Eiropas Ekonomikas un sociālo lietu komitejas Atzinums par tematu "Komisijas paziņojums Padomei, Eiropas Parlamentam, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai — Drošas informācijas sabiedrības stratēģija — Dialogs, partnerība un atbildības apzināšanās"

COM(2006) 251 galīgā redakcija

(2007/C 97/09)

Komisija saskaņā ar Eiropas Kopienas dibināšanas līguma 262. pantu 2006. gada 31. maijā nolēma konsultēties ar Eiropas Ekonomikas un sociālo lietu komiteju par augstāk minēto tematu.

Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa, kas bija atbildīga par Komitejas dokumenta sagatavošanu minētajā jautājumā, 2007. gada 11. janvārī pieņēma atzinumu, pamatojoties uz ziņotāja *PEZZINI* kga sagatavoto projektu.

Eiropas Ekonomikas un sociālo lietu komiteja 433. plenārajā sesijā, kas notika 2007. gada 15. un 16. februārī (16. februāra sēdē), ar 132 balsīm par, un 2 atturoties, pieņēma šādu atzinumu.

1. **Secinājumi un ieteikumi**

1.1 Komiteja ir pārliecināta, ka informācijas drošības problēma izraisa arvien lielākas bažas uzņēmumiem, pārvaldēm, publiskā un privātā sektora struktūrām un katram atsevišķam iedzīvotājam.

1.2 Kopumā Komiteja piekrīt analīzēm un argumentiem, ar ko pieprasa jaunu stratēģiju ar nolūku paaugstināt tīklu un informācijas drošību pret uzbrukumiem un ielaušanos, kas neņem vērā ģeogrāfiskās robežas.

1.3 Komiteja uzskata, ka, ņemot vērā minētās parādības apjomu un tās sekas ekonomikas nozarē un privātajā dzīvē, Komisijai būtu jāveic papildu pasākumi, lai īstenotu novatorisku un daudzveidīgu stratēģiju.

1.3.1. Komiteja arī uzsver, ka nesen Komisija izstrādāja jaunu paziņojumu par informācijas drošību un ka drīzumā vajadzētu būt gatavam jaunam dokumentam par šo pašu jautājumu. Komiteja patur tiesības nākotnē izstrādāt sīkāk izstrādātu atzinumu, kas ņemtu vērā visus paziņojumus.

1.4 Komiteja uzsver, ka informācijas drošības aspekts nekādā gadījumā nevar būt nodalīts no personas datu aizsargāšanas nostiprināšanas un no brīvību aizsardzības, kuras garantē Eiropas Cilvēktiesību konvencija.

1.5 EESK rodas jautājums, kāda šobrīd ir priekšlikuma pievienotā vērtība salīdzinājumā ar 2001. gadā pieņemto integrēto pieeju, kuras mērķis ir vienāds ar šajā paziņojumā norādīto mērķi ([1]).

1.5.1. Priekšlikumam pievienotais "Ietekmes novērtējuma" ([2]) dokuments satur dažus interesantus labojumus, salīdzinot ar 2001. gada nostāju, bet tas tika nopublicēts tikai vienā valodā, un līdz ar to nav pieejams daudziem Eiropas pilsoņiem, kas izdara savus secinājumus par visās Kopienas valodās pieejamo oficiālo dokumentu.

1.6 Komiteja norāda uz 2005. gadā Tunisijā notikušā pasaules sammita par informācijas sabiedrību secinājumiem, kurus 2006. gada 27. martā parakstīja ANO Asambleja:

— nediskriminējošas piekļuves principi;

— IKT kā miera stiprināšanas instrumenta veicināšana;

— instrumenti, lai stiprinātu demokrātiju, kohēziju un labu pārvaldību;

— nelikumību novēršana cilvēktiesību ievērošanā ([3]).

1.7 Komiteja uzsver, ka dinamiskai un integrētai Kopienas stratēģijai papildus dialogam, partnerībai un atbildības apziņai vajadzētu īstenot:

— profilakses pasākumus;

— pāreju no drošības uz informācijas apdrošināšanu ([4]);

— droša un atzīta ES tiesiski regulējošā un sankciju piemērošanas pamata izveidi;

— tehniskās standartizācijas nostiprināšanu;

([1]) Skat. EESK atzinumu par tematu "Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai Tīklu un informācijas drošība — priekšlikums Eiropas politikas pieejai", OV C 48, 21.2.2002, 33. lpp.

([2]) "Ietekmes novērtējuma dokumentam" nav tāda pati nozīme, kāda ir "Stratēģijas dokumentam".

([3]) ANO 27.03.2006, Ieteikumi Nr. 57 un 58. *Tunis Final Document* nº 15.

([4]) Skat. "*Emerging technologies in the context of security*", KPC (Kopīgais pētniecības centrs) — Institūts iedzīvotāju aizsardzībai un drošībai, stratēģisku pētījumu žurnāls, 2005. gada septembris, Eiropas Komisija, http://serac.jrc.it.

— lietotāju digitālā identifikācija;

— Eiropas analīžu un prognožu (*Foresight*) par informācijas drošību īstenošanas uzsākšanu multimodālas tehniskas konverģences apstākļos;

— Eiropas un valstu risku novērtēšanas mehānismu nostiprināšanu;

— pasākumus, kas vērsti uz informātikas monokultūru rašanās novēršanu;

— Kopienas koordinācijas pastiprināšanu Eiropas un starptautiskajā mērogā;

— *ICT Security Focal Point* izveidošanu starp ģenerāldirektorātiem;

— Eiropas tīkla (*European Network*) un Informācijas drošības tīkla (*Information Security Network*) izveidošanu;

— Eiropas pētījumu par informācijas drošību nozīmes palielināšanu;

— Eiropas dienas "Drošais dators" iedibināšanu;

— Kopienas izmēģinājuma pasākumus dažāda veida un līmeņa skolās par informācijas drošību.

1.8 Visbeidzot EESK uzskata, ka nolūkā nodrošināt dinamisku un integrētu Kopienas stratēģiju jāparedz atbilstošs budžeta finansējums, nostiprinot Kopienas mēroga iniciatīvas un saskaņošanas pasākumus, kas spētu vienoti pārstāvēt Eiropu pasaulē.

2. **Pamatojumi**

2.1 Informācijas sabiedrības drošībai ir būtiska nozīme, lai nodrošinātu uzticēšanos un uzticamību tīkliem un komunikāciju pakalpojumiem, kas ir ekonomikas un sabiedrības attīstības izšķirošie faktori.

2.2 Tīkliem un informācijas sistēmām jābūt aizsargātiem, lai tie saglabātu konkurences un uzņēmējdarbības spējas, nodrošinātu elektronisko sakaru integritāti un nepārtrauktību, novērstu krāpšanu un nodrošinātu privātās dzīves aizsardzību ar likumu.

2.3 2004. gadā aptuveni 90 % Eiropas uzņēmumu aktīvi izmantoja internetu un 65 % no tiem izveidoja savu tīmekļa vietni; tiek lēsts, ka aptuveni puse no Eiropas iedzīvotājiem regulāri izmanto internetu un 25 % mājsaimniecību pastāvīgi izmanto platjoslas pieslēgumu ([5]).

([5]) *i2010:Drošas informācijas sabiedrības stratēģija.* Informācijas sabiedrības un plašsaziņas līdzekļu ģenerāldirektorāts — Factsheet 8 (2006. gada jūnijā), EK Informācijas sabiedrība un plašsaziņas līdzekļi http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

2.4 Kaut arī investīciju apjoms pieaug, tikai 5-13 % no kopējiem informāciju tehnoloģijās ieguldītajiem līdzekļiem tiek tērēti drošības risinājumiem. Tas nav pietiekami. Nesen veiktos pētījumos konstatēts, ka no aptuveni 30 protokoliem, kuru galvenās struktūras ir līdzīgas, 23 protokoli ir neaizsargāti pret vairākiem protokoliem paredzētiem uzbrukumiem ([6]). Turklāt katru dienu nosūta vidēji 25 miljoni mēstuļu (*spam*) ([7]), un tapēc Komiteja izsaka gandarījumu par šajā sakarā nesen iesniegto Komisijas priekšlikumu.

2.5 Attiecībā uz datorvīrusiem ([8]), līdz ar elektronisko komunikācijas tīklu un sistēmu arvien straujāko attīstību ir savairojušies tārpi (*worms*) ([9]) un spiegprogrammatūra (*spyware*) ([10]) minētie tīkli un sistēmas kļūst arvien sarežģītākas un vienlaikus arī neaizsargātākas — viens no šā trūkuma iemesliem ir multivides, mobilās telefonijas un režģiskās skaitļošanas (*GRID infoware*) ([11]) programmu konverģence, un šo tīklu un sistēmu vājās vietas ir iespēja izspiest naudu, piedraudot ar pakalpojumatteices uzbrukumu (*DDoS extortion*), identifikācijas datu zādzības tīmeklī, pikšķerēšana (*phishing*) ([12]), pirātisms ([13]) utt., šīs informācijas sabiedrībai piemītošās drošības problēmas Eiropas Kopiena ir apspriedusi 2001. gadā ([14]) publicētā paziņojumā. EESK ir sniegusi komentārus ([15]) par minēto paziņojumu un norādījusi trīs galvenās rīcības jomas:

— īpaši drošības pasākumi,

([6]) Ziņojumi pirmajā starptautiskajā konferencē par pieejamību, uzticamību un drošību (ARES'06) — sējums 00 ARES 2006, izdevējs IEEE Computer Society.

([7]) SPAM — nelūgta komerciāla elektroniskā vēstule. Vārda "spam" ("mēstule") sākotnējā nozīme ir "cūkgaļa un šķiņķis ar garšvielām" ("spiced pork and ham"), tā sauca gaļas konservus, ko daudz lietoja 2. pasaules kara laikā, kad tie kļuva par ASV armijas un Apvienotās Karalistes iedzīvotāju galveno pārtiku. Tā kā šos konservus ēda gadiem (tie netika normēti), iedzīvotājiem tie beigās bija apnikuši.

([8]) Datorvīruss: īpaša programmatūra, kas pieder pie ļaunprātīgu programmatūru kategorijas, kura, ja tiek palaista, spēj, sevi pavairojot, inficēt datnes, parasti bez lietotāja ziņas. Vīrusi var būt vairāk vai mazāk kaitīgi operētājsistēmai, kurā ir iekļuvuši, bet pat labākajā gadījumā tie izraisa zināmu brīvpiekļuves atmiņas (*RAM*), centrālā procesora (*CPU*) un vietas uz cietā diska izšķiešanu.

([9]) e-pasta tārps ir destruktīva programma, kas uzbrūk tīklam, tā savāc e-pasta adreses no klienta e-pasta programmas (piemēram, *MS Outlook*) un pēc tam izsūta simtiem e-pasta vēstuļu uz šīm e-pasta adresēm, turklāt pati tārpa programma ir pievienota šīm vēstulēm kā piesaistne (*attachment*).

([10]) Spiegprogrammatūra (*spyware*) = programma, kas slepeni vāc informāciju par lietotāja darbībām internetā, tā instalē pati sevi, par to neinformējot lietotāju un lietotājam par to nezinot, proti, bez lietotāja piekrišanas un kontroles.

([11]) Režģiskās skaitļošanas programmas (*GRID infoware*) = dara iespējamu ļoti dažādu plašā ģeogrāfiskā areālā izkaisītu datorresursu (piemēram, superdatoru, klasteru, datu glabāšanas sistēmu, datu avotu, instrumentu, cilvēku) koplietošanu, atlasi un vienlaicīgu izmantošanu, tos virtuāli apkopojot kā vienu un nedalāmu resursu, lai skaitļošanas jomā risinātu sarežģītas problēmas un tādus uzdevumus, kuru risināšanai jāapstrādā daudz datu.

([12]) Pikšķerēšana (*phishing*) = informācijas tehnoloģiju jomā tā sauc krāpšanas metodi, kuras mērķis ir izvilināt personu apliecinošus un konfidenciālus datus, proti, identifikācijas datu zādzību, ko veic, nosūtot viltotas e-pasta vēstules, kas izskatās gluži kā īstas.

([13]) Pirātisms = programmatūras "pirātu" lietots vārds, ar ko apzīmē programmatūru, kuras aizsardzība pret kopēšanu ir uzlauzta un ko iespējams lejupielādēt tīmeklī.

([14]) COM(2001) 298 galīgā redakcija.

([15]) Skat. 1. zemsvītras piezīmi.

— tiesiskais regulējums, tostarp arī attiecībā uz datu un privātuma aizsardzību,

— kibernoziedzības apkarošana.

2.6 Informātikas uzbrukumu atklāšana, identificēšana un novēršana tīklā ir problēma, kam jāmeklē atbilstoši risinājumi, ņemot vērā pastāvīgas konfigurācijas izmaiņas, piedāvāto un attīstīto IP un pakalpojumu daudzveidību, asinhrono uzbrukuma veidu ārkārtīgo sarežģītību ([16]).

2.7 Diemžēl drošības jomā ieguldīto investīciju atdeves nepārredzamība un nepietiekama lietotāju atbildības apzināšanās ir iemesli, kādēļ riski netiek pienācīgi novērtēti un drošības kultūras attīstībai netiek pievērsta pienācīga uzmanība.

3. **Komisijas priekšlikums**

3.1 Ar "Paziņojumu par Drošas informācijas sabiedrības stratēģiju" ([17]). Komisija vēlas uzlabot informācijas drošību, izstrādājot dinamisku, integrētu stratēģiju, kas balstās uz:

a) dialoga sekmēšanu starp publiskās pārvaldes iestādēm un Komisiju, veicot valstu politiku salīdzinošo novērtēšanu (*benchmarking*) un i-pārvaldības drošos apstākļos paraugprakšu (*best practices*) noteikšanu;

b) iedzīvotāju un MVU lielāku ieinteresēšanu par efektīvām drošības sistēmām, pateicoties Komisijas veicinošai lomai un lielākai Eiropas tīklu un informācijas drošības aģentūras (*AESRI/ENISA*) dalībai;

c) dialogu par instrumentiem un noteikumiem, lai panāktu līdzsvaru starp drošību un pamattiesībām, ietverot privātās dzīves aizsardzību.

3.2 Turklāt Komisijas paziņojumā ir paredzēta Eiropas tīklu un informācijas drošības aģentūras uz uzticēšanos balstīta partnerība ar pienācīgu datu apkopošanas sistēmu par drošības pārkāpumiem, lietotāju uzticēšanās līmeni un drošības rūpniecības attīstību. Šī partnerība notiktu:

a) ar dalībvalstīm;

b) ar patērētājiem un lietotājiem;

c) ar informācijas drošības rūpniecību;

d) ar privāto sektoru,

izveidojot ES daudzvalodu informācijas un risku brīdināšanas portālu, lai norisinātos stratēģiska partnerība starp privāto sektoru, dalībvalstīm un pētniekiem.

3.2.1 Turklāt paziņojumā ir paredzēta lielāka ieinteresēto personu atbildība par vajadzībām un riskiem drošības jomā.

3.2.2 Attiecībā uz starptautisko sadarbību un sadarbību ar trešām valstīm "tīklu un informācijas drošības jautājumu visaptverošā dimensija uzliek Komisijai pienākumu gan starptautiskā līmenī, gan sadarbībā ar dalībvalstīm pastiprināt tās centienus sekmēt visaptverošu sadarbību tīklu un informācijas drošības jautājumos" ([18]), bet šāds norādījums netiek atkārtots punktos par dialogu, partnerību un atbildības apzināšanos.

4. **Piezīmes**

4.1 Komiteja piekrīt analīzēm un argumentiem, kas pamato Eiropas integrētu un dinamisku tīklu un informācijas drošības stratēģiju, uzskatot drošības jautājumu par būtisku, lai veicinātu labvēlīgāku attieksmi pret IT pielietošanu un palielinātu uzticēšanos tām. EESK nostāja ir uzsvērta vairākos atzinumos ([19]).

4.1.1 Komiteja vēlreiz uzsver ([20]), ka "Interneta tīkls un jaunās tehnoloģijas komunikācijām tiešsaistes režīmā (kā piemēram mobilie telefoni, kabatas plānotāji ar multimediju funkcijām un kas pieslēdzami internetam, kuru lietošana pašreiz ļoti izplatās) ir būtiski instrumenti zināšanu ekonomikas, e-ekonomikas un e-administrācijas attīstībai".

([16]) *Multivariate Statistical Analysis for Network Attacks Detection. Guangzhi Qu, Salim Hariri* — 2005 US, 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]) COM(2006) 251 galīgā redakcija, 31.05.2006.

([18]) Skat. COM 251/2006, 3. nod. priekšpēdējā rindkopa.

([19]) Skat. šādus dokumentus:
- EESK atzinums par tematu "Priekšlikumu Eiropas Parlamenta un Padomes Direktīvai par tādu datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu, ar ko labo Direktīvu 2002/58/EK", — OV C 69, 21.3.2006, 16. lpp.;
- EESK atzinums par tematu "Komisijas paziņojums Padomei, Eiropas Parlamentam, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "i2010 — Eiropas informācijas sabiedrība izaugsmei un nodarbinātībai"" — OV C 110, 9.5.2006, 83. lpp.;
- EESK atzinums par tematu "Priekšlikumu Eiropas Parlamenta un Padomes lēmumam, kas ievieš daudzgadīgu Kopienas programmu ar mērķi veicināt drošāku interneta un jauno tehnoloģiju lietošanu tiešsaistes režīmā" — OV C 157, 28.6.2005, 136. lpp.;
- EESK atzinums par tematu "Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai Tīklu un informācijas drošība — priekšlikums Eiropas politikas pieejai" — OV C 48, 21.2.2002, 33. lpp.;

([20]) Skatīt 19. zemsvītras piezīmes 3. ievilkumu.

4.2 *Stingrāki Komisijas priekšlikumi*

4.2.1 Tomēr Komiteja uzskata, ka Komisijas piedāvāto pieeju, kas balsta šo integrēto un dinamisko stratēģiju uz atvērtu un visaptverošu dialogu, kā arī partnerību un pastiprinātu atbildības apzināšanos starp visām ieinteresētajām pusēm, bet sevišķi ar lietotājiem, var tālāk paplašināt.

4.2.2 Minētā nostāja tika uzsvērta Komitejas iepriekšējos atzinumos: "Šai cīņai, lai tā būtu efektīva, tāpat ir tieši jāattiecas uz visiem interneta lietotājiem, kuriem ir jābūt apmācītiem un informētiem par veicamajiem piesardzības pasākumiem un lietojamajiem līdzekļiem, lai nodrošinātos pret bīstamu vai nevēlamu elementu saņemšanu vai lai viņi netiktu izmantoti par starpniekiem šādu elementu sūtīšanā. Komiteja uzskata, ka rīcības plāna informācijas un apmācības daļā galvenā prioritāte ir jāpiešķir lietotāju līdzdalībai." ([21])

4.2.3 Komiteja uzskata, ka lietotāju un iedzīvotāju līdzdalībai jānotiek tādā veidā, lai saskaņotu nepieciešamo informācijas un tīklu aizsardzību ar pilsoņu brīvībām un lietotāju tiesībām uz drošu pieslēgumu par mērenu maksu.

4.2.4 Ir jāuzskata, ka informācijas drošības pētīšana veido izmaksas patērētājam arī laika nozīmē, kas tiek patērēts, lai novērstu vai pārvarētu šķēršļus. Komiteja uzskata, ka vajadzētu noteikt obligātu pretvīrusu aizsardzības sistēmu automātisku abonēšanu katram datoram, kuras lietotājs var iedarbināt vai nē, bet kuras ir iekļautas precē jau no paša sākuma.

4.3 *Dinamiskāka un novatoriskāka Kopienas stratēģija*

4.3.1 Turklāt Komiteja uzskata, ka ES vajadzētu izvirzīt tālejošākus mērķus un radīt novatorisku, integrētu un dinamisku stratēģiju ar jaunām iniciatīvām, kā, piemēram:

— mehānismi, kas ļauj digitāli identificēt atsevišķus lietotājus, kuriem pārāk bieži jāievada savi personas dati;

— pasākumi ar ETSI starpniecību ([22]), kas būtu priekšnoteikums IKT drošai izmantošanai, kas var piedāvāt detalizētus un ātrus risinājumus ar noteiktu kopīgu drošības līmeni visā Eiropas Savienībā;

— profilakses pasākumi ar minimālo drošības priekšnoteikumu integrāciju informācijas un tīklu sistēmās un izmēģinājuma pasākumu uzsākšana, ieviešot drošības nodarbības visu veidu un līmeņu skolās;

— Eiropas līmenī droša un atzīta tiesiski regulējošā pamata izveidošana. Šāds pamats, piemērojot to informācijas tehnoloģijām un tīkliem, ļautu veikt pāreju no informācijas drošības uz informācijas apdrošināšanu;

— Eiropas un valstu risku novērtēšanas mehānismu nostiprināšana un lielāka tiesību aktu un noteikumu piemērošanas spēja, lai vērstos pret kibernoziegumiem, kas tiek izdarīti pret privātās dzīves neaizskaramību un datu arhīviem;

— pasākumi, lai izvairītos no informātikas monokultūru rašanās ar tādiem produktiem un risinājumiem, kurus ir daudz vieglāk nelegāli pavairot. Atbalsts daudzveidīgiem daudzkultūru jauninājumiem, kas vērsti uz Vienotas Eiropas informācijas telpas izveidi (*SEIS, Single European Information Space*).

4.3.2 Komiteja uzskata, ka būtu lietderīgi izveidot IKT drošības kontaktpunktu *(ICT Security Focal Point)* starp ģenerāldirektorātiem ([23]). Tas ļautu rīkoties:

— Komisijas iekšējo dienestu līmenī;

— atsevišķu dalībvalstu līmenī, izstrādājot horizontālus risinājumus attiecībā uz sadarbspēju, identifikācijas pārvaldību, privātās dzīves aizsardzību, brīvu piekļuvi informācijai un pakalpojumiem un attiecībā uz minimālo drošības priekšnoteikumu aspektiem;

— starptautiskajā līmenī, lai dažādās situācijās varētu nodrošināt vienotu Eiropas nostāju, kā, piemēram, ANO, G8, ESAO, *ISO*.

4.4 *Pastiprinātas ES koordinācijas darbības*

4.4.1 ESSK piešķir lielu nozīmi Eiropas tīkla (*European Network*) un Informācijas drošības tīkla (*Infomation Security Network*) izveidošanai, ar kura starpniecību varēs veicināt aptaujas, pētījumus un semināru par drošības mehānismiem un to sadarbspēju, par modernu kriptogrāfiju un privātās dzīves aizsardzību.

4.4.2 EESK uzskata, ka šajā ļoti delikātajā jomā jāpalielina Eiropas pētniecības nozīme, lietderīgi sintezējot:

— Eiropas drošības pētniecības programmas (*ESRP*) ([24]), kas iekļauta Septītajā pamatprogrammā zinātniskās pētniecības, tehnoloģiskās attīstības un demonstrācijas pasākumu jomā,

([21]) Skatīt 19. zemsvītras piezīmes 3. ievilkumu.

([22]) ETSI, Eiropas Telekomunikāciju standartu institūts. Skat. īpaši 2006. gada 16. un 17. janvāra semināru. ETSI cita starpā izstrādāja specifikāciju nelegālai pārtveršanai (TS 102 232; 102 233; 102 234), internata piekļuvēm *Lan Wireless* (TR 102 519), elektroniskiem parakstiem un izstrādāja *GSM GPRS* un *UMTS* drošības algoritmus.

([23]) Šādus *Security Focal Point* starp ģenerāldirektorātiem varētu finansēt Septītās zinātniskās pētniecības, tehnoloģiskās attīstības un demonstrācijas pasākumu pamatprogrammas īpašas programmas "Sadarbība" IST prioritātes vai Eiropas drošības pētniecības programmas (*ESRP*) ietvaros.

([24]) Skat. 7. pamatprogramma — EK PAT&D pamatprogramma, īpaša programma "Sadarbība"; tematiskā prioritāte "Drošības pētniecība" ar budžetu 1,35 miljardi eiro laika posmam no 2007. līdz 2013. gadam.

— programmas *Safer Internet Plus*;

— un Eiropas programmas svarīgāko infrastruktūras objektu aizsardzībai (*EPCIP*) saturu ([25]).

4.4.3 Šiem ieteikumiem varētu pievienot Eiropas dienas "Drošais dators" iedibināšanu, kuru atbalstītu ar valstu izglītības kampaņām skolās un informatīvās kampaņām patērētājiem par informācijas aizsardzības procedūrām ar personālā datora starpniecību. Protams, šī informācija tiktu sniegta papildus informācijai par reģistrētiem tehnoloģiskiem sasniegumiem plašajā un mainīgajā izgudrojumu jomā.

4.4.4 Komiteja ir vairākkārtīgi uzsvērusi, ka "Viedoklis par digitālo darījumu drošību un uzticēšanās šo darījumu drošībai ietekmē to, cik ātri uzņēmumi savā darbībā sāks izmantot IKT. Patērētāju vēlmi norādīt kredītkartes numuru tīmekļa vietnē ievērojami ietekmē patērētāja viedoklis par attiecīgā darījuma drošību." ([26]).

4.4.5 Komiteja ir pārliecināta, ka, ņemot vērā nozares milzīgo izaugsmes potenciālu, ir jāveicina īpašas politikas jomas un jāpiemēro esošās jaunajiem sasniegumiem. Drošības, informātikas jomā Eiropas mēroga iniciatīvas ir jāsasaista ar integrētu stratēģiju, paplašinot nozares robežas un nodrošinot saskaņotu un drošu IKT izmantošanu sabiedrībā.

4.4.6 Komiteja uzskata, ka atsevišķu nozīmīgu stratēģiju, kā šīs, izstrāde virzās pārāk lēni birokrātisko un kultūras šķēršļu dēļ, ko dalībvalstis liek nepieciešamajiem lēmumiem, kuri jāpieņem Kopienas mērogā.

4.4.7 Komiteja arī uzskata, ka Kopienas resursi ir nepietiekami, lai īstenotu daudzus un steidzamus projektus, kuri var sniegt konkrētus risinājumus jaunām ar globalizāciju saistītām problēmām, ja tie tiek īstenoti Kopienas mērogā.

4.5 *Patērētāja aizsardzības lielāka drošība ES*

4.5.1 Komiteja apzinās, ka dalībvalstis ir īstenojušas tehnoloģiskus drošības pasākumus un drošības pārvaldes procedūras saskaņā ar pašu vajadzībām, cenšoties koncentrēties uz dažādiem aspektiem. Arī šī iemesla dēļ ir grūti sniegt viennozīmīgu, efektīvu atbildi uz drošības problēmām. Izņemot dažus administratīvus tīklus, starp dalībvalstīm nepastāv sistemātiska pārrobežu sadarbība, kaut arī katra valsts atsevišķi nevar risināt drošības jautājumus.

4.5.2 Turklāt Komiteja uzskata, ka ar Padomes Lēmumu 2005/222/GIA tika izveidots tiesu un citu kompetento iestāžu sadarbības pamats, lai, tuvinot to krimināltiesības uzbrukumu pret informācijas sistēmām jomā, nodrošinātu dalībvalstu vienotu pieeju attiecībā uz:

— nelikumīgu piekļuvi informācijas sistēmām;

— pretlikumīgiem traucējumiem, kuri tīši izraisa nopietnus informācijas sistēmas darbības traucējumus vai pārtraukumu;

— nelikumīgiem traucējumiem, kas skar tīšu informācijas sistēmas datu dzēšanu, postīšanu, bojāšanu, sagrozīšanu, likvidēšanu vai padara tos nepieejamus;

— kūdīšanu, palīdzības sniegšanu, līdzdalību iepriekš minētajos pārkāpumos.

4.5.3 Turklāt ietvarlēmumā ir norādīti kritēriji juridisku personu atbildības noteikšanai un iespējamās sankcijas, kas var tikt piemērotas, kad to atbildība ir pierādīta.

4.5.4 Dialogā ar dalībvalstu publiskās pārvaldes iestādēm Komiteja atbalsta Komisijas priekšlikumu, ka minētajām iestādēm jāuzsāk darbības, lai veiktu salīdzinošo novērtēšanu savu valstu politikai attiecībā uz tīklu un informācijas sistēmu drošību, ietverot īpašās politikas, kas skar publisko sektoru. Šāds ierosinājums bija ietverts EESK 2001. gada atzinumā ([27]).

4.6 *Izplatītāka drošības kultūra*

4.6.1 Attiecībā uz informācijas drošības rūpniecības līdzdalību, tai jānodrošina efektīvas garantijas, lai aizsargātu klientu tiesības uz privāto dzīvi un konfidencialitāti, izmantojot savu iekārtu materiālajai uzraudzībai un komunikāciju kodifikācijai instrumentus, kas atbilst jaunākajai tehnoloģiju attīstībai ([28]).

([25]) COM(2005) 576, 17.11.2005.
([26]) Skatīt 19. zemsvītras piezīmes 2. ievilkumu.
([27]) Skat. atzinumu CESE 1474/2001., 28.11.2001., ziņotājs — *RETUREAU* kgs.
([28]) Skat. Direktīvu 97/66/EK par personas datu apstrādi telekomunikāciju nozarē (OV L 24, 30.1.1998.).

4.6.2 Attiecībā uz informētības uzlabošanas darbību Komiteja uzskata, ka ir svarīgi izveidot īstu "drošības kultūru", kas būtu pilnībā savienojama ar informācijas, komunikācijas un vārda brīvību. Daudzi lietotāji neapzinās visus ar datorpirātismu saistītus riskus, savukārt daudzi pakalpojumu operatori, pārdevēji vai sniedzēji nespēj novērtēt nepietiekamo aspektu esamību un apjomu.

4.6.3 Kaut arī privātās dzīves un personīgo datu aizsardzība ir prioritārie mērķi, patērētājiem ir arī tiesības uz efektīvu aizsardzību pret spiegošanu, izmantojot spiegprogrammatūras un datnes (*spyware* un *web bugs*) vai citas metodes. Ir vajadzīgi arī efektīvi pasākumi, lai novērstu surogātpasta (*spamming*) ([29]) praksi (masveidīga nepieprasītu paziņojumu nosūtīšana), kas bieži vien izriet no šīm nelikumībām. Šāda veida ielaušanās nodara kaitējumu tās upuriem ([30]).

4.7 *Spēcīgāka un aktīvāka ES Aģentūra*

4.7.1 Komiteja piekrīt, ka Eiropas tīklu un informācijas drošības aģentūrai (*ENISA*) konkrēti un pastiprināti jādarbojas gan saistībā ar informētības uzlabošanas kampaņām, gan jo sevišķi sakarā ar operatoru un lietotāju informēšanas un apmācības darbībām, kā EESK jau ieteica nesen pieņemtajā atzinumā ([31]) par publisko elektronisko sakaru pakalpojumu sniegšanu.

4.7.2 Visbeidzot, attiecībā uz piedāvātajām darbībām, lai palielinātu katras ieinteresēto personu grupas atbildības apzināšanos, tās šķiet vērstas uz subsidiaritātes principa stingru ievērošanu. Tās tiešām ir jāīsteno dalībvalstīm un privātajam sektoram saskaņā ar to īpašajām atbildības jomām.

4.7.3 Eiropas tīklu un informācijas drošības aģentūrai (*ENISA*) vajadzētu izmantot Eiropas tīkla *European Network and Information Security Network* palīdzību, lai organizētu kopīgus pasākumus, kā, piemēram, Kopienas informācijas drošības trauksmes daudzvalodu portālu individualizētai un interaktīvai informācijai saprotamā valodā, īpaši individuāliem visdažādākā vecuma lietotājiem un mazajiem un vidējiem uzņēmumiem.

Briselē, 2007. gada 16. februārī.

Eiropas Ekonomikas un sociālo lietu komitejas
priekšsēdētājs
Dimitris DIMITRIADIS

([29]) Franciski "*pollu postage*".

([30]) Skat. EESK atzinumus par tematiem: "*Elektronisko sakaru tīkli*" (OV C 123, 25.4.2001., 50. lpp.), "*Elektroniskā tirdzniecība*" (OV C 169, 16.6.1999., 36. lpp.) un "*Elektroniskās tirdzniecības ietekme uz vienoto tirgu*" (OV C 123, 25.4.2001., 1. lpp.).

([31]) Skatīt 19. zemsvītras piezīmes 1. ievilkumu.