# Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal "Komisjoni teatis nõukogule, Euroopa Parlamendile, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele — Turvalise infoühiskonna strateegia — dialoog, partnerlus ja aktiivne osalemine"

*KOM(2006) 251 (lõplik)*

(2007/C 97/09)

31. mail 2006 otsustas komisjon vastavalt EÜ asutamislepingu artiklile 262 konsulteerida Euroopa Majandus- ja Sotsiaalkomiteega järgmises küsimuses: *"Komisjoni teatis nõukogule, Euroopa Parlamendile, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele — Turvalise infoühiskonna strateegia — dialoog, partnerlus ja aktiivne osalemine"*

Asjaomase töö ettevalmistamise eest vastutava transpordi, energeetika, infrastruktuuri ja infoühiskonna sektsiooni arvamus võeti vastu 11. jaanuaril 2007. Raportöör oli hr PEZZINI.

Euroopa Majandus- ja Sotsiaalkomitee võttis täiskogu 433. istungjärgul 15.–16. veebruaril 2007 (16. veebruari istungil) vastu järgmise arvamuse. Poolt hääletas 132, erapooletuks jäi 2.

## 1. **Järeldused ja soovitused**

1.1 Euroopa Majandus- ja Sotsiaalkomitee veendumuse kohaselt on teabeturve ettevõtete, haldusorganite, riigi- ja eraasutuste ning eraisikute jaoks üha suurenev probleem.

1.2 Euroopa Majandus- ja Sotsiaalkomitee ühineb põhiosas uut strateegiat nõudvate analüüside ja argumentidega, et parandada võrgu- ja teabeturvet ning tõkestada rünnakuid ja sissetungimised, mis ei tunne riigipiire.

1.3 Euroopa Majandus- ja Sotsiaalkomitee usub, et komisjon peaks tegema veel jõupingutusi, et jõustada uuenduslik ja kooskõlastatud strateegia, milles arvestatakse nähtuse ulatust ja selle mõju majandusele ja eraelule.

1.3.1 Lisaks juhib komitee tähelepanu asjaolule, et komisjon võttis hiljuti vastu teatise teabeturbe kohta ning lähitulevikus avaldatakse samal teemal veel üks dokument. Euroopa Majandus- ja Sotsiaalkomitee jätab endale õiguse koostada tulevikus ulatuslikum arvamus, milles võetakse arvesse kõiki teatiseid.

1.4 Euroopa Majandus- ja Sotsiaalkomitee rõhutab, et teabeturbe aspekti ei tohi mitte mingil juhul lahutada andmekaitse tõhustamisest ja vabaduste kaitsest, mis on tagatud Euroopa inimõiguste konventsiooniga.

1.5 Euroopa Majandus- ja Sotsiaalkomitee küsib, milline on kõnealuse ettepaneku lisaväärtus praeguses olukorras võrreldes 2001. aastal vastu võetud tervikliku lähenemisviisiga, mille eesmärk oli sama kui nüüd esitatud teatisel ([1]).

1.5.1 Ettepanekule lisatud mõjuhinnang ([2]) on 2001. aasta olukorraga võrreldes mitmes punktis samm paremuse pool, kuid see on avaldatud vaid ühes keeles ning seetõttu mõistetamatu paljudele Euroopa kodanikele, kes kujundavad oma arvamuse ühenduse keeltes kättesaadava ametliku dokumendi järgi.

1.6 Euroopa Majandus- ja Sotsiaalkomitee tuletab meelde 2005. aastal Tuneesias toimunud infoühiskonda käsitleva tippkohtumise järeldusi, mis võeti vastu ÜRO peaassambleel 27. märtsil 2006:

— mittediskrimineeriva juurdepääsu põhimõte;

— info- ja sidetehnoloogia kasutamine rahu tagamise vahendina;

— demokraatia, ühtekuuluvuse ja hea valitsemistava tugevdamise vahendid;

— kuritarvituste ennetamine inimõigusi järgides ([3]).

1.7 Euroopa Majandus- ja Sotsiaalkomitee rõhutab, et dünaamiline ja terviklik ühenduse strateegias peaks lisaks dialoogile, partnerlusele ja aktiivsele osalemisele hõlmama järgmist:

— ennetusmeetmed;

— vajadus liikuda teabeturbest edasi "teabekindlustusele" ([4]);

— turvalise ja tunnustatud ELi õigusliku raamistiku loomine, milles kehtestatakse ka karistused;

— tehniline standardimise tugevdamine;

([1]) EMSK arvamus "Komisjoni teatis nõukogule, Euroopa Parlamendile, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele "Võrgu- ja teabeturve: ettepanek Euroopa poliitilise lähenemisviisi kohta"", EÜT C 48, 21.2.2002, lk 33.

([2]) Mõjuhinnang ei ole sedavõrd kaalukas kui strateegia dokument.

([3]) ÜRO soovitused nr 57 ja nr 58, 27.3.2006; Tuneesia, lõppdokument nr 15.

([4]) "Emerging strategies in the context of security", Ühisuuringute Keskus — Kodanike kaitse ja julgeoleku instituut, strateegiauuringute väljaanne, september 2005, Euroopa Komisjon, http://serac.jrc.it.

— kasutajate digitaalne tuvastamine

— Euroopa tulevikuanalüüside käivitamine mitmekesise tehnoloogiliselt ühtlustatud teabeturbe kohta;

— Euroopa ja liikmesriikide tugevamad riskihindamise mehhanismid;

— teabe monokultuuride tekkimise tõkestamise meetmed;

— parem ühendusepoolne kooskõlastamine Euroopa ja rahvusvahelisel tasandil;

— peadirektoraatide vahelise info- ja sidetehnoloogia turvakeskuse loomine;

— Euroopa võrgu- ja teabeturbevõrgustiku loomine;

— Euroopa teabeturbeuuringute rolli optimeerimine;

— Euroopa arvutiturbepäeva sisseviimine;

— ELi teabeturbe alased näidistegevused eri tüüpi koolides.

1.8 Euroopa Majandus- ja Sotsiaalkomitee on seisukohal, et ühenduse dünaamilise ja tervikliku strateegia tagamiseks on vaja eraldada vastavad eelarvevahendid ning kavandada ühenduse tasandil koostöö parandamise algatusi ja meetmeid, mis võimaldaks Euroopa Liidul maailmaga ühtselt platvormilt suhelda.

## 2. **Põhjused**

2.1 Infoühiskonna turvalisus on peamine proovikivi sidevõrkude ja -teenuste usaldusväärsuse ja kindluse tagamisel, sest need on majanduse ja ühiskonna arengu otsustavad tegurid.

2.2 Teabevõrke ja -süsteeme tuleb kaitsta, et säilitada konkurentsivõime ja kaubeldavus, tagada elektroonilise side terviklikkus ja järjepidevus, hoida ära pettusi ja tagada eraelu õiguslik kaitse.

2.3 Elektrooniline side ja sellega seotud teenused on kogu telekommunikatsioonisektori suurim segment: 2004. aastal kasutas 90 % Euroopa ettevõtetest aktiivselt Internetti ja 65 % töötas välja oma veebilehe, samal ajal kui arvestuste alusel kasutab ligikaudu pool Euroopa elanikest korrapäraselt Internetti ja 25 % majapidamistest kasutab püsivalt lairibaühendust ([5]).

([5]) i2010: turvalise infoühiskonna strateegia — teabeleht nr 8 (juuni 2006), Euroopa Komisjon, infoühiskond ja meedia. http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

2.4 Investeeringute arengut silmas pidades on turvalisuse heaks tehtavate kulutuste maht ainult 5-13 % kõikidest infotehnoloogiasse tehtavatest investeeringutest. See protsendimäär on liiga väike. Viimaste uuringute kohaselt on keskmiselt 30 protokollist, mida võtmestruktuurid jagavad, 23 vastuvõtlikud multiprotokolli rünnetele ([6]). Hinnangute kohaselt saadetakse iga päev keskmiselt 25 miljonit elektroonilist rämpspostisõnumit ([7]) ja seetõttu tervitab Euroopa Majandus- ja Sotsiaalkomitee komisjoni hiljutist ettepanekut kõnealuse teema kohta.

2.5 Arvutiviiruste ([8]), ussviiruste ([9]) ja nuhkvara ([10]) kiire levik on toimunud paralleelselt elektroonilise side süsteemide ja võrkude kiire arenguga. Need muutusid üha keerukamaks ja samal ajal üha haavatavamaks, seda ka multimeedia, mobiiltelefonide ja GRIDi teabevara ([11]) süsteemide ühtluse tõttu: väljapressimisjuhtumid, mille käigus kasutati hajutatud teenusetõkestamise ründeid, identiteedi vargus internetis, andmepüük ([12]), piraatlus ([13]) jne, on proovikivid infoühiskonna turvalisusele, mida Euroopa Ühendus käsitles kolme alljärgneva sekkumistelje alusel 2001. aasta teatises ([14]) (Euroopa Majandus- ja Sotsiaalkomitee on koostanud teatise kohta ka arvamuse ([15])):

— erilised turvameetmed;

([6]) Proceedings of the First International Conference on Availability, Reliability and Security — köide 00, ARES 2006, väljaandja IEEE Computer Society.

([7]) SPAM = soovimatu kaubanduslik e-kiri. Spam tähendas alguses vürtsisealiha- ja singikonserve (spiced pork and ham), mis oli väga populaarne Teise maailmasõja ajal, kui sellest sai USA üksuste ja Ühendkuningriigi elanike jaoks põhitoiduaine. Pärast aastaid kestnud ülemäärast konservide tarbimist sai inimestel sellest isu täis.

([8]) *Arvutiviirus*: õelvara kategooriasse kuuluv spetsiaalne tarkvara, mis võib käivitamisel nakatada faile nii, et need paljundavad ennast ise, tavaliselt ilma, et kasutaja seda märkaks. Viirused võivad põhjustada erineva ulatusega kahju peremees-opsüsteemile ja lõpuks põhjustada ressursside raiskamist RAM, CPU ja kõvaketta ruumi osas. (http://et.wikipedia.org/wiki/Arvutiviirus).

([9]) Uss — ise leviv õelvara: e-posti uss on hävitava toimega võrgurünne, mis kogub kliendi e-posti programmist (nt MS Outlook) kõik e-posti aadressid ja saadab manuses oleva ussprogrammiga nendel e-posti aadressidel sadu e-kirju.

([10]) Nuhkvara — tarkvaraprogrammid, mis salvestavad kasutaja Internetis surfamise "jäljed" ja installeerivad end ise, kasutajat teavitamata ja tema teadmata, nõusolekuta ja kontrollita.

([11]) GRIDi teabevara — võimaldab paljusid üksteisest eemal asuvaid arvutiressursse (nt superarvutid, arvutiklastrid, mälusüsteemid, andmeallikad, vahendid, inimressursid) jagada, valida ja koondada ning seob need ühtseks ressursiks keerukate arvutuste ja andmemahukate arvutirakenduste teostamiseks.

([12]) Andmepüük — infotehnoloogias kirjeldab see mõiste muukimise vormi, millega soovitakse saavutada juurdepääs isiku- ja konfidentsiaalsetele andmetele eesmärgiga varastada ID. Sellele eesmärgil saadetakse võltsitud elektroonilisi teateid, mis on koostatud selliselt, et mõjuvad autentsena.

([13]) Piraatlus — nn tarkvarapiraatide poolt kasutatav mõiste tarkvara kohta, mille paljundamiskaitse on eemaldatud ja mis on allalaadimiseks Internetti installeeritud.

([14]) KOM(2001) 298 (lõplik).

([15]) Joonealune märkus 1.

— õiguslik raamistik koos andmekaitse ja eraelu kaitsega;

— küberkuritegude vastane võitlus.

2.6 Infotehnoloogiavastaste rünnete kindlakstegemine, tuvastamine ja ennetamine võrgusüsteemi raames on proovikivi sobivate lahenduste otsimisel, sest konfiguratsioonid muutuvad pidevalt, võrguprotokollid ning pakutavad ja arendatavad teenused on mitmekesised ja asünkroonsed ründevormid on äärmiselt keerukad ([16]).

2.7 Kahjuks alahinnatakse riske ja turvakultuuri arendamisele pööratakse vähe tähelepanu, sest investeeringute tulusus on turvavaldkonnas vaevumärgatav ja kasutajate omavastutus nõrgalt välja kujunenud.

## 3. **Komisjoni ettepanek**

3.1 Turvalise infoühiskonna strateegiat ([17]) käsitleva teatisega tahab komisjon parandada teabeturvet dünaamilise ja tervikliku strateegia kaudu järgmistel alustel:

a) asutuste ja komisjoni vahelise dialoogi parandamine liikmesriikide meetmete võrdleva hindamise ja *elektroonilise side* turvalisuse alaste heade tavade väljaselgitamise kaudu;

b) VKEde ja kodanike teadlikkuse suurendamine tõhusate turvasüsteemide valdkonnas komisjoni algatuste ning Euroopa Võrgu- ja Infoturbeameti (ENISA) suurema kaasamise kaudu;

c) vahendeid ja sätteid käsitlev dialoog, et tagada tasakaalustatud suhe turvalisuse ja põhiõiguste, kaasa arvatud eraelu kaitse vahel.

3.2 Lisaks sätestatakse teatises, et ENISA loob usaldusväärse partnerluse, et töötada välja asjakohane raamistik turvaintsidente, tarbijate usaldust ja turvatööstuse suundumusi käsitlevate andmete kogumiseks:

a) liikmesriikidega;

b) tarbijate ja kasutajatega;

c) teabeturbetööstusega;

d) erasektoriga,

ja rajab mitmekeelse ELi portaali, mis annab teavet ja hoiatab riskide eest erasektori, liikmesriikide ja teadlaste strateegilise partnerluse huvides.

3.2.1 Lisaks sätestatakse teatises asjahuviliste ringkondade suurem vastutus turvavaldkonna vajaduste ja riskide eest.

3.2.2 Rahvusvahelise koostöö osas kolmandate riikidega märgib komisjon, et "võrgu- ja teabeturbe globaalne ulatus sunnib komisjoni suurendama pingutusi võrgu- ja teabeturbealase ülemaailmse koostöö edendamisel nii rahvusvahelisel kui liikmesriikidega kooskõlastamise tasandil" ([18]). Kahjuks ei kajastu see soovitus dialoogi, partnerluse ja aktiivse osalemise meetmete puhul.

## 4. **Märkused**

4.1 Euroopa Majandus- ja Sotsiaalkomitee nõustub piiranguteta analüüside ja kaalutlustega tervikliku ja dünaamilise Euroopa strateegia loomiseks võrgu- ja teabeturbe eesmärgil, sest peab turvaküsimust oluliseks, et soodustada positiivset suhtumist infotehnoloogiasse ja suurendada usaldust viimatinimetatu vastu. Komitee seisukohad on kajastatud arvukates arvamustes ([19]).

4.1.1 Euroopa Majandus- ja Sotsiaalkomitee kinnitab taas ([20]), et "Internet ja uued võrgupõhised sidetehnoloogiad (näiteks mobiiltelefonid ja multimeediafunktsioonidega pihuarvutid, mis on laialt levimas) … on komitee arvates teadmistepõhise majanduse, e-majanduse ja e-valitsuse arengu peamiseks vahendiks".

---

([16]) Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* — 2005 USA, Arizona
Internet Technology Laboratory, ECE Department, The University of Arizona, http://www.ece.arizona.edu/~hpdc
Mazin Yousif, Intel Corporation, USA. Work supported in part by a grant from Intel Corporation IT R&D Council.

([17]) KOM(2006) 251, 31.5.2006.

([18]) KOM(2006) 251, 3. peatüki eelviimane lõik.

([19]) — EMSK arvamus *"Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv andmete säilitamise kohta, mida on töödeldud üldkasutatavate elektrooniliste sideteenuste osutamisel, ja millega muudetakse direktiivi 2002/58/EÜ"*.— ELT C 69, 21.3.2006, lk 16
— EMSK arvamus *"Komisjoni teatis nõukogule ja Euroopa Parlamendile, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele: i2010 — Euroopa infoühiskond majanduskasvu ja tööhõive eest."* — ELT C 110, 9.5.2006, lk 83
— EMSK arvamus *"Ettepanek Euroopa Parlamendi ja nõukogu otsuse kohta, millega luuakse ühenduse mitmeaastane programm, edendamaks Interneti ja uute võrgupõhiste tehnoloogiate turvalisemat kasutamist"*. ELT C 157, 28.6.2005, lk 136
— EMSK arvamus "Komisjoni teatis nõukogule ja Euroopa Parlamendile, Euroopa Majandus- ja Sotsiaalkomiteele ja Regioonide Komiteele võrgu- ja infoturbe kohta: ettepanek Euroopa lähenemisviisi kohta" — EÜT C 48, 21.1.1002, lk 33.

([20]) Joonealune märkus 19, kolmas taane

4.2 *Komisjoni ettepanekute tugevdamine*

4.2.1 Komisjoni ettepaneku kohaselt peaks kõnealune dünaamiline ja terviklik strateegia tuginema kõiki osapooli hõlmavale avatud ja integreerivale dialoogile ning sidusrühmade, eelkõige kasutajate partnerlusele, ning nende aktiivsele osalemisele. Komitee on seisukohal, et lähenemine peaks olema veelgi laiem.

4.2.2 Kõnealust hoiakut rõhutati varasemates arvamustes: "Et olla tõhus, peab see võitlus puudutama samuti otseselt kõiki Interneti kasutajaid, keda tuleb koolitada ja teavitada ettevaatusabinõudest ja vahenditest, mida kasutada selleks, et varustada ennast selliste ohtlike või ebasoovitavate materjalide vastuvõtmise vastu, ja et mitte lasta end kasutada selliste materjalide edastamiseks. Tegevuskava teavitamise ja koolituse osa peaks komitee arvamuse kohaselt omistama prioriteetse tähtsuse kasutajate kaasamisele" ([21]).

4.2.3 Euroopa Majandus- ja Sotsiaalkomitee arvamuse kohaselt tuleb kasutajad ja kodanikud kaasata aga sellisel viisil, et vajalik teabe- ja võrgukaitse oleks kooskõlas kodanike õiguste ja kasutajate õigusega turvalisele juurdepääsule ja taskukohastele hindadele.

4.2.4 Meeles tuleb pidada, et teabeturve nõuab tarbijatelt kulutusi, seda ka takistuste kõrvaldamisele või vältimisele kulutatud aja mõttes. Euroopa Majandus- ja Sotsiaalkomitee on seisukohal, et juba arvuti soetamisel peaks sellega kohustuslikus korras olema kaasas viirustõrjesüsteem. Kasutaja saaks valida, kas ta soovib seda sisse või välja lülitada, kuid süsteem peaks arvutis kohe alguses olema.

4.3 *Dünaamilisem ja uuenduslikum ühenduse strateegia*

4.3.1 Lisaks peaks EL seadma Euroopa Majandus- ja Sotsiaalkomitee arvates auahnemad eesmärgid, kutsuma ellu uuenduslikku, tervikliku ja dünaamilise strateegia ja esitama uued algatused, nagu näiteks:

— mehhanismid, mis võimaldavad digitaalselt tuvastada üksikasutajaid, kellel praegu palutakse liiga tihti sisestada isiklikke andmeid.

— ETSI meetmed ([22]), mis võivad toimida info- ja sidetehnoloogia turvalise kasutamise eeldusena ja pakkuda kiireid lahendusi, mida määratletakse kogu ELis ühtse turvalisuse piirmäära alusel;

— ennetusmeetmed turvalisuse miinimumnõuete integreerimise kaudu teabe- ja võrgusüsteemidesse ja näidistegevuste, näiteks turvakursuste läbiviimine igat tüüpi koolides;

— turvalise ja tunnustatud õigusliku raamistiku loomine Euroopa tasandil; selle raamistiku kohandamine teabe ja võrkudega, et võimaldada teabeturbelt üle minna "teabekindlustusele";

— Euroopa ja liikmesriikide riskihindamismehhanismide parandamine ja suurem võimsus seaduste ja eeskirjade rakendamiseks, tõkestamaks teabekuritegevust eraelu ja andmearhiivide suhtes;

— meetmed kergemini haavatavate toodete ja lahendustega IT monokultuuride tekkimise ärahoidmiseks; uute paljukultuuriliste uuenduste toetamine eesmärgiga luua ühtne Euroopa teaberuum (SEIS — *Single European Information Space*);

4.3.2 EMSK soovitab luua peadirektoraatide vahelise info- ja sidetehnoloogia turvapunkti ([23]). Turvapunkt võimaldaks:

— komisjoni talituste koostööd;

— liikmesriikide tasandil koostalitlusvõime, ID halduse, eraelu kaitse, teabele ja teenustele vaba juurdepääsu, turvalisuse miinimumnõuete horisontaalseid lahendusi kasutades;

— rahvusvahelisel tasandil, et Euroopa Liit kõneleks eri organisatsioonides, näiteks ÜROs, G 8-s, OSCEs ja ISOs ühehäälselt.

4.4 *Vastutustundlikumad kooskõlastamismeetmed ELi tasandil*

4.4.1 EMSK peab väga oluliseks ka Euroopa võrgu- ja teabeturbevõrgustiku loomist, mille kaudu on võimalik läbi viia küsitlusi, uuringuid ja töötubasid turvamehhanismide ja nende koostalitlusvõime, arenenud kodeerimise ja eraelu kaitse kohta.

4.4.2 EMSK usub, et Euroopa teadustegevuse rolli saaks selles väga tundlikus sektoris optimeerida alljärgnevate programmide kasuliku sünteesiga:

— Euroopa julgeoleku-uuringute programmi (ESRP) ([24]), teadus- ja arendustegevuse seitsmes raamprogramm;

([21]) Joonealune märkus 19, kolmas taane.

([22]) ETSI = Euroopa Telekommunikatsioonistandardite Instituut; vt eriti 16.–17. jaanuari 2006. aasta töötuba. ETSI on töötanud muuhulgas välja spetsifikatsioonid ebaseadusliku pealtkuulamise (TS 102 232, 102 233 ja 102 234), raadiokohtvõrgu Interneti-juurdepääsude (TR 102 51) ja elektrooniliste allkirjade kohta, samuti GPRS ja UMTS mobiiltelefonide turvaalgoritmid.

([23]) Seda peadirektoraatide vahelist keskust võiks rahastada teadus- ja arendustegevuse seitsmenda raamprogrammi eriprogrammi "Koostöö" IST prioriteetide raames või Euroopa julgeoleku-uuringute programmi (ESRP) kaudu.

([24]) Cf. FP7, ühenduse teadusuuringute ja tehnoloogiaarenduse seitsmes raamprogramm, "Koostöö" programm; turvalisuse uurimisprioriteedid eelarvega 1,35 miljardit eurot perioodiks 2007–2013.

— programm *Safer Internet Plus*;

— Euroopa kriitilise infrastruktuuri kaitse programm (EPCIP) ([25])

4.4.3 Nendele ideedele võiks lisada veel Euroopa arvutiturbe päeva sisseviimise; selle päeva raames korraldataks koolides riiklikke hariduskampaaniaid ja kodanikele suunatud teabekampaaniaid teabekaitsemeetodite kohta arvutites. See oleks loomulikult lisa teabele tehnoloogilise progressi kohta arvutite üha muutuvas valdkonnas.

4.4.4 Euroopa Majandus- ja Sotsiaalkomitee on korduvalt rõhutanud järgmist: "Digitaalsete tehingute tajutav turvalisus ja usaldusväärsus määrab selle, kui kiiresti suudavad ettevõtted info- ja sidetehnoloogiat oma tegevuses kasutusele võtta. Tarbija valmisolekut anda mõnel veebilehel oma krediitkaardi number mõjutab see, kuivõrd turvalisena tarbija seda toimingut tajub." ([26])

4.4.5 Euroopa Majandus- ja Sotsiaalkomitee on veendunud, et sektori tohutut kasvupotentsiaali arvestades on vaja võtta erimeetmeid ja kohandada olemasolevad meetmed uute suundumustega. Euroopa teabeturbe algatused peavad olema kooskõlas tervikliku strateegiaga, kõrvaldades eri sektorite vahelised piirid ning tagades info- ja sidetehnoloogia ühtlase ja turvalise leviku ühiskonnas.

4.4.6 Euroopa Majandus- ja Sotsiaalkomitee leiab, et mitmed olulised strateegiad, kaasa arvatud siin käsitletav, edenevad liiga aeglaselt bürokraatlike ja kultuuriliste takistuste tõttu, mida liikmesriigid seavad olulistele ühenduse tasandil langetatavatele otsustele.

4.4.7 Samuti leiab Euroopa Majandus- ja Sotsiaalkomitee, et ühenduse eraldatud ressursid ei ole piisavad mitmete kiireloomuliste projektide elluviimiseks; nimetatud projektid saavad anda globaliseerumisest tulenevatele uutele probleemidele konkreetseid vastuseid vaid siis, kui need viiakse ellu ühenduse tasandil.

4.5 *ELi tarbijakaitse tugevam tagatis*

4.5.1 Euroopa Majandus- ja Sotsiaalkomitee teab, et liikmesriigid on tehnoloogilised turvameetmed ja turvajuhtimise meetodid välja töötanud enda vajadusi arvestades ja keskenduvad sealjuures eri aspektidele. Seetõttu on raske leida turvaprobleemidele ühemõttelist ja tõhusat vastust. Kui välja arvata mõned haldusvõrgud, siis puudub liikmesriikide vahel süstemaatiline piiriülene koostöö, kuigi turvaküsimusi ei ole liikmesriikidel võimalik eraldi lahendada.

4.5.2 Euroopa Majandus- ja Sotsiaalkomitee juhib siiski tähelepanu, et nõukogu on raamotsusega 2005/222/JSK loonud kohtute ja muude pädevate asutuste koostöö raamistiku, et tagada eri riikide karistusõiguse sätete kohandamise teel liikmesriikide ühtne lähenemisviis järgmistele teabesüsteemide ründeid käsitlevatele aspektidele:

— ebaseaduslik sisenemine teabesüsteemidesse;

— ebaseaduslik sekkumine teabesüsteemi töö tahtliku takistamise või katkestamise kaudu;

— ebaseaduslik andmetesse sekkumine eesmärgiga teabesüsteemis asuvad arvutiandmed kustutada, kahjustada, rikkuda, muuta, sulustada või ligipääsmatuks muuta;

— eelnimetatud kuritegudele kallutamine või nendele kaasaaitamine.

4.5.3 Lisaks on raamotsuses esitatud kriteeriumid juriidiliste isikute vastutuse tuvastamiseks ning nimetatud sanktsioonid, mida on võimalik vastutuse tuvastamise korral kohaldada.

4.5.4 Dialoogi osas liikmesriikide asutustega toetab Euroopa Majandus- ja Sotsiaalkomitee komisjoni ettepanekut, et kõnealused asutused peavad teostama riigi teabevõrkude ja -süsteemide turbe alaste tegevuspõhimõtete (sealhulgas avaliku sektori konkreetsete tegevuspõhimõtete) võrdleva hindamise. See ettepanek esitati EMSK 2001. aasta arvamuses ([27]).

4.6 *Turvakultuuri laiem levitamine*

4.6.1 Teabeturbetööstus peab tõhusal viisil tagama, et tema paigaldiste materiaalsel järelevalvel ja side kodeerimisel kasutatakse vahendeid, mis vastavad tehnika arengu tasemele, et kaitsta klientide õigust eraelule ja konfidentsiaalsusele ([28]).

([25]) KOM(2005) 576, 17.11.2005.
([26]) Joonealune märkus 19, teine taane.
([27]) Joonealune märkus 19, neljas taane.
([28]) Vt direktiivi 97/66/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset telekommunikatsioonisektoris (EÜT L 24, 30.1.1998).

4.6.2 Teadlikkuse suurendamise meetme osas peab Euroopa Majandus- ja Sotsiaalkomitee esmatähtsaks tõelise turvakultuuri loomist, mis on täielikult kooskõlas teabe-, side- ja sõnavabadusega. Paljud kasutajad ei ole kõikidest arvutipiraatluse turvariskidest teadlikudki, samal ajal kui paljud operaatorid, müüjad või teenuseosutajad ei suuda hinnata, kas ja millises ulatuses esineb süsteemis nõrku kohti.

4.6.3 Eraelu ja isikuandmete kaitse on esmatähtsad eesmärgid, tarbijatel on aga ka õigus tõeliselt tõhusale kaitsele isikuandmete kuritarvitamise eest eriliste nuhkprogrammide abil (nuhkvara ja nn veebilutikad) või muul viisil. Samuti tuleb asuda tõhusalt tõkestama rämpsposti ([29]) (laiaulatuslik soovimatute sõnumite saatmine), mis nende kuritarvitustega sageli kaasneb. Seesugused sekkumised kahjustavad asjaomaseid isikuid ([30]).

4.7 *Tugevam ja aktiivsem ELi amet*

4.7.1 Euroopa Majandus- ja Sotsiaalkomitee toetab Euroopa Võrgu- ja Infoturbeameti (ENISA) ulatuslikumat ja tõhusamat osalemist teadlikkuse suurendamise meetme võtmisel, aga samuti ja eelkõige operaatorite ja kasutajate teavitamise ja koolitamise meetmete puhul, nagu rõhutati juba komitee hiljuti esitatud arvamuses ([31]) üldkasutatavate elektrooniliste sideteenuste osutamise kohta.

4.7.2 Iga asjahuviliste ringkondade rühma omavastutuse suurendamise meetmete osas on siinkohal ilmselt rangelt kinni peetud subsidiaarsuse põhimõttest. Nimetatud meetmete teostamine vastavalt eripädevustele on tõepoolest liikmesriikide ja erasektori ülesanne.

4.7.3 ENISA peaks saama Euroopa võrgu- ja teabeturbevõrgustikult abi, et korraldada ühist tegevust; samuti peaks ENISA kasutama ELi mitmekeelset ohtudest teavitavat veebiportaali selleks, et edastada igas vanuses erakasutajatele ja VKEdele arusaadavas sõnastuses personaliseeritud ja interaktiivset teavet.

Brüssel, 16. veebruar 2007

Euroopa Majandus- ja Sotsiaalkomitee
president
Dimitris DIMITRIADIS

([29]) Pr k pollupostage.

([30]) Vt arvamusi "Elektroonilise side võrgud" (EÜT C 123, 25.4.2001, lk 50), "E-kaubandus" (EÜT C 169, 16.6.1999, lk 36) ja "E-kaubanduse mõju ühtsele turule" (EÜT C 123, 25.4.2001, lk 1).

([31]) Joonealune märkus 19, esimene taane.