5.8 EMSK jääb arvamuse juurde, et määrus (EMÜ) nr 4056/86 tuleks tühistada ja asendada komisjoni uue määrusega, mis peaks võimaldama grupierandit. Uus eeskiri peaks rangelt järgima standardeid, mis on loodud vastavalt Euroopa esimese astme kohtu ja komisjoni praktikale (näit. TACA juhtum). Laevanduskonverentsisüsteem tuleks säilitada ka selleks, et kaitsta ühenduse laevaomanike konkurentsivõimelisust kogu maailmas. Kui suuremate lastivedajate jaoks võivad olla sobivad liidud ja muud koostöökokkulepped, siis väikesed ja keskmise suurusega lastivedajad vajavad oma turuosa säilitamiseks laevanduskonverentse, seda eriti kauplemisel arengumaadega. Erandi kaotamisel võivad olla väikeste lastivedajate jaoks konkurentsivõimelisust piiravad tagajärjed, suurendades veelgi suurte lastivedajate domineerivat positsiooni.

5.9 Kõnealust üleminekuperioodi peaks komisjon kasutama selleks, et jälgida liinilaevandusturul toimuvaid arenguid, kaasa arvatud konsolideerumistrende. Lisaks peaks komisjon konsulteerima teiste jurisdiktsioonidega (OECD), püüdes leida sobivat alternatiivset süsteemi, mis oleks kohaldatav kogu maailmas.

5.10 EMSK toetab valge raamatu ettepanekuid seoses trampteenuste ja kabotaaži käsitlemisega, sest enamik juhtumeid selles valdkonnas ei tekita konkurentsiprobleemi. Õiguskindluse tagamiseks palutakse komisjonil siiski koostada õigusalased suunised puistlastivedude puulidele ja spetsialiseeritud laevandusele, nii et laevandusettevõtetel oleks endil võimalik hinnata, kas nende tegevus vastab EÜ asutamislepingu artiklile 81.

5.11 EMSK loodab olla kasulik valges raamatus alustatud ajurünnaku jätkukäsitlustes.

Brüssel, 16. detsember 2004

Euroopa majandus- ja sotsiaalkomitee
president
Anne-Marie SIGMUND

Euroopa majandus- ja sotsiaalkomitee arvamus teemal "Ettepanek Euroopa Parlamendi ja nõukogu otsuse kohta, millega luuakse ühenduse mitmeaastane programm edendamaks interneti ja uute võrgupõhiste tehnoloogiate turvalisemat kasutamist"

K(2004) 91 (lõplik) — 2004/0023 (COD)

(2005/C 157/24)

26. märtsil 2004 otsustas nõukogu, vastavalt Euroopa Ühenduse asutamislepingu artiklile 153, taotleda Euroopa majandus- ja sotsiaalkomitee arvamust ülelmainitud teemal.

Transpordi, energia, infrastruktuuride ja infoühiskonna osakond, kellele tehti ülesandeks ette valmistada komitee tööd selles osas, töötas välja oma arvamuse 5. oktoobril 2004 (raportöör: hr RETUREAU, kaasraportöör: pr DAVISON).

Oma 413. plenaaristungil 15. ja 16. detsembril 2004. aastal (16. detsembri istungil) võttis Euroopa majandus- ja sotsiaalkomitee 147 poolt- ja 1 erapooletu häälega vastu järgmise arvamuse:

1. **Arvamuse eelnõu kokkuvõte**

1.1 Komisjon soovitab algatada uus projekt "*Safe Internet*", kuid tugevdades seda, võttes arvesse infoühiskonna kiireid arenguid kommunikatsioonivõrgustike osas. Niisiis antakse projektile nimeks "*Safe Internet plus*" (2005—2008).

1.2 Lisaks komisjoni esitatud ettepanekule parlamendi ja nõukogu otsuse kohta on komitee analüüsinud projekti Safer Internet plus (2005/2008) *ex ante* hinnangut, mille allikaks on "*Commission Staff working paper*" SEC(2004) 148 ja K(2004) 91 lõplik. Ta toetab uue tegevusplaani ja selle eesmärkide rakendusvälja laiendamist, võttes arvesse internetile juurdepääsu võimaluste kiiret arengut ja mitmekesistumist ning kiire interneti ja püsiühenduste arvu väga kiiret kasvu. Komitee ütleb välja oma täiendavad soovitused poliitilise ja normatiivse tegevuse osas üldiste tähelepanekute ja erimärkuste osas, eelkõige:

— tehnilised ja juriidilised normid (kohustuslikud ja vabatahtlikud);

— kasutajate haridus ja koolitus;

— võrguruumi ja juurdepääsu pakkujate ja teiste osapoolte kohustused (krediitkaarte väljastavad ettevõtted, otsingumootorid…);

— tarkvara autorite ja turvavahendite pakkujate vastutus;

— haavatavate isikute kaitsmine pettuste või väära teabe vastu (erinevad pettused, erinevate ravimite "vabamüük", ilma meditsiinilise väljaõppeta isikute poolt pakutavad nõuanded või ravikuurid…).

2. **Komisjoni ettepanek (kokkuvõte)**

2.1 Välja pakutud programmi eesmärk on soodustada interneti ja võrgupõhiste tehnoloogiate turvalisust lõppkasutaja, eelkõige laste ja noorte jaoks kodus ja koolis. Selleks on ettenähtud assotsiatsioonide ja teiste rühmade (uurimisrühmad, tarkavaraarendajad, õppeasutused...) poolt loodud selliste projektide kaasrahastamine, mis võimaldavad luua kaitsemeetmeid: "*hot line*" tüüpi, rämpsposti ja viiruste vastu, nt "intelligentseid" Interneti kasutamise filtreid.

2.2 Eelmist turvalise interneti plaani (1999—2002) pikendati aastateks 2003—2004.

2.3 Komisjoni internetileht toob välja projekti *Safe Internet* (turvaline internet) all kuni 2003. aasta lõpuni juba teostatud projektide loetelu. ([1])

2.4 Praegune ettepanek (2005—2008) laieneb ka uutele võrgupõhistele kommunikatsioonivahenditele, mille osas on kavas tõhustada võitlust ebaseadusliku ja ohtliku sisuga materjalide vastu, kaasa arvatud viirused ja teised kahjustavad või ebasoovitavad materjalid (*rämpspost*).

2.5 Selle võitluse tõhustamine on õigustatud ühenduse institutsioonides paljudel põhjustel, millest olulisemad on:

— eraisikute, ettevõtete, ametiasutuste ja erainstitutsioonide (VVO-d) kiire interneti pikaajalise või püsiühenduse kiire arendamine;

— Internetile ja uutele võrgupõhistele allikatele (millest paljud ei ole taotletud — *e-mailid, sms-id)* juurdepääsu vahendite ja meetodite mitmekesistamine, ja sisu suurem atraktiivsus (multimeedia);

— Ebasoovitava ja võimalikult ohtliku või ebakohase sisu dramaatiliselt laienenud levik loob uusi ohte laiale avalikkusele (viirused: kettaruumi hõivamine, andmete kuritarvitamine või hävitamine, ohvri kommunikatsioonivahendite kasutamine ilma loata; rämpspost *(spams)*: läbilaskevõime ja kettaruumi kuritarvitamine, elektronpostkastide vallutamine, mis takistab või häirib interneti ja sidevahendite kasutamist ja põhjustab olulisi kulutusi, mida ei kanna "reostaja" vaid lõppkasutaja) ja teatud olulistele kasutajate kategooriatele, nagu lapsed (seksuaalse sisuga rämpspost, ebakohased sõnumid ja kohtamisele kutsed pedofiilide poolt interneti jututubades (*chat rooms*);

— Ebakohane sisu, mis on lastele väga kergesti kättesaadav, laste eest vastutavatele isikutele praegu kättesaadavate filtreerimisvahendite väga küsitava efektiivsuse tõttu.

2.6 Programmi peamine eesmärk on kaitsta lapsi ja toetada nende eest vastutavaid isikuid (vanemad, kasvatajad, õpetajad jne) või nende moraalseid huvisid ja heaolu kaitsvaid isikuid. Niisiis puudutab programm sotsiaalsektori, laste õiguste, rassismi, ksenofoobia ([2]) vastase võitluse ja igasuguse diskrimineerimisega ning tarbijakaitse ja kodanikuvabaduste kaitsega jms tegelevaid valitsusväliseid organisatsioone.

2.7 See puudutab ka valitsusi, seadusandlikke-, kohtu- ja politseiasutusi ja haldusorganeid. Materiaalõigust ja protseduuriõigust tuleb kohandada, koolitada ja varustada piisaval arvul töötajaid.

2.8 See puudutab ka tööstust, millel on vaja turvalist keskkonda tarbijate usalduse suurendamiseks.

2.9 Ülikoolid ja teadusuuringud võivad valgustada uute meediate kasutamist laste poolt. Parim viis turvalisuse-alase sõnumi edasi andmiseks on tutvustada kurjategijate meetodeid meedia valdkonnas, otsida uusi tehnilisi lahendusi ja pakkuda sõltumatut vaatepunkti regulatsiooni ja iseregulatsiooni protsessidest sõltuvate huvide lepitamise kohta.

2.10 Programmil on kaks mõõdet. Sotsiaalses plaanis on programm keskendunud valdkondadele, kus regulatsioon ja turg ei suuda üksi kasutajate turvalisust tagada. Majanduslikus plaanis tuleb edendada interneti ja võrgupõhiste tehnoloogiate turvalist kasutamist, luues usaldusliku õhkkonna.

2.11 Umbes 50 miljoni euro suurune finantseering on kavas arendamaks tehnilisi ja juriidilisi vahendeid, tarkvara ja teavet tõhusamaks võitluseks võrkude ja terminalipunktide rünnakute vastu ja nende kuritahtliku kasutamise vastu ebasoovitava sisuga ja moraalselt, sotsiaalselt või majanduslikult kahjuliku mõjuga elementide kaudu.

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

([2]) Need teemad on valitud komitee poolt eelnevalt tehtud uurimuse alusel.

3. **Komitee üldised tähelepanekud**

3.1 Komitee meenutab oma varasemaid seisukohti laste kaitse kohta internetis ja esimese tegevusplaani kohta. ([1]) Ta tervitab ettepanekut uue plaani kohta võitluseks ebaseadusliku või kahjuliku sisu vastu võrgupõhises suhtluses (vt I. kokkuvõte, käesoleva dokumendi alguses). Komitee toetab programmi *Safer Internet plus* eesmärke ja prioriteete kui vahendeid interneti turvalisuse parendamiseks. Siiski rõhutab komitee probleemi väga laia ulatust ja vajadust rahvusvahelise tegevuse ja määrustike järele, et sellele vastu seista.

3.2 Internet ja uued võrgupõhised kommunikatsioonitehnoloogiad (näiteks mobiiltelefonid ja multimeedia funktsioonidega pihuarvutid, mis on laialt levimas) on komitee arvates teadmistepõhise majanduse, e-majanduse ja e-valitsuse arengu peamiseks vahendiks. Need on muutlikud kultuuriala kommunikatsiooni- ja töö- ning vaba aja vahendid. Seega on esmatähtis tagada kommunikatsioonivõrgustike toimimise turvalisus ja pidevus, kuna tegemist on olulise avaliku teenusega, mis peab jääma avatuks, kättesaadavaks ja mille vastu kasutajatel peab olema usaldus, et ta saaks täita oma erinevaid ülesandeid parimates tingimustes. Kaasata informatsioon interneti turvalisemaks muutmise kohta erinevatesse e-Euroopa programmidesse, eelkõige koolituse osas, oleks kulu-efektiivsuse mõistes üks kõige paljulubavam võimalus saavutada osalevate isikute suurt arvu.

3.3 Internetis valitsevat väljendus- ja suhtlusvabadust kergendab ka ühenduse, kaasa arvatud kiire internetiühenduse suhteliselt madal hind, mis annab üha lihtsamini juurdepääsu multimeediamaterjalidele. Ainult mõned tugeva demokraatia puudujäägiga riigid kontrollivad oma kodanikele kättesaadavate teadete ja materjalide sisu, tehes seda nende vabaduse pideva piiramise hinnaga. Komitee hinnangul tuleb tagada suurenenud turvalisus säilitades ja edendades teabe-, kommunikatsiooni- ja väljendusvabadust.

3.4 Siiski on see väljendus- ja teabevabaduse ala, mida kujutab endast üleilmne võrk, kasutatav rohkem kui teised kommunikatsioonivahendid ebaseaduslikel eesmärkidel nagu pedofiilia või rassistliku ja ksenofoobse sisuga materjalide levitamine; osa nendest materjalidest võib osutuda kahjulikuks teatud publikule, eriti alaealistele, nagu pornograafia või hasartmängud (viimased on mõnes riigis koguni keelatud) ja erinevad kriminaalsed tegevused (läbilaskevõime kuritarvitamine või andmete ja serverite kuritahtlik kasutamine). Komitee kiidab seega heaks tegevusplaani laiendamise kõigile elektroonilistele kommunikatsioonivahenditele, millele võib osaks saada väline ebasoovitav või vaenulik juurdepääs.

3.5 Selle uue ja järjest kasvava ruumi regulatsiooni muudab keeruliseks asjaolu, et see on rahvusvaheline avatud võrgustik, mis on kättesaadav kõigile igast serverist või kliendiarvutist mis on vabalt ühendatud peaaegu kõikjalt maailmast. Paljudes riikides on veel nõrk või puudulik seadusandlus mis võimaldab Euroopa ühenduses keelatud lehekülgedel jätkata tegevust. On väga oluline, et Euroopa Liit avaldaks arvamust ja tegutseks rahvusvahelise tegevuse toetuseks, eelkõige koos peamiste maadega Põhja-Ameerikas ja Aasias, kus kiire internetiühendus on väga levinud, et kaitsta kõige haavatavamaid, ja et võidelda tõhusamalt mittesobiva sisuga (rämpspostituse) e-kirjade vastu, mis ähvardab elektronposti arengut, ja viiruste leviku vastu, mis nõrgestab internetimajandust. Kuigi need on vajalikud Euroopa ühenduse ruumis, tuleb teostatavad vahendid kaasata ka üleilmsesse lähenemisse.

3.6 Kuna veel ei ole olemas rahvusvahelisi kokkuleppeid, võib teatud sisuga materjalide keelamise vastu mõnes riigis koguni TBT ([2]) (tehniliste kaubandustõkete) raames esitada kaebuse WTO-le, seda küsimust tuleks käsitleda käimasolevatel läbirääkimistel.

3.7 Õiguse territoriaalsus ja riiklike seadusandluste mitmekesisus on keeruline lahendamist nõudev probleem. Tehnoloogia areng võimaldab ka otsest igat laadi dokumentide vahetust isikute vahel (P2P, *peer to peer*), kaasa arvatud krüpteeritud dokumendid, mille sisu on võimatu kontrollida: iga masinat või võrku saab kasutada ühe keerulisemate materjalide saatmiseks, igasse serverisse on võimalik sisse logida anonüümselt ja jälgi jätmata ning kasutada võimsaid ja isegi "purunematuid" krüpteerimisvahendeid.

3.8 Kodulehtede ja ajaveebide (*weblog)* mood, äriliste või elektrooniliste finantsteenuste lehekülgede areng, paljud informatiivsed, harivad, teaduslikud ja tehnilised internetilehed, kuid ka pornograafia, hasartmängud jms on põhjuseks, miks maailmas on sadu miljoneid internetilehti. Mingit kontrolli on siiski võimalik teostada võtmesõnade indekseerimisel otsimootorite poolt. Otseühenduste ja automaatse edasisuunamisega võrgukohtade, nagu rämpspost *(spams)* loomist saab samuti kontrollida internetiteenuse osutaja poolt: reklaam ja muu sel moel edasi saadetud ebasoovitav materjal võib olla üldise kahjustava iseloomuga (läbilaskevõime kuritarvitamine, viirused) või kahjustav teatud vastuvõtjatele, nagu lapsed (moraalne või psühholoogiline kahju).

([1]) EMSK arvamus teemal "Programm lapsepõlve kaitseks internetis", pr DAVISON Ettekandja, EÜT C 48, 21.2.2002 ja teemal "Komisjoni teatis nõukogule, Euroopa Parlamendile, majandus- ja sotsiaalkomiteele ja regioonide komiteele – võrkude ja informatsiooni turvalisus : Ettepanek Euroopa poliitilise lähenemisviisi kohta" , ettekandja hr RETUREAU, EÜT C 48, 21.2.2002 ning teemal "Roheline raamat alaealiste ja inimväärikuse kaitse kohta audiovisuaalsete ja informatsiooniteenuste osas", ettekandja pr BARROW, EÜT C 287, 22.9.1997.

([2]) "Tehnilised kaubandustõkked" on lepped, mis käsitlevad teenuste osutamise ja vahetamise tehnilisi takistusi, nt USA *vs* Antigua ja Barbuda juhtum, mis käsitleb *offshore* piirkonnas toimuvaid rahamänge. Otsus on edasi kaevatud MKO'le, dokument nr 03-4429 – ref WT/DS285/3 26.8.2003, kes tegeleb kaebusega. http://www.wto.org/french/tratop_f/dispu_f/distabase_wto_members1_f.htm.

3.9 Internetti kasutavad maffiagrupeeringud, petturid, viiruste autorid, piraadid, tööstusspioonid ja teised õiguserikkujad oma tegevuse arendamiseks. Selle mahasurumine on keeruline, kuigi politsei eriüksused on paljudes riikides asunud neid tuvastama ja lokaliseerima, et neid jälitada ja tuvastatud kriminaalne tegevus lõpetada; see eeldab üldiselt rahvusvahelist kootööd, mida tuleks rohkem soodustada.

3.10 Kuidas võidelda selliste kriminaalsete tegevuste vastu nagu pedofiilide võrgulehed? Nende keelustamine ei tohiks olla juriidiliselt keeruline, kuid tuleks luua võimalused selliste võrgustike avastamiseks; kuidas kaitsta ka lapsi pedofiilide eest, kes tegutsevad jututubades, mida noored eriti hindavad, et neid kohtamisele meelitada. Küsimus ei ole neil konkreetsetel juhtudel keelustamise ja sanktsioneerimise seaduslikkuses, vaid vahendites, kuidas seda teostada.

3.11 Internetiteenuse pakkujad ei saa kontrollida ja jälgida kõiki võrgulehti ja kõiki teateid (mis on erakirjavahetus). Seevastu kohtu, politsei või volitatud lastekaitseteenistuse nõudmisel peavad nad vastama koheselt taotlustele või otsustele selliste võrgulehtede sulgemise kohta ja seda kasutavate isikute tuvastamise kohta, see eeldab, et informatsiooni võrku lülitamise ja ühenduste kohta säilitataks mingi teatud aja jooksul.

3.12 Krediitkaardikompaniid, otsingumootorid ja interneti ühenduse pakkujad peaksid viima läbi kontrolle, avastamaks pedofiilseid ja muid kriminaalse sisuga internetilehti, kasutades indikaatorina näiteks võtmesõnu ja geograafilisi piirkondi. Selle järgi peaksid nad tulemustest teavitama politseid. Sama tehnikat tuleks kasutada tuvastamaks "tarbijaid", kes tellivad lastepornot või "*snuff*"filme ([1]) krediitkaardiga. Vajadusel peaks seadusandlus selliseid kontrolle nõudma. Interneti otsingumootorid peaksid vähendama võimalusi leida lastepornot või muid kriminaalse sisuga materjale võtmesõnade ja fraaside kasutamise läbi.

3.13 See eeldab ka riigivõimu poolseid kohaseid võitlusvahendeid, kvalifitseeritud personali, üldist piiriülest koostööd ja tasakaalustatud norme siseriiklikul, Euroopa ja rahvusvahelisel tasandil, mis ei piira interneti kasutajate vabadusi, võimaldades samas muuta tegutsemisvõimetuks kahjustavaid isikuid ja rühmitusi, kes kasutavad neid võrke edastamaks ebaseaduslikke materjale ja ebakohase või kahjuliku sisuga materjalide blokeerimist.

3.14 Samuti, et olla tõhus, peab see võitlus puudutama otseselt kõiki interneti kasutajaid, keda tuleb koolitada ja teavitada ettevaatusabinõudest ja vahenditest, mida kasutada, et varustada ennast selliste ohtlike või ebasoovitavate materjalide vastuvõtmise vastu, ja et mitte olla kasutatud selliste materjalide edastamiseks. Tegevusplaani informeerimise ja koolituse osa peaks komitee arvamuse kohaselt omistama prioriteetse tähtsuse kasutajate mobiliseerimisele selleks, et nad kannaksid iseenda ja oma ülalpeetavate tegevuse eest vastutust. Näiteks on probleemsed mitteametlikud tervisealased internetileheküljed. Enda kaitsmiseks peavad ettevõtted hoolitsema oma töötajate koolituse eest ja oma võrkude ning e-kaubanduse võrgulehtede turvaliseks muutmise eest, kuid ka valitsusasutused ja riiklikud ning erainstitutsioonid peavad kasutama samu turvalisuse strateegiaid ja tagama töödeldud andmete, eelkõige isiklikku laadi andmete absoluutse konfidentsiaalsuse. Teadvustamise suurenemisega peaks kaasnema kvaliteetsete võrgumaterjalide edendamine ja õhutamine tervislikele võrguvälistele tegevustele ning aitaks vältida liigset Internetis viibimist ja mängimist, sest see võib pikapeale teatud ebaküpseid isikuid mõjutada.

3.15 Kasutajad peavad oma vahendeid, mis aitavad neil lihtsalt teatada ebaseaduslikest materjalidest, mida nad internetis kohtavad, spetsialiseeritud kõnekeskustele või tunnustatud asutustele või politsei eriüksustele, hoiatamaks võimuasutusi, et need saaks vajadusel tarvitusele võtta vajalikud meetmed. Vanematele tuleks suunata hoiatusi riikides, kus laste väärkohtlemine *online* pornograafiaks erinevatel kandjatel on levinud, näiteks liidu välispiirialadel; see võiks olla osa koostööprogrammist RELEX.

3.16 Kiites heaks programmi erieesmärgid: võimaldada kasutajatel teatada ebaseaduslikest materjalidest (*hotlines*), arendada soovimatu sisuga materjalide filtreerimise tehnoloogiaid, materjalide klassifitseerimine, võitlus rämpsposti vastu, tööstuse autoregulatsioon, ja teadmine tehnoloogiate turvalisest kasutamisest, soovitab komitee oma erimärkustes, et vajalik oleks arvestada veel mõnda lisaeesmärki.

4. **Komitee erimärkused**

4.1 Komitee on juba varem komisjonile esitanud soovi, et ülemäärast bürokraatiat EL finantseeritavate programmide puhul vähendataks, eriti selleks, et lihtsustada väikeprojektide ja kohaliku tasandi VVOde ligipääsu neile programmidele. Komitee toetab seiret keskendumisega programmi raames saavutatud konkreetsetele tulemustele ja välja pakutud lahenduste efektiivsusele. Tulemustest teatamine peaks olema vähem salastatud.

4.2 Komitee jaoks tuleks arvesse võtta normatiivseid meetmeid, mis toetaksid lõppkasutajate kaitset, võimalusel selle programmi raames või siis komisjoni uue algatuse läbi.

([1]) Filmid, kus näidatakse erilist vägivalda ja piinamist ning tõelist surma.

4.3 Täielikult tuleks rakendada Internetile ligipääsu võimaldava tarkvara ja serverite haldussüsteemide tarkvara autorite vastutust ja võitlust sissetungide vastu; kasutajatel peaks olema garantii, et nende tarkvaraprogrammide autorid kasutavad parimat tehnikat ja ajakohastavad oma tooteid regulaarselt. Autoregulatsioon, ja vajadusel kohustuslik ühenduse norm, peaks klientide kindlustunnet veelgi tugevdama.

4.4 Internetiteenuse pakkujad peaksid välja pakkuma (mida paljud nende hulgast juba ka teevad) lihtsaid vahendeid viirusevastaseks võitluseks võrgulehel, enne kirja või sellele lisatud dokumentide avamist, ja pakkuma võimalusi posti eelnevaks filtreerimiseks rämpsposti vastu. See võib olla äriliseks eeliseks neile teenusepakkujatele, kes teevad tõsiseid pingutusi oma klientide kaitsmiseks. Asjaolu tõttu, et lapsed on interneti kasutamises vanematest sageli sammujagu ees, peaksid posti filtreerimise, viiruste kõrvaldamise ja vanemliku kontrolli süsteemid olema eelnevalt installeeritud ja lihtsad kasutada ja hallata isikutele, kellel ei ole erilisi tehnilisi teadmisi.

4.5 Programm peaks edendama ka uurimistööd erinevate programmide koodi "veekindluse" kontrollimise spetsiaalsete turvalisuse ja kaitsealaste tarkvaraprogrammide ja teiste vahendite osas, õhutama või vajadusel kohustama teenuse osutajaid tarnima kiiresti parandused *(patches)* kõigile tuvastatud või teatatud puuduste jaoks, mis on võimaldanud rünnakuid ning arendama riistvara- ja tarkvaraliste tulemüüride efektiivsust ning filtreerimise ja materjalide tegeliku päritolu tuvastamise meetodeid.

4.6 Komitee oleks soovinud, et eelmise plaani *Safer Internet* efektiivsuse ja plaani raames saavutatud tulemuste hinnangut, koos käsitletud probleemide liigitusega kategooriate kaupa, oleks levitatud palju laiemalt. Tuleks tagada, et kõik seosed finantseeritud projektidega jääks aktiivseks ja oleks kasutajatele paremini tuntud. Komisjoni kodulehekülg peaks sisaldama teavet ka erinevates liikmesriikides või kolmandates riikides omandatud vastavate algatuste, kogemuste, teabevahetuse ja koostöö ideede kohta.

4.7 On täiesti võimalik vastu võtta seaduslikke meetmeid. Interneti teenusepakkujad, krediitkaardikompaniid, otsingumootorid on alati vastuvõtlikud regulatsioonile ja mõned kasutavad juba autoregulatsiooni. Kriminaalkaristused terrorismi, rassismi, suitsiidi või lastepornograafiat propageerivate võrgulehtede vastu peaks olema ranged ja mõjuvad; suuremaid rahvusvahelisi pingutusi tuleks teha selliste võrgulehtede tuvastamiseks ja lokaliseerimiseks, et lasta need siis olukorrast sõltuvalt sulgeda või alustada sellesuunalisi läbirääkimisi vastava lehekülje asukohariigi ametivõimudega.

5. **Järeldused**

Toetades küll täielikult programmi *"Safer Internet plus"* jätkamist ja laiendamist leiab komitee (kes muuseas kutsus üles selle loomisele), et kuritarvituste tõsidus ja laiaulatuslikkus, esmajoones laste vastu, eeldab kiireid täiendavaid seadusandlikke tegevusi ja praktilisi meetmeid vastavalt vajadusele järgmistes valdkondades:

— kõigi asjaomaste ettevõtete üldine kohustus kaitsta lapsi ja kasutajaid laiemalt ning eriti kõige kergemini haavatavaid,

— filtreerimissüsteemide installeerimine vaikimisi,

— selged turvalisuse sõnumid kõigi *online* jututubade *(chat rooms)* esilehtedel ja juurdepääsuportaalidel,

— toetus ühingutele, kes loovad otseliinid (*hot lines*) teavitamiseks lapsi tõsiselt kahjustavatest võrgulehtedest ja tegevustest,

— krediitkaartide kasutamise takistamine lasteporno ja muude kriminaalse sisuga materjalide tellimiseks, kui ka rahapesuks Interneti vahendusel,

— vanemate ja haridustöötajate ning ka riigi esindajate hoiatamine ja neile suunatud tegevuste toetamine riikides, kus laste väärkohtlemine pornograafilisel eesmärgil kujutab tõsist probleemi,

— enam tegevust laste pornograafilistel eesmärkidel kasutamise ja organiseeritud kuritegevuse seoste osas,

— kahjustava sisuga materjalide tuvastamise ja teavitamise süsteem ja rassistlike materjalide äravõtmine, informatsiooni levitamine interneti teel toimuvate pettuste ja selliste ainete, mis tervist võivad kahjustada kohta, et kaitsta haavatavaid või halvasti informeeritud isikuid,

— koostöö ja ühised reeglid rahvusvahelisel tasandil tõhusamaks võitluseks rämpsposti vastu,

— rahvusvaheline koostöö (varajase hoiatuse süsteemi parendamine) ja hirmutavad kriminaalkaristused viiruste levitajatele ja era- ning avalik-õiguslike võrkude ebaseadusliku kasutamise eest kriminaalsetel eesmärkidel (sisetungimine võrgu hõivamise eesmärgil tööstusspionaaži puhul, läbilaskevõime rikkumine ja teised kuritarvituslikud kasutused).

Brüssel, 16. detsember 2004.

Euroopa majandus- ja sotsiaalkomitee

president

Anne-Marie SIGMUND