan een veilige omgeving om het vertrouwen van de consumenten te versterken.

2.9 Universiteiten en onderzoekers kunnen hun licht laten schijnen over het gebruik van de nieuwe media door kinderen. De beste manier om voorlichting over veiligheid te geven, is de gebruikers erop te attenderen hoe criminelen zich van de media bedienen. Daarnaast moeten nieuwe technische oplossingen worden gezocht, en is het zaak een onafhankelijk standpunt in te nemen t.a.v. de wenselijkheid van regelgeving c.q. zelfregulering.

2.10 Het programma heeft een dubbele dimensie. Op sociaal vlak richt het programma zich op gebieden waarop de veiligheid van gebruikers niet louter met regelgeving en de marktwerking kan worden gewaarborgd. Op economisch vlak is het programma bedoeld om een veilig gebruik van internet en online-technologieën te bevorderen door een klimaat van vertrouwen te scheppen.

2.11 Er wordt een bedrag van ongeveer 50 miljoen euro ter beschikking gesteld voor de ontwikkeling van technische en juridische instrumenten, software en informatie, om nog doeltreffender te kunnen optreden tegen een invasie of frauduleus gebruik van netwerken en computers d.m.v. ongevraagde inhoud die vanuit moreel, sociaal of economisch oogpunt schadelijk kan zijn.

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

([2]) Zie eerdere adviezen van het EESC.

3. **Algemene opmerkingen van het EESC**

3.1 Het EESC herinnert aan de standpunten die het in eerdere adviezen over de bescherming van kinderen op internet en over het eerste actieplan heeft ingenomen. ([1]) Het is verheugd over het voorstel voor een nieuw plan ter bestrijding van illegale en schadelijke inhoud in de online-communicatie (zie de samenvatting van het ontwerpadvies aan het begin van dit document). Het staat achter de doelstellingen en prioriteiten van het programma *Safer internet plus*, als een van de mechanismen die in stelling worden gebracht om de veiligheid op het internet te verbeteren. Het EESC onderstreept echter de zeer grote reikwijdte van het probleem, en de behoefte aan internationale maatregelen en regelgeving om dit probleem aan te pakken.

3.2 Het internet en de nieuwe online-communicatietechnologieën (zoals mobiele telefoons en elektronische zakagenda's met multimediafuncties, die sterk in opkomst zijn), zijn in de ogen van het EESC fundamentele instrumenten voor de ontwikkeling van de kenniseconomie, e-economie en e-*government*. Het zijn veelzijdige instrumenten t.b.v. communicatie, cultuur, werk en vrijetijdsbesteding. Het is dus van wezenlijk belang dat de veiligheid en continuïteit van de communicatienetwerken zijn gewaarborgd, omdat het gaat om essentiële openbare diensten, die open en toegankelijk moeten blijven en waarin alle gebruikers vertrouwen moeten hebben, zodat de vele, uiteenlopende functies in optimale omstandigheden kunnen worden uitgeoefend. De informatie over een veiliger internet integreren in de verschillende e-Europe programma's, met name op het gebied van opleiding, is vanuit het oogpunt van de kosteneffectiviteit een van de meest veelbelovende tactieken, waarmee een groot publiek kan worden bereikt.

3.3 De op het internet heersende vrijheid van meningsuiting en communicatie wordt nog vergroot door de relatief lage verbindingskosten, zelfs van hogesnelheidsverbindingen, die steeds gemakkelijker toegang geven tot multimedia-inhoud. Slechts een aantal landen met een duidelijk tekortschietende democratie willen de communicatie en de voor hun onderdanen beschikbare inhoud kunnen controleren, wat een permanente inbreuk op de vrijheden betekent. Het EESC is van mening dat de veiligheid moet worden vergroot, maar dat de vrijheid van informatie, communicatie en meningsuiting tevens gewaarborgd moeten zijn.

3.4 Deze ruimte voor vrijheid van meningsuiting en informatie — het internet — wordt, meer nog dan andere communicatiemiddelen, tevens gebruikt voor illegale activiteiten zoals pedofilie of de verspreiding van racistische en van vreemdelingenhaat getuigende inhoud. Ook kunnen sommige soorten inhoud schadelijk zijn voor bepaalde bevolkingsgroepen, met name minderjarigen, zoals pornografie of gokspelletjes (die in sommige landen zelfs verboden zijn) en diverse criminele activiteiten (pedofilie, misbruik van de breedband of een frauduleus gebruik van gegevens en servers). Het EESC stemt derhalve in met de uitbreiding van het actieplan tot alle elektronische communicatiemiddelen die ongevraagd toegang bieden of toegankelijk zijn voor mensen met vijandige bedoelingen.

3.5 De regelgeving van deze nieuwe materie is zeer complex omdat het een internationaal en open netwerk is, dat voor iedereen vrij toegankelijk is, vanaf iedere server of computer die aangesloten is op het netwerk, in welk land dan ook. Vele landen hebben echter nog steeds een tekortschietende of onvoldoende wetgeving op dit gebied, waardoor websites die in de EU verboden zijn hun activiteiten elders kunnen voortzetten. Het is van het grootste belang dat de EU samen met de landen waar breedbandinternet het meest verspreid is, zoals in Noord Amerika en Azië, aandringt op en zich inzet voor internationale maatregelen om de allerzwaksten in de samenleving te beschermen, en om een doeltreffender strijd aan te binden tegen ongewenste inhoud (*spam*), die de ontwikkeling van de elektronische communicatie bedreigt, en tegen de verspreiding van virussen, die de digitale economie kwetsbaar maken. Ofschoon zij noodzakelijk zijn in EU-verband, moeten de middelen om e.e.a. te bereiken ook in een wereldwijde aanpak worden geïntegreerd.

3.6 Zolang er op dit gebied geen internationale overeenkomsten bestaan, kan het verbod op bepaalde soorten inhoud in sommige landen zelfs aanleiding geven tot het indienen van een klacht bij de WTO, in het kader van een TBT-procedure ([2]); deze kwestie moet in de lopende onderhandelingen worden meegenomen.

3.7 Het territoriale karakter van het recht en de verscheidenheid van de nationale wetgevingen vormen een lastig probleem. De stand van de technologie maakt de rechtstreekse uitwisseling van allerlei soorten bestanden mogelijk (P2P, *peer to peer*), met inbegrip van versleutelde bestanden waarvan de inhoud oncontroleerbaar is. Iedere computer of netwerk kan worden gebruikt voor het opslaan en versturen van meer geavanceerde inhoud, en het is mogelijk anoniem toegang te krijgen tot iedere server zonder sporen na te laten, en zeer sterke en zelfs „onbreekbare" versleutelmethoden te gebruiken.

3.8 Er zijn wereldwijd honderden miljoenen websites: persoonlijke websites en *weblogs* (die nu zo in de mode zijn), commerciële sites of financiële online-diensten, en een veelvoud aan informatieve, educatieve, wetenschappelijke en technische maar ook pornografische en ontspanningssites met (geld)spelletjes. Toch is het mogelijk een zeker toezicht uit te oefenen tijden de indexering van sleutelwoorden door zoekmachines. De totstandbrenging van rechtstreekse verbindingen en sites voor de automatische verzending van inhoud, zoals *spam*, kunnen ook worden gecontroleerd door IAP's (*Internet Access Providers*, aanbieders van toegang tot het internet); aldus verzonden reclame en andere ongevraagde inhoud kunnen algemene schade aanrichten (misbruik van de breedband, virussen), of alleen schadelijk zijn voor bepaalde groepen gebruikers, zoals kinderen (morele of psychologische schade).

([1]) Advies van het EESC over een „Programma voor de bescherming van kinderen op internet", rapporteur: mevrouw DAVISON, in PB C 48 van 21/02/2002, en over de „Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's - Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak", rapporteur: de heer RETUREAU, in PB C 48 van 21/02/2002, evenals het advies over het „Groenboek over de bescherming van minderjarigen en de menselijke waardigheid in de context van de audiovisuele en informatiediensten", rapporteur: mevrouw BARROW, in PB C 287 van 22/09/1997.

([2]) TBT = „technical barriers to trade" (technische handelsbelemmeringen); overeenkomsten inzake technische handelsbelemmeringen en het verrichten van diensten. Zie bijvoorbeeld de zaak USA vs. Antigua en Barbuda, Measures Affecting the Cross-Border Supply of Gambling and Betting Services, beroep bij de WTO tegen het besluit van het panel (http://www.wto.org/english/tratop_e/dispu_e/distabase_wto_members1_e.htm) document 03-4429 cote WT/DS285/3 van 26/08/2003. Lopende zaak.

3.9 Het internet wordt gebruikt door de maffia, fraudeurs, bedenkers van virussen, piraten, industriële spionnen en andere delinquenten, om er hun activiteiten te ontplooien. De repressie hiervan is geen sinecure, hoewel in veel landen gespecialiseerde politiediensten zich bezighouden met het identificeren en lokaliseren van de daders, zodat zij kunnen worden vervolgd en een einde kan worden gemaakt aan vastgestelde criminele activiteiten. Dit vergt over het algemeen een internationale samenwerking, die meer zou moeten worden bevorderd.

3.10 Hoe kunnen criminele activiteiten, zoals pedofiliewebsites, worden bestreden? Een verbod hierop behoeft geen juridische problemen op te leveren, maar het komt erop aan instrumenten te ontwikkelen om dergelijke netwerken op te sporen. Hoe kunnen kinderen worden beschermd tegen pedofielen, die zich ophouden in de onder jongeren populaire *chatrooms*, waar zij proberen afspraakjes te maken met kinderen? De vraag is niet of een verbod en de repressie in deze bijzondere gevallen legitiem is, maar hoe daaraan in de praktijk vorm kan worden gegeven.

3.11 Aanbieders van ruimte en toegang (IAP's) kunnen niet alle doorgegeven websites en communicatie (= privé-correspondentie) controleren. Wel moeten zij, op bevel van een rechter, de politie of daartoe bevoegde kinderbeschermingsorganisaties, onmiddellijk reageren op verzoeken of beslissingen tot sluiting van dergelijke sites en de identificatie van de gebruikers daarvan. Dit houdt in dat informatie over de vorming van netwerken en over verbindingen een tijd lang moet worden bewaard.

3.12 Kredietkaartmaatschappijen, aanbieders van zoekmotoren en toegang zouden, bijvoorbeeld m.b.v steekproeven, hun bestanden moeten doorlichten om aan de hand van aanwijzingen zoals sleutelwoorden of geografische gebieden, pedofiliewebsites of websites met anderszins criminele inhoud op te speuren, en daarvan vervolgens aangifte te doen bij de politie. Dezelfde techniek zou moeten worden gebruikt om „klanten" van kinderpornografie en snuffmovies ([1]), die daarvoor met hun kredietkaart betalen, te identificeren. Zonodig zouden dergelijke onderzoeken bij wet moeten worden verplicht. Zoekmotoren zouden het ook voor surfers minder gemakkelijk moeten maken om kinderpornografie of andere criminele inhoud op te sporen m.b.v. sleutelwoorden en zinnen.

3.13 Hiervoor is het zaak dat de overheid beschikt over adequate bestrijdingsmiddelen en gekwalificeerd personeel, een wijdverbreide grensoverschrijdende samenwerking en evenwichtige normen op nationaal, Europees en internationaal niveau, die de vrijheid van internauten niet aantasten, terwijl het tevens mogelijk moet worden gemaakt om individuen en groepen die deze netwerken gebruiken om illegale inhoud te verspreiden, uit te schakelen, en ongeschikte of schadelijke inhoud welbewust tegen te houden.

3.14 Om doeltreffend te zijn moet de bestrijding rechtstreeks zijn gericht tot alle gebruikers van het internet; zij moeten worden onderricht en voorgelicht over de te nemen voorzorgsmaatregelen en de middelen waarmee zij zich kunnen wapenen tegen schadelijke of ongewenste inhoud, of om te voorkomen dat zij als doorgeefluik voor dergelijke inhoud worden gebruikt. In het onderdeel van het actieplan dat betrekking heeft op voorlichting en vorming moet volgens het EESC een hoge prioriteit worden toegekend aan het mobiliseren van de gebruikers, om ze meer verantwoordelijkheidsgevoel te geven, voor henzelf en voor de personen die van hen afhankelijk zijn. Een probleem zijn bijvoorbeeld niet-gereguleerde gezondsheidssites. Ook ondernemingen moeten zich beschermen door aandacht te besteden aan de educatie van hun personeel en de beveiliging van hun netwerken en e-commerce websites, maar ook overheden en openbare en particuliere instellingen moeten een veiligheidsbeleid hebben en instaan voor de absolute vertrouwelijkheid van de verwerkte data, met name van persoonlijke gegevens. De bewustwording moet gepaard gaan met de bevordering van kwaliteitsinhoud op het internet; daarnaast moeten *off-line*-activiteiten worden aangemoedigd, als alternatief voor langdurig „surfen" of voor bepaalde spelletjes die op termijn van nadelige invloed kunnen zijn op minderjarigen.

3.15 Gebruikers moeten de mogelijkheid hebben illegale inhoud die zij op de netwerken tegenkomen, op eenvoudige wijze aan te geven bij een erkend meldpunt (via een speciaal noodnummer) of gespecialiseerde politiedienst, om de overheid te waarschuwen, opdat zij de nodige maatregelen kan nemen. In landen waar vaak kinderen worden misbruikt voor de vervaardiging van kinderporno voor publicatie op het internet of andere dragers, bijvoorbeeld landen die grenzen aan de Unie, moeten ouders hiervoor worden gewaarschuwd. Dit zou in bepaalde samenwerkingsprogramma's van DG RELEX kunnen worden opgenomen.

3.16 Het EESC stemt in met de specifieke doelstellingen van het programma — gebruikers de gelegenheid geven om via hotlines aangifte te doen van illegale inhoud, ontwikkeling van filtertechnologieën voor ongewenste inhoud, classificatie van verschillende soorten inhoud, bestrijding van *spam*, zelfregulering van de industrie en mensen meer bewust maken van een veilig gebruik van het internet — maar stelt hieronder enkele aanvullende doelstellingen voor die naar zijn mening nuttig zijn.

4. **Bijzondere opmerkingen van het EESC**

4.1 Het EESC heeft er in het verleden al bij de Commissie op aangedrongen dat de overdreven bureaucratie in de door de EU gefinancierde programma's wordt teruggedrongen, met name om de toegang tot de financiering van microprojecten of lokale NGO's te vergemakkelijken. Het is voorstander van een controle die is gericht op de tastbare resultaten van het programma en de doeltreffendheid van de voorgestelde oplossingen. De informatie over de oplossingen zou een minder vertrouwelijk karakter moeten hebben.

4.2 Naar het oordeel van het EESC zouden normstellende maatregelen voor de bescherming van eindgebruikers moeten worden overwogen, zo mogelijk in het kader van dit programma, of anders van een ander, nieuw initiatief van de Commissie.

([1]) Films met gruwelijke scènes (geweld, martelingen, moord) die werkelijk hebben plaatsgevonden.

4.3 Auteurs van software die toegang geeft tot het internet en makers van computerbesturingssystemen of systemen voor virusbescherming moeten volledig aansprakelijk worden gemaakt. De gebruikers zouden de garantie moeten hebben dat de auteurs van deze software gebruik maken van de beste bestaande technieken, en hun producten regelmatig up-to-date maken. Zelfregulering, en bij gebrek daaraan een communautaire regeling, zou de klanten meer waarborgen moeten bieden.

4.4 De aanbieders van toegang zouden (wat velen van hen nu al doen) op voorhand eenvoudige anti-virussoftware en filters moeten aanbieden voor het verzenden en ontvangen van e-mails en attachments en de bescherming tegen *spam*. Dit kan een concurrentievoordeel betekenen voor aanbieders die serieuze inspanningen doen om hun klanten te beschermen. Aangezien kinderen vaak meer en beter gebruik weten te maken van het internet dan hun ouders, moeten de systemen voor het filteren van e-mails, het onderscheppen van virussen en beschermen tegen indringers, alsook de systemen voor ouderlijk toezicht van te voren worden geïnstalleerd, en gemakkelijk kunnen worden gebruikt en toegepast, óók door personen zonder bijzondere technische kennis.

4.5 Ook zou het programma het onderzoek moeten stimuleren naar gespecialiseerde software en andere methoden om de „waterdichtheid" van de diverse codes van beveiligings- of beschermingssoftware te verifiëren, en zouden aanbieders moeten worden aangespoord of eventueel worden verplicht om snel *patches* (correcties) te verstrekken voor alle geconstateerde of gemelde gebreken die binnendringing mogelijk maken, om de doeltreffendheid van de *firewalls* te vergroten en steeds betere filter- en opsporingsmethoden te ontwikkelen om de werkelijke oorsprong van inhoud te identificeren en te filteren.

4.6 Het EESC had graag gezien dat aan de evaluatie van de doeltreffendheid en de resultaten van het vorige *Safer internet*-programma (waarbij die resultaten zijn ingedeeld naar categorie van met ieder project aangepakte problemen) meer bekendheid wordt gegeven. Er zou op moeten worden toegezien dat alle links naar gefinancierde projecten actief blijven, en dat zij meer bekend zijn bij de personen voor wie zij zijn bestemd. Ook zou de website van de Commissie informatie moeten bieden over de initiatieven en ervaringen in lidstaten of derde landen, om nuttige kennis en ervaringen met samenwerking uit te wisselen.

4.7 Het is perfect mogelijk e.e.a. wettelijk te regelen. *Internet Access Providers*, uitgevers van kredietkaarten en aanbieders van zoekmachines kunnen zonder uitzondering aan regelgeving worden onderworpen, en sommige passen nu al zelfregulering toe. De straffen voor websites die aanzetten tot terrorisme, racisme, zelfmoord of kinderpornografie moeten streng zijn en een afschrikwekkend effect sorteren. Er zouden meer internationale inspanningen moeten worden gedaan om dergelijke sites op te sporen en te lokaliseren, zodat deze sites kunnen worden afgesloten voor zover dat mogelijk is; zo niet dan zouden onderhandelingen moeten worden gevoerd met de landen die dergelijke sites herbergen.

5. **Conclusies**

Het EESC stemt weliswaar in met de voortzetting en uitbreiding van het programma „*Safer Internet plus*" (het heeft er zelfs mede voor gezorgd dat dit programma er is gekomen), maar is van mening dat de ernst en strekking van de dreiging van misbruik, in de eerste plaats jegens kinderen, dringend aanvullende wettelijke maatregelen en soms ook praktische maatregelen vergt, op de volgende gebieden:

— een algemene plicht voor alle betrokken exploitanten om kinderen en meer in het algemeen de gebruikers, met name de meest kwetsbare, te beschermen;

— standaardinstallatie van filtersystemen;

— duidelijke veiligheidsboodschappen op de startpagina's van websites en *chat rooms*;

— ondersteuning van instanties die *hotlines* instellen waarop aangifte kan worden gedaan van websites en online-activiteiten die ernstige schade toebrengen aan kinderen;

— voorkómen dat kredietkaarten kunnen worden gebruikt om kinderporno en andere illegale inhoud te bestellen op het internet, en voor witwasoperaties;

— waarschuwingen en acties gericht aan ouders en opvoeders, en aan de autoriteiten van landen waar kindermishandeling t.b.v. kinderporno een zorgwekkende omvang aanneemt;

— méér maatregelen om de banden tussen kinderporno en de georganiseerde misdaad te bestrijden;

— systemen om schadelijke inhoud op te sporen en informatie hierover te geven, en systemen om racistische inhoud van het internet te halen, en verspreiding van informatie over pogingen tot oplichting of de verkoop van stoffen die de gezondheid kunnen beïnvloeden via internet, om kwetsbare of slecht geïnformeerde personen te beschermen;

— streven naar internationale samenwerking en gemeenschappelijke regels om doeltreffender op te treden tegen *spam*;

— internationale samenwerking (verbetering van het systeem voor vroegtijdige waarschuwing) en afschrikwekkende sancties voor verspreiders van virussen en voor illegaal gebruik van private en publieke netwerken voor criminele doeleinden (zoals binnendringen van het netwerk voor bedrijfsspionage, misbruik van de breedband en andere vormen van misbruik).

Brussel, 16 december 2004

De voorzitter
van het Europees Economisch en Sociaal Comité
A.-M. SIGMUND