5.8 EESK håller fast vid att förordning 4056/86 bör upphävas och ersättas av en ny kommissionsförordning för linjekonferenser som innebär att man beviljar ett gruppundantag. Det nya systemet skulle strikt följa de riktlinjer som fastställts i rättspraxis genom beslut från Europeiska gemenskapernas förstainstansrätt och kommissionen (jfr beslutet om TACA). Konferenssystemet skulle också finnas kvar för att upprätthålla konkurrenskraften hos gemenskapens rederier globalt sett. När det gäller de stora transportörerna kan ”allianser” och andra typer av samarbetsavtal vara lämpliga tillvägagångssätt, men små och medelstora transportörer behöver fortfarande konferenserna för att kunna behålla sina marknadsandelar, särskilt i handeln med utvecklingsländerna. Avskaffandet av undantaget kan resultera i att konkurrenskraften minskar för de små transportörerna och att de större transportörernas dominerande position förstärks.

5.9 Den mellanliggande övergångsperioden bör kommissionen använda för övervakning av utvecklingen av marknaden för linjesjöfart, inbegripet konsolideringstendenser. Kommissionen bör dessutom samråda med företrädare för andra jurisdiktioner (OECD) i syfte att ta fram ett lämpligt alternativt system som kan användas globalt.

5.10 EESK stöder vitbokens förslag i fråga om tramp- och cabotagetjänster eftersom de allra flesta fall i denna sektor inte skulle orsaka konkurrensproblem. För att klargöra rättsläget bör dock kommissionen utforma rättsliga riktlinjer om bulkpooler och specialiserad linjefart, som rederierna kan använda vid sin egen bedömning av om huruvida de efterlever EG-fördragets artikel 81.

5.11 EESK hoppas att få bidra till uppföljningen av den diskussion som inletts genom vitboken.

Bryssel den 16 december 2005

Europeiska ekonomiska och sociala kommitténs
ordförande
Anne-Marie SIGMUND

Yttrande från Europeiska ekonomiska och sociala kommittén om ”förslag till Europaparlamentets och rådets beslut om inrättandet av ett flerårigt gemenskapsprogram för att främja en säkrare användning av internet och ny online-teknik”

(KOM(2004) 91 slutlig – 2004/0023 COD)

(2005/C 157/24)

Den 26 mars 2004 beslutade rådet att i enlighet med artikel 153 i EG-fördraget rådfråga Europeiska ekonomiska och sociala kommittén om ovannämda yttrande.

Facksektionen för transporter, energi, infrastruktur och informationssamhället, som svarat för kommitténs beredning av ärendet, antog sitt yttrande den 5 oktober 2004. Föredragande var **Daniel Retureau** och medföredragande **Ann Davison**.

Vid sin 413:e plenarsession den 15–16 december 2004 (sammanträdet den 16 december 2004) antog Europeiska ekonomiska och sociala kommittén följande yttrande med 147 röster för och 1 nedlagd röst:

1. **Sammanfattning av utkastet till yttrande**

1.1 Kommissionen har för avsikt att nylansera projektet ”Safer Internet” men i utvidgad form för att svara mot informationssamhällets snabba utveckling i fråga om kommunikationsnät. Därför kallas projektet ”Safer Internet plus” (2005–2008).

1.2 Utöver det förslag till Europaparlamentets och rådets beslut som kommissionen lagt fram har EESK även studerat förhandsutvärderingen av Safer Internet plus (2005–2008) som ingår i kommissionens arbetsdokument SEK(2004) 148 och i KOM(2004) 91 slutlig. Kommittén stöder en utvidgning av tillämpningsområdet och målsättningarna för den nya handlingsplanen. Utvidgningen tar hänsyn till den snabba utvecklingen och de många nya formerna av uppkoppling till Internet. Vidare beaktas den synnerligen snabba ökningen av olika former av höghastighetsanslutningar och ständig uppkoppling. EESK formulerar en rad kompletterande förslag till politiska och normativa åtgärder under rubrikerna allmänna kommentarer och särskilda kommentarer, bl.a. gällande följande:

— De tekniska och rättsliga normerna (bindande eller frivilliga).

— Utbildning och fortbildning för användare.

— Åligganden som berör leverantörer av Internettjänster och webbplatser samt övriga aktörer (kreditkortsföretag, sökmotorer etc).

— Ansvar som åligger producenter av mjukvara och leverantörer av säkerhetsprogram.

— Skydd mot bedrägerier eller tvivelaktig information för sårbara användargrupper (olika former av lurendrejeri, fri försäljning av aktiva läkemedel, hälsorådgivning eller hälsovård som utförs av personer utan sådan behörighet).

2. **Kommissionens förslag (sammanfattning)**

2.1 Kommissionens förslag till program har som syfte att främja en trygg användning av Internet och online-teknik för slutanvändaren, särskilt barn och unga hemma eller i skolan. Därför planeras samfinansiering av olika organisationers och andra gruppers (forskarlag, mjukvaruproducenter, läroanstalter) projekt för att utveckla skydd: t.ex. ”heta linjer”, program mot spam och virus samt ”intelligenta” Internetfilter.

2.2 Den tidigare planen för ett säkert Internet för perioden 1999–2002 förlängdes till 2003–2004.

2.3 På kommissionens webbplats förtecknas projekt som redan avslutats inom programmet *Safer Internet* före slutet av 2003 ([1]).

2.4 Det nya förslaget för perioden 2005–2008 omfattar även nya kommunikationsformer på nätet och syftar till en förstärkt kamp mot otillåtet och menligt material, inklusive virus och annat skadligt eller oönskat material (spam).

2.5 Denna förstärkta kamp kan för EU-institutionernas del motiveras av flera olika orsaker, av vilka de viktigaste är följande:

— Den snabba utvecklingen av höghastighetsanslutningar med långvarig eller ständig uppkoppling för privatpersoner, företag, myndigheter och privata instanser (icke-statliga organisationer).

— Diversifieringen av medel och metoder för tillträde till Internet och till nytt online-innehåll som i många fall är oönskat (e-post, textmeddelanden till mobiltelefoner) samt till ett mer attraktivt online-innehåll (multimedia).

— Den dramatiska ökningen av oönskat, riskfyllt eller olämpligt material som utgör hot för användarna i allmänhet (virus: angrepp på lagringsutrymmet, förflyttning eller raderande av information, otillåten användning av offrets kommunikationsverktyg, spam: missbruk av bandbredden och lagringsutrymmen samt angrepp på e-posten, vilket hindrar eller stör nyttoanvändning av Internet och kommunikationen samt orsakar höga kostnader som inte betalas av avsändarna av skräpmaterial utan av slutanvändaren) eller för särskilda större grupper av användare, t.ex. barn (skräppost med explicit sexuellt innehåll, olämplig e-post och uppmaningar från pedofiler om möten på diskussionsforum för kommunikation i realtid (*chat rooms*).

— Olämpligt material som barn lätt kan komma åt till följd av den relativt låga effektiviteten hos de befintliga filter som står till buds för personer som ansvarar för barn.

2.6 Programmets huvudsakliga syfte är att skydda barnen och erbjuda stöd för dem som ansvarar för barnen (föräldrar, lärare, tränare osv.) eller som värnar om barnens moraliska integritet och deras välbefinnande. Därmed berör programmet även icke-statliga organisationer inom den sociala sektorn, barns rättigheter, konsumentskydd, försvar av samhälleliga rättigheter, kampen mot rasism, främlingsfientlighet ([2]) och alla andra former av diskriminering, konsumentskydd och skydd för de medborgerliga rättigheterna osv.

2.7 Programmet är även av intresse för regeringarna och för deras lagstiftande organ, rättsväsende och polisväsende samt för ämbetsverken. Den materiella rätten och processrätten måste anpassas och ett tillräckligt antal anställda måste få utbildning och ges verktyg.

2.8 Programmet kan även intressera industrin, som behöver en trygg miljö för att stärka konsumenternas förtroende.

2.9 Universiteten och forskningen kan även ge upplysningar om hur barn använder de nya medierna. Det bästa sättet att sprida kunskap om säkerhet är att informera om kriminella metoder inom dessa medier, ta fram nya tekniska lösningar och erbjuda ett neutralt synsätt på hur de olika berörda intressena kan förenas utgående från förfaranden för reglering och självreglering.

2.10 Programmet har två olika inriktningar. På det sociala planet inriktas det på områden där reglerna och marknaden inte ensamma kan garantera säkerhet för användarna. På det ekonomiska planet är det fråga om att främja trygg användning av Internet och online-teknik genom att skapa ett klimat som präglas av förtroende.

2.11 Finansiering på ungefär 50 miljoner euro har föreslagits för utvecklingen av tekniska och rättsliga instrument, mjukvara och information i syfte att effektivisera bekämpningen av intrång i nätverk och i dataterminaler eller av bedräglig användning av dessa i form av oönskat material som kan vara skadligt psykiskt, socialt eller ekonomiskt.

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

([2]) Dessa teman motsvarar en tidigare begäran från kommittén.

3. **Allmänna kommentarer**

3.1 EESK erinrar om kommitténs tidigare ställningstaganden om skydd av barn på Internet och om den första handlingsplanen ([1]). Kommittén välkomnar förslaget till en ny plan för bekämpning av otillåtet och skadligt material inom online-kommunikation (se avsnitt I, Sammanfattning, i början av dokumentet). EESK stöder målsättningarna och prioriteringarna i programmet Safer Internet Plus som en av mekanismerna för ökad säkerhet på Internet. Kommittén vill dock understryka att problemet är synnerligen omfattande och att det behövs internationella insatser och regler för att angripa det.

3.2 Internet och de nya teknikerna för online-kommunikation (t.ex. mobiltelefoner eller anslutningsbara planeringskalendrar i fickformat med multimediafunktioner som just nu har ett stort uppsving) utgör enligt kommittén grundläggande element för utvecklingen av kunskapsekonomin, e-ekonomi och e-förvaltning. De är instrument för kommunikation rörande kultur, arbete och fritid som ständigt förändras. Därför är det av största betydelse att garantera kommunikationsnätens säkerhet och kontinuitet. Det handlar nämligen om en väsentlig allmännyttig tjänst som bör förbli öppen och tillgänglig och som samtliga användare skall kunna lita på för att de många funktionsmöjligheterna skall kunna utnyttjas under bästa möjliga omständigheter. Information om hur Internet kan göras säkrare bör integreras i en rad program inom e-Europe, särskilt inom utbildningen. Med tanke på förhållandet mellan kostnad och effektivitet skulle detta vara en lovande metod för att nå ut till många människor.

3.3 Yttrande- och kommunikationsfriheten på Internet underlättas av de relativt låga anslutningskostnaderna, inberäknat höghastighetsanslutning, som gör att det blir allt lättare att få tillgång till multimedialt innehåll. Endast några länder som uppvisar ett stort demokratiskt underskott försöker att kontrollera den kommunikation och det innehåll som är tillgängligt för deras medborgare genom att ständigt inskränka dessa friheter. Kommittén anser att man måste säkerställa en högre grad av säkerhet samtidigt som man bevarar och främjar informations-, kommunikations- och yttrandefriheten.

3.4 Det område för yttrande- och informationsfrihet som det världsomspännande nätet utgör används dock i högre grad än andra kommunikationsformer även för olaglig verksamhet såsom pedofili eller spridning av rasistiskt och främlingsfientligt stoff. Visst material kan även visa sig vara skadligt för en del användargrupper, särskilt minderåriga, t.ex. pornografi eller spel om pengar (de sistnämnda är rentav förbjudna i vissa länder) och annan brottslig verksamhet (angrepp på bandbredden eller bedräglig användning av information och av servrar). EESK stöder med andra ord att handlingsplanen utvidgas till samtliga elektroniska kommunikationsmedel som kan drabbas av oönskade eller bedrägliga intrång utifrån.

3.5 De nya reglerna på detta nya, kraftigt expanderande område är svåra att införa eftersom nätverket är världsomfattande, öppet och tillgängligt för alla från vilken server eller dator som helst som man fritt kan koppla upp sig från, i snart sagt varje land i världen. Men i många länder är lagstiftningen fortfarande bristfällig eller otillräcklig, vilket gör det möjligt för webbplatser som förbjudits i EU att fortsätta sin verksamhet. Det förefaller mycket viktigt att EU förespråkar och tar initiativ till internationella åtgärder, särskilt tillsammans med de länder där Internet per bredband är utbrett (i Nordamerika och Asien) i syfte att skydda de mest sårbara och vidta effektivare åtgärder mot oönskade meddelanden (spam), som är ett hot mot utvecklingen av kommunikation per e-post, samt åtgärder mot spridning av virus som undergräver den digitala ekonomin. Även om man eftersträvar lösningar på EU-nivå måste de även fungera på ett världsomspännande plan.

3.6 I de fall då det saknas internationella överenskommelser kan visst material i vissa länder t.o.m. leda till att klagomål lämnas in till WTO inom ramen för TBT ([2]). Den frågan bör behandlas under de pågående förhandlingarna.

3.7 Den territoriella aspekten av lagstiftningen och skillnaderna mellan de olika medlemsstaternas lagstiftning är ett problem som är svårt att övervinna. Dagens teknik möjliggör också ett direkt utbyte av filer av alla slag (P2P, *peer to peer*), däribland krypterade filer vars innehåll inte kan kontrolleras. Alla datorer eller nätverk som är on-line kan användas till att spara och skicka ut ett alltmer sofistikerat innehåll. Det är också möjligt att ansluta sig till vilken server som helst anonymt och utan möjlighet att spåra, samt att använda mycket robusta, ibland till och med ”oknäckbara”, krypteringsmetoder.

3.8 Personliga sidor och *weblogs*, utvecklingen av webbplatser med e–handel och elektroniska finansiella tjänster, det stora antalet olika webbplatser av informativ, utbildningsmässig, vetenskaplig eller teknisk, men också pornografisk, art och webbplatser med spel om pengar osv. gör att det finns flera hundra miljoner olika webbplatser i världen. En viss kontroll kan ändå utövas i samband med sökmaskiners indexering av nyckelord. Det är också möjligt för företag som tillhandahåller anslutning till Internet att kontrollera direkta förbindelser och webbplatser som har automatiskt utskick av innehåll, som t.ex. spam. Reklam och andra former av oönskat innehåll som skickas ut på detta sätt kan vara allmänt skadliga (olaglig användning av bredband, virus) eller särskilt skadliga för vissa mottagare såsom barn (moraliskt eller psykologiskt).

([1]) EESK:s yttrande om ”Ett program för skydd av barn på Internet” (föredragande: Ann Davison), EGT C 48, 21.2 2002, och yttrandet om ”Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén – Nät- och informationssäkerhet: förslag till en europeisk strategi” (föredragande: Daniel Retureau), EGT C 48, 21.2 2002 samt yttrandet om ”Grönbok om skyddet av minderåriga och den mänskliga värdigheten inom de audiovisuella tjänsterna och informationstjänsterna” (föredragande: Jocelyn Barrow), EGT C 287, 22.9 1997.

([2]) ”Technical Barriers to Trade”. Avtal rörande tekniska hinder för handel och tillhandahållande av tjänster. Se t.ex. det oavslutade målet USA/Antigua och Barbuda om spel om pengar i offshore-miljö, panelbeslut som har lett till klagomål till WTO (http://www.wto.org/french/tratop_f/dispu_f/distabase_wto_members1_f.htm), dokument 03-4429 WT/DS285/3 av den 26 augusti 2003.

3.9 Maffiagrupper, bedragare, virusspridare, pirater, industrispioner och andra kriminella utnyttjar Internet för att sprida sin verksamhet. Det är mycket svårt att bekämpa den här typen av kriminell verksamhet, trots att man inom polisen har upprättat specialenheter i en rad länder för att identifiera, lokalisera, spåra och stoppa kriminell verksamhet som har konstaterats. Detta förutsätter normalt ett internationellt samarbete, vilket bör främjas i högre grad.

3.10 Hur bekämpar man kriminell verksamhet som t.ex. webbplatser med pedofili? Ett förbud för dessa lär inte ge upphov till några rättsliga problem, men det vore lämpligt att först utforma medel för att spåra sådana nätverk. Hur skyddar man barn mot pedofiler som använder sig av direkta diskussionsforum som särskilt besöks av unga, för att arrangera personliga möten. Frågan är inte huruvida det är berättigat med förbud och bekämpning i dessa särskilda fall, utan snarare vilka medel man skall använda för att uppnå dessa mål.

3.11 Tillhandahållare av Internetanslutning kan inte övervaka och kontrollera alla webbplatser och all kommunikation som finns på Internet (eftersom mycket faller inom ramen för privat post). Däremot måste en tillhandahållare som får en begäran av en domare, polis eller behörig barnskyddsorganisation omedelbart reagera på denna begäran eller på beslut om nedläggning av webbplatser och om identifikation av deras användare. Detta förutsätter att information om innehåll som lagts ut på nätet och om de användare som har besökt webbplatserna i fråga sparas under en viss tid.

3.12 Kreditkortsföretag, sökmotorer och tillhandahållare av Internetanslutning bör genomföra stickprovskontroller för att spåra upp sidor med pedofili eller annat olagligt innehåll genom att följa ledtrådar som nyckelord och geografiska områden. Därefter skall de rapportera om dessa till polisen. Samma teknik bör användas för att identifiera ”kunder” som beställer barnpornografi och s.k. *snuff movies* [1] med kreditkort. Om det är nödvändigt bör man kräva sådana kontroller genom lagstiftning. Sökmotorer för Internet bör också minska möjligheterna för surfare att finna barnpornografi och annat olagligt innehåll genom sökord och fraser.

3.13 För detta krävs också från de offentliga myndigheternas sida anpassade bekämpningsmetoder, kvalificerad personal, ett omfattande gränsöverskridande samarbete och väl avvägda standarder på nationell, europeisk och internationell nivå som inte påverkar Internetanvändarnas frihet. Man måste dock samtidigt kunna hindra personer och grupper som utnyttjar Internet för att sprida olagligt innehåll och frivilligt blockera olämpligt och skadligt innehåll.

3.14 För att man skall uppnå resultat med dessa insatser bör de direkt beröra alla Internetanvändare. Användarna måste informeras om försiktighetsåtgärder som är nödvändiga att vidta och om medel att ta till för att skydda sig mot farligt eller oönskat innehåll eller mot att utnyttjas som mellanled för sådant innehåll. Enligt kommittén bör man inom ramen för den del av handlingsplanen som rör information och utbildning ge hög prioritet åt mobilisering av användarna, så att de tar ansvar för sig själva och de personer som är beroende av dem. T.ex. uppstår problem med oreglerade hälsorelaterade webbplatser. För att skydda sig bör också företag satsa på utbildning av personal och säkerhet för nätverk och webbplatser med e-handel. Även offentliga och privata administrationer och institutioner bör föra en sådan säkerhetspolitik och garantera diskretion när det gäller behandling av uppgifter, särskilt personliga uppgifter. En ökad medvetenhet om problemet bör åtföljas av insatser för att främja kvalitativt innehåll på nätet, och för att uppmuntra till off line-aktiviteter som alternativ till överdrivet Internetsurfande eller vissa rollspel som på lång sikt kan påverka omogna personer.

3.15 Internetanvändarna måste ha möjlighet att lätt kunna anmäla olagligt innehåll som de upptäcker på nätet till särskilda telejourer eller andra behöriga organ, eller till särskilda polisenheter, i syfte att underrätta de offentliga myndigheterna så att dessa kan vidta nödvändiga åtgärder när så behövs. Man bör varna föräldrar i länder där det ofta förekommer övergrepp mot barn för pornografiska ändamål på nätet och i andra medier, t.ex. i de länder som gränsar till EU. Detta skulle kunna ingå i vissa av RELEX-samarbetsprogrammen.

3.16 EESK stöder programmets särskilda målsättningar, dvs. att göra det möjligt för användarna att anmäla olagligt innehåll (*hotlines*), utveckla teknik för filtrering av oönskat innehåll, klassificera innehåll, bekämpa spam, uppmuntra självreglering inom industrin och sprida kunskaper om en säkrare teknikanvändning, men vill i sina särskilda kommentarer föreslå ytterligare några mål som vi anser vara nödvändiga att beakta.

4. **Särskilda kommentarer**

4.1 Kommittén har redan tidigare uppmanat kommissionen att reducera den överdrivna byråkratin inom de program som finansieras av EU, framför allt för att underlätta finansieringen av mikroprojekt eller lokala icke-statliga organisationers projekt. EESK stöder kontroll som fokuseras på påtagliga resultat som uppnåtts inom ramen för programmet och ett effektivt genomförande av föreslagna lösningar. Lösningarna bör spridas på ett öppnare sätt.

4.2 Kommittén anser att man bör överväga lagstiftningsåtgärder för att skydda slutanvändarna, genom detta program när så är möjligt, eller i annat fall genom ett nytt kommissionsinitiativ.

[1] Filmer där det kraftiga våldet, tortyren och morden är verkliga.

4.3 Producenter av programvara som ger tillgång till Internet och av serveroperativsystem eller system för bekämpning av intrång bör bära fullt ansvar för sina produkter. Användarna bör få garantier för att programvaruproducenter använder den bästa tekniken som finns tillgänglig och regelbundet uppdaterar sina produkter. Självreglering, eller annars EU-lagstiftning, bör stärka kundernas garantier.

4.4 Företag som tillhandahåller Internetanslutning bör erbjuda användarna (vilket många av dem redan gör) lätthanterliga antivirusprogram och program för filtrering av *spam* för e-post och bifogade filer. Detta innebär en kommersiell fördel för företag som gör ordentliga ansträngningar för att skydda sina kunder. Med anledning av att barn ofta kunskapsmässigt ligger ett steg före sina föräldrar när det gäller Internetanvändning bör system för filtrering av e-post, eliminering av virus och skydd mot intrång installeras i förväg och vara lätta att använda för vuxna utan några större tekniska kunskaper.

4.5 Programmet bör också främja forskning om specialiserade programvaror och andra medel för att kontrollera ”sårbarheten” hos de koder som används för olika programvaror för säkerhet och skydd. Vidare bör det anmoda eller, om det behövs, tvinga leverantörerna att snabbt genomföra *patches* (uppdateringar) för alla konstaterade eller rapporterade brister som möjliggör intrång samt utveckla effektivare hårdvaru- eller mjukvarubaserade brandväggar liksom metoder för filtrering och identifiering av olika innehålls ursprung.

4.6 Kommittén hade gärna sett att utvärderingen av effektiviteten och de resultat som uppnåtts inom ramen för den föregående handlingsplanen för ett säkrare Internet, klassificerat enligt problemtyper som projekten haft, hade fått större spridning. Det vore lämpligt att försäkra sig om att alla länkar till finansierade projekt förblir aktiva och bli mer kända bland användarna. Kommissionens webbplats bör också innehålla information om initiativ och erfarenheter i medlemsstaterna eller tredje land när det gäller att sprida kunskap, utbyte och samarbete av nytta.

4.7 Det är fullt möjligt att vidta rättsliga åtgärder. Både tillhandahållare av Internet, kreditkortsföretag och sökmotorer kan regleras och vissa tillämpar redan självreglering. De straffrättsliga påföljderna för webbplatser som stöder terrorism, rasism, självmord eller barnpornografi bör vara stränga och avskräckande. Större internationella insatser bör göras för att identifiera och lokalisera sådana webbplatser, för att i största möjliga utsträckning se till att de läggs ned, och i annat fall inleda förhandlingar om detta med de länder där webbplatserna hör hemma.

5. **Slutsatser**

Europeiska ekonomiska och sociala kommittén stöder en fortsättning och utvidgning av programmet *Safer Internet Plus* (EESK begärde för övrigt att man skulle upprätta programmet) och menar att det allvarliga och utbredda missbruket, framför allt det som riktar sig mot barn, i varje enskilt fall kräver omedelbara och kompletterande lagstiftningsåtgärder och praktiska insatser:

— En allmän skyldighet för alla berörda operatörer att skydda barn och mer allmänt alla användare, framför allt de mest sårbara.

— Automatisk installering av filtreringssystem.

— Tydliga säkerhetsmeddelanden på alla hemsidor (på välkomstsidorna) och portaler med åtkomst till *chat rooms* för on line-diskussioner.

— Stöd till sammanslutningar som upprättar direktlinjer (*hotlines*) för rapportering av webbplatser och aktiviteter på Internet som är skadliga för barn.

— Blockering av kreditkortsanvändning för beställning av barnpornografi och annat olagligt innehåll på nätet samt penningtvätt.

— Varningar och insatser som riktar sig direkt till föräldrar, lärare och myndigheter i de länder som har stora problem med övergrepp mot barn för barnpornografiska ändamål.

— Fler åtgärder när det gäller förbindelsen mellan utnyttjande av barn och organiserad brottslighet.

— System för identifiering av och information om skadligt innehåll, bekämpning av rasistiskt innehåll samt spridning av information om försök till bedrägeri eller försäljning av hälsovådliga ämnen på Internet, i syfte att skydda sårbara eller dåligt informerade personer.

— Samarbete och gemensamma regler på internationell nivå för en effektivare bekämpning av spam.

— Internationellt samarbete (förbättrat system för tidig varning) och avskräckande straffrättsliga sanktioner mot personer som sprider datavirus och olagligt använder privata och offentliga nätverk i kriminellt syfte (intrång i nätverk för industrispionage, olaglig användning av bredband och andra olagliga handlingar).

Bryssel den 16 december 2004

Europeiska ekonomiska och sociala kommitténs
ordförande
Anne-Marie SIGMUND