Europos ekonomikos ir socialinių reikalų komiteto nuomonė dėl Komisijos komunikato Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl saugios informacinės visuomenės strategijos — Dialogas, partnerystė ir teisių suteikimas

COM(2006) 251 final

(2007/C 97/09)

Europos Komisija, vadovaudamasi Europos bendrijos steigimo sutarties 262 straipsniu, 2006 m. gegužės 31 d. nusprendė pasikonsultuoti su Europos ekonomikos ir socialinių reikalų komitetu dėl *Komisijos komunikato Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl saugios informacinės visuomenės strategijos — Dialogas, partnerystė ir teisių suteikimas*

Transporto, energetikos, infrastruktūros ir informacinės visuomenės skyrius, kuris buvo atsakingas už Komiteto darbo šiuo klausimu organizavimą, 2007 m. sausio 11 d. priėmė savo nuomonę. Pranešėjas Antonello Pezzini.

433-iojoje plenarinėje sesijoje, įvykusioje 2007 m. vasario 16 d., Europos ekonomikos ir socialinių reikalų komitetas priėmė šią nuomonę 132 nariams balsavus už, nė vienam prieš ir 2 susilaikius.

1. **Išvados ir rekomendacijos**

1.1 Komitetas yra įsitikinęs, kad informacijos saugumas kelia vis didesnį rūpestį įmonėms, viešojo valdymo institucijoms, viešosioms ir privačioms organizacijoms ir pavieniams asmenims.

1.2 Komitetas iš esmės pritaria atliktų tyrimų rezultatams ir argumentams sukurti naują tinklų ir informacijos saugumo ir kovos su atakomis ir įsiskverbimu, kuriems nėra jokių geografinių ribų, strategiją.

1.3 Komitetas mano, kad, atsižvelgiant į šių reiškinių mastą ir į jų poveikį ekonomikai ir asmens privatumui, Komisija turėtų dėti daugiau pastangų pažangiai ir suderintai strategijai įgyvendinti.

1.3.1 Komitetas tai pat atkreipia dėmesį, kad Komisija neseniai priėmė naują komunikatą dėl informacijos saugumo ir artimiausiu metu pateiks kitą dokumentą šiuo klausimu. Komitetas mano galėsiantis pateikti išsamesnę nuomonę, kurioje bus atsižvelgta į visus šiuo klausimu pateiktus komunikatus.

1.4 Komitetas ypač pabrėžia, kad informacijos saugumas negali būti atsiejamas nuo asmens duomenų apsaugos stiprinimo ir pagrindinių laisvių, kurias užtikrina Europos žmogaus teisių konvencija.

1.5 Komitetas, atsižvelgdamas į dabartinę padėtį, kelia klausimą, kokia papildomą naudą teikia pasiūlymas palyginti su 2001 m. patvirtintu integruotu ES požiūriu, kuriuo buvo siekiama panašių tikslų kaip ir čia nagrinėjamame komunikate ([1]).

1.5.1 Poveikio analizės ataskaitoje ([2]), kuri buvo pateikta pasiūlymo priede, siūloma 2001 m. priimtą dokumentą papildyti keletu įdomių požiūrių. Kadangi dokumentas buvo paskelbtas tik viena kalba, jo perskaityti negalėjo daugelis Europos piliečių, kurie savo nuomonę formuoja remdamiesi oficialiu įvairiomis Bendrijos kalbomis paskelbtu dokumentu.

1.6 Komitetas primena pagrindines 2005 m. Tunise vykusio aukščiausio lygio susitikimo dėl informacinės visuomenės išvadas, kurios buvo patvirtintos 2006 m. kovo 27 d. vykusioje JT asamblėjoje:

— suteikti lygias galimybes naudotis informacija;

— skatinti naudoti IRT taikiems tikslams;

— įgyvendinti priemones demokratijai, sanglaudai ir geram valdymui stiprinti;

— užkirsti kelią žmogaus teisių pažeidimams ([3]).

1.7 Komitetas pritaria, kad Bendrijos dinamiškoje ir integruotoje strategijoje greta dialogo, partnerystės ir atsakomybės būtų numatyta:

— prevencijos veiksmai;

— perėjimas nuo informacijos saugumo prie informacijos apdraudimo ([4]);

— sukurti patikimą ir pripažintą ES teisinę ir reguliavimo sistemą, kuri numatytų sankcijas;

— skatinti techninį standartizavimą;

([1]) EESRK nuomonė dėl *Komisijos komunikato Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl tinklų ir informacijos saugumo: Europos politinio požiūrio pasiūlymas* OL C 48, 2002 2 21, p. 33.

([2]) „Poveikio ataskaita“ neturi tos pačios reikšmės, kaip „strateginis dokumentas“.

([3]) JT, 2006 3 27, 57 ir 58 rekomendacijos. Nr. 15, galutinis dokumentas priimtas Tunise.

([4]) Žr. *Emerging technologies in the context of security, JRC (Europos Sąjungos Jungtinių mokslinių tyrimų centras)* — Piliečių gynimo ir saugumo institutas (IPSC), strateginiai tyrimai, 2005 m. spalio mėn., Europos Komisija, http://serac.jrc.it.

— skaitmeninė vartotojų atpažintis;

— atlikti informacijos saugumo Europos lygmens analizę ir perspektyvinius tyrimus atsižvelgiant į daugiafunkcinių technologijų konvergenciją;

— Europos ir nacionalinių rizikos vertinimo mechanizmų kūrimas;

— Priemonės, trukdančios informacinėms monokultūroms susidaryti;

— koordinavimo Bendrijoje — tiek ES, tiek nacionaliniu lygiu — stiprinimas;

— sukurti ryšių koordinavimo centrą „IRT saugumas“ (angl. *ICT Security Focal Point*), jungiantį daugelį generalinių direktoratų;

— sukurti Europos tinklų ir informacijos saugumo sistemą (angl. *European Network and Information Security Network*);

— naudotis visomis Europoje atliekamų tyrimų informacijos saugumo srityje galimybėmis;

— paskelbti „Europos informacijos saugumo dieną“;

— pradėti eksperimentinio pobūdžio informacijos saugumo akcijas visose įvairių lygių mokymo įstaigose.

1.8 Komitetas mano, kad siekiant sukurti dinamišką ir integruotą Bendrijos strategiją, būtina numatyti pakankamai lėšų iniciatyvoms ir veiksmams, kurių tikslas — sustiprinti koordinavimą Bendrijoje ir reikšti vieningą Europos poziciją pasaulyje.

2. **Pagrindimas**

2.1 Informacinės visuomenės saugumas — esminis iššūkis stiprinant pasitikėjimą tinklais ir elektroninių ryšių paslaugomis bei siekiant pastarųjų patikimumo, kadangi tai yra pagrindiniai ekonomikos ir socialinio vystimosi veiksniai.

2.2 Tinklai ir informacinės sistemos turi būti apsaugoti siekiant išsaugoti konkurencingumą ir komercinius gebėjimus, užtikrinti elektroninių ryšių vientisumą ir tęstinumą, užkirsti kelią sukčiavimui ir užtikrinti teisėtą privatumo apsaugą.

2.3 Elektroniniai ryšiai ir su jais susijusios paslaugos sudaro didžiausią telekomunikacijų sektoriaus dalį: 2004 m. apie 90 proc. Europos įmonių naudojosi interneto paslaugomis, o 65 proc. šių įmonių sukūrė savo interneto svetaines, tačiau statistika rodo, kad tik pusė Europos gyventojų nuolat naudojasi interneto paslaugomis ir tik 25 proc. šeimų nuolat naudojasi prieiga prie plačiajuosčio ryšio ([5]).

([5]) 2010 e. saugios informacinės visuomenės strategija — GD Informacinė visuomenė ir žiniasklaida, informacinis biuletenis Nr. 8 (2006 m. birželio mėn.) http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf.

2.4 Nepaisant to, kad investicijos sparčiai auga, išlaidos saugumui sudaro tik nuo 5 iki 13 proc. visų investicijų į informacinių technologijų plėtrą. Šie skaičiai yra labai maži. Neseniai atlikti tyrimai parodė, kad vidutiniškai iš 30 interneto protokolų (IP), naudojančių tas pačias pagrindines struktūras, 23 pažeidžiami, kai susiduria su kitų protokolų atakomis ([6]). Be to, suskaičiuojama, kad kasdien perduodama iki 25 milijonų nepageidaujamo elektroninio pašto laiškų (*spam*) ([7]). Komitetas palankiai vertina neseniai pateiktą Komisijos pasiūlymą, kuriame nagrinėjama ši problema.

2.5 Kalbant apie kompiuterių virusų problemą ([8]), reikėtų paminėti, kad sparčiai ir dideliu mastu plito „kompiuterių kirminai“ (*worms*) ([9]) ir „šnipukai“ (*spyware*) ([10]) kartu su nuolat besivystančiomis elektroninių ryšių sistemomis ir tinklais, kurie nuolat sudėtingėjo ir todėl tapo dar labiau pažeidžiami, visų pirma dėl įvairialypės įrangos, mobilaus ryšio ir GRID tinklų (*GRID infoware*) ([11]) konvergencijos. DDoS (*Distributed Denial of Service*) neteisėtos atakos, tapatybės vagystės internetu, duomenų vagystės (*phishing*) ([12]), piratavimas internete ([13]) ir kt. — informacinės visuomenės saugumo problemos, kurių sprendimus Europos Komisija stengėsi apibrėžti jau 2001 m. komunikate ([14]), dėl kurio Komitetui buvo suteikta galimybė pateikti nuomonę ([15]) ir pasiūlyti tris priemones:

— konkrečias saugumo priemones;

([6]) *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)* — Tomas 00 ARES 2006 m., leidėjas *IEEE Computer Society*.

([7]) *Spam* — nepageidaujamas elektroninis paštas. Pirmoji angliško trumpinio *spam* reikšmė buvo *spiced pork and ham* (kiauliena su prieskoniais ir kumpis), t.y., konservuota mėsa, kuri buvo plačiai vartojama Antrojo pasaulinio karo metais ir tapo pagrindiniu JAV karinių pajėgų ir Jungtinės Karalystės gyventojų produktu. Keletą metų vartojant šį produktą, kuris buvo platinamas be apribojimų, žodis *spam* žmonėms sukeldavo nemalonius pojūčius.

([8]) Kompiuteriu virusas — „kenkėjiška“ programinė įranga, kuria paleidus galima pakenti informacijos rinkmenoms ir juos nukopijuoti dažniausiai apie tai nežinant vartotojui, virusai gali daugiau ar mažiau pakenti kompiuterio operacinei sistemai ir net pačios mažiausios žalos atveju bus netinkamai išnaudota atmintinė (RAM, CPU), bei užimti vietą kietajame diske (www.wikipedia.org/wiki/Virus_informatique).

([9]) Kirminas — „kenkėjiška“ programinė įranga galinti kurti savo kopijas. Elektroninio pašto kirminas — trikdanti tinklo ataka, kurios metu nukopijuojami kliento elektroninio pašto dėžutėje esantys (pvz., *MS Outlook*) adresai, po to šiais adresais siunčiami šimtai elektroninių laiškų, kuriais platinama virusinė programa.

([10]) „Šnipukai“ — programinė įranga įrašanti vartotojo veiksmus ir instaliuojama automatiškai be vartotojo žinios, pritarimo ir kontrolės.

([11]) *GRID infoware* — suteikia galimybę naudotis, rūšiuoti, kaupti labai įvairius kompiuterių išteklius, pasklidusius po visą pasaulį (superkompiuteriai, blokiniai (*compute clusters*), atminties sistemos, duomenų bazės, priemonės, žmogiškieji ištekliai), ir juos sujungti į vieną bendrą bazę, naudojamą didelės apimties skaičiavimams atlikti ir pritaikyti įvairioms taikomosioms programoms, kurioms reikia daug duomenų.

([12]) Duomenų vagystės (*phishing*) — informatikoje taip vadinama įsilaužimo forma, naudojama asmens ir konfidencialiems duomenims neteisėtai gauti siekiant pavogti tapatybę ir išsiųsti klaidinančius elektroninius laiškus naudojant autentiškus duomenis.

([13]) Piratavimas internete (*piracy*) — šis terminas naudojamas interneto „piratų“, kai programinė įrangos apsauga, draudžianti daryti kopijas, sulaužoma ir tampa prieinama internete.

([14]) COM(2001) 298 final.

([15]) Žr. 1 išnašą.

— reguliavimo sistemą, kurioje būtų numatyta duomenų ir privatumo apsauga;

— kova su elektroniniais nusikaltimais.

2.6 Tinklų sistemos elektroninių atakų registracija, identifikavimas ir prevencija — sudėtingas uždavinys ieškant tinkamų sprendimų, kadangi programinė įranga nuolat tobulėja, keičiasi tinklo protokolų ir siūlomų paslaugų įvairovė, o kartu sudėtingėja ir elektroninės atakos formos ([16]).

2.7 Investicijų į saugumą neapčiuopiama grąža ir nepakankama vartotojų atsakomybė, deja, neleido tinkamai įvertinti rizikos ir dėti visų galimų pastangų saugumo kultūrai vystyti.

3. **Komisijos pasiūlymas**

3.1 Komunikatu dėl saugios informacinės visuomenės strategijos ([17]) Komisija siekia pagerinti informacijos saugumą sukurdama dinamišką ir integruotą strategiją, kurioje nurodoma:

a) užtikrinus geresnį saugumą, stiprinti viešojo valdymo institucijų ir Komisijos dialogą remiantis valstybių narių elektroninio ryšio politikos ir geriausios patirties lyginamuoju vertinimu;

b) Komisijai atliekant skatinamąjį vaidmenį ir aktyviau dalyvaujant Europos tinklų ir informacijos saugumo agentūrai (ETISA), kuri atsakinga už tinklų ir informacijos saugumą, geriau supažindinti piliečius ir MVĮ su veiksmingomis apsaugos sistemomis;

c) užmegzti dialogą apie reglamentavimo būdus ir priemones siekiant užtikrinti saugumo ir pagrindinių teisių pusiausvyrą, įskaitant teisę į privatumą.

3.2 Be to komunikate numatyta, kad, remiantis tinkamu duomenų rinkimą reglamentuojančiu teisiniu pagrindu dėl saugumo pažeidimų, vartotojų pasitikėjimo ir informacijos saugumo pramonės plėtojimo, ETISA užmegs patikimą partnerystę su:

a) valstybėmis narėmis,

b) vartotojais,

c) informacijos saugumo pramone,

d) privačiu sektoriumi,

kuriant daugiakalbį europinį informacijos ir perspėjimo apie pavojų portalą, kurio tikslas užtikrinti strateginę privataus sektoriaus, valstybių narių ir mokslininkų partnerystę.

3.2.1 Be to, komunikatas suinteresuotiems subjektams numato daugiau atsakomybės saugumo poreikio ir galimo pavojaus atžvilgiu.

3.2.2 Tarptautinio bendradarbiavimo ir bendradarbiavimo su trečiosiomis šalimis atžvilgiu „tinklų ir informacijos saugumas yra aktualus visam pasauliui, tai verčia Komisiją tiek tarptautiniu lygmeniu, tiek ir bendradarbiaujant su valstybėmis narėmis, dėti daugiau pastangų skatinant pasaulinį bendradarbiavimą tinklų ir informacijos saugumo klausimais“ ([18]). Tačiau šis teiginys neatsispindi numatytuose dialogo ir partnerystės plėtojimo bei atsakomybės suteikimo veiksmuose.

4. **Pastabos**

4.1 Komitetas pritaria svarstymams ir teiginiams, pagrindžiantiems integruotą ir dinamišką Europos strategiją, kuria siekiama pagerinti tinklų ir informacijos saugumą. Jis mano, kad saugumo klausimas yra esminis siekiant skatinti palankesnį požiūrį į informacinių technologijų (IT) diegimą ir pagerinti jų patikimumą. EESRK savo poziciją išdėstė daugelyje pateiktų nuomonių ([19]).

4.1.1 Komitetas dar kartą pabrėžia ([20]), kad „internetas ir interneto technologijos (tokios kaip mobilieji telefonai arba vis labiau populiarėjantys delniniai kompiuteriai, galintys prisijungti prie interneto ir turintys daugialypės terpės funkciją) yra svarbiausios žiniomis grindžiamos ekonomikos, elektroninės ekonomikos bei elektroninės vyriausybės vystymo priemonės“.

([16]) *Multivariate Statistical Analysis for Network Attacks Detection*. *Guangzhi Qu, Salim Hariri**, 2005 m. JAV, Arizonos valstija.
Interneto technologijų laboratorija, ECE (Elektroninės ir kompiuterių inžinerijos) fakultetas, Arizonos universitetas, http://www.ece.arizona.edu/~hpdc
Mazin Yousif, „Intel“ Korporacija, JAV. — Darbas parengtas iš dalies jį finansuojant „Intel“ Korporacijos IT mokslinių tyrimų ir taikomosios veiklos tarybos stipendija.

([17]) 2006 m. gegužės 31 d. COM(2006) 251 final.

([18]) Žr. COM(2006) 251 3 punktą, priešpaskutinę pastraipą.

([19]) Žr. šiuos dokumentus:
— EESRK nuomonė dėl *Pasiūlymo priimti Europos Parlamento ir Tarybos direktyvą dėl duomenų, tvarkomų teikiant viešąsias elektroninių ryšių paslaugas, saugojimo ir iš dalies pakeičiančią Direktyvą 2002/58/EB* — OL C 69, 2006 3 21 p. 16;
— EESRK nuomonė dėl *Komisijos komunikato Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl i2010 — Europos informacinė visuomenė augimui ir užimtumui skatinti* — OL C 110, 2006 5 9 p. 83;
— EESRK nuomonė dėl *Pasiūlymo priimti Europos Parlamento ir Tarybos sprendimą sukurti daugiametę Bendrijos programą, skatinančią saugesnį naudojimąsi internetu bei naujosiomis interneto technologijomis* OL C 157, 2005 6 28 p. 136;
— EESRK nuomonė dėl *Komisijos komunikato Tarybai, Europos Parlamentui, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl tinklų ir informacijos apsaugos: Pasiūlymas priimti politinį sprendimą Europos lygiu* OL C 48, 2002 2 21 p. 33.

([20]) Žr. 19 išnašos trečią įtrauką.

4.2 *Pritarti ryžtingesniems Komisijos pasiūlymams*

4.2.1 Komitetas vis dėlto mano, kad Komisijos siūlomas požiūris, kuriuo siekiama sukurti integruotą ir dinamišką strategiją remiantis atviru ir visas suinteresuotas šalis apimančiu dialogu, ir glaudesne jų, o visų pirma vartotojų, partneryste ir didesnės atsakomybės jiems suteikimas, galėtų būti dar išplėstas.

4.2.2 Tokio požiūrio Komitetas laikėsi ankstesnėse savo nuomonėse: „Kad ši kova būtų efektyvi, į ją turėtų būti įtraukiami visi interneto vartotojai. Interneto vartotojus reiktų mokyti bei informuoti apie apsaugos priemones bei metodus, naudojamus apsaugai nuo pavojingos ar nepageidaujamos informacijos gavimo, taip pat ir nuo to, kad jie patys netaptų šios informacijos perdavimo punktais. Komiteto nuomone, veiksmų plano prioritetu, atsižvelgiant į mokymą ir informavimą, turėtų būti interneto naudotojų mobilizavimas“ ([21]).

4.2.3 Komitetas mano, kad vartotojai ir piliečiai turėtų dalyvauti tik užtikrinant būtiną informacijos ir tinklo apsaugą bei privatumą ir vartotojų teisę naudotis saugia prieiga už prieinamą kainą.

4.2.4 Reikėtų pabrėžti, kad informacijos saugumo siekis susijęs su vartotojų sąnaudomis ne tik laiko, sugaišto kliūtims pašalinti ar jas apeiti, požiūriu. Komiteto manymu, reikėtų numatyti reikalavimą automatiškai visuose kompiuteriuose instaliuoti antivirusines apsaugos sistemas, kurias vartotojas pasirinktų paleisti ar ne, tačiau nuo pat gaminio įsigijimo tokia galimybė būtų numatyta.

4.3 *Kurti dinamišką ir pažangią Bendrijos strategiją*

4.3.1 Be to, EESRK mano, kad Europos Sąjunga turėtų kelti aukštesnius tikslus ir sukurti pažangią, integruotą ir dinamišką strategiją, grindžiamą šiomis naujomis iniciatyvomis:

— diegti sistemas, užtikrinančias skaitmeninę vartotojų atpažintį, kadangi jų pernelyg dažnai reikalaujama tapatumą patvirtinančių duomenų;

— užtikrinti saugias prieigos prie IRT ([22]), leidžiančių rasti konkrečius ir greitus sprendimus, sąlygas, kurios yra bendrą Europos Sąjungos saugumą lemiantis veiksnys;

— imtis prevencinių veiksmų įvedant minimalius informacinių sistemų ir tinklo saugumo reikalavimus ir eksperimentinio pobūdžio informacijos saugumo akcijų visose ir įvairių lygių mokymo įstaigose;

— Europos lygiu sukurti patikimą ir pripažintą teisinę ir reguliavimo sistemą, kuri būtų taikoma informatikos srityje ir tinklams. Tokia sistema leistų žengti žingsnį nuo informatikos saugumo informatikos patikimumo link;

— tobulinti Europos ir nacionalines rizikos vertinimo sistemas ir užtikrinti geresnį įstatymų bei kitų teisės aktų nuostatų įgyvendinimą, kad būtų baudžiama už su privačiu gyvenimu ir informacijos rinkmenomis susijusius nusikaltimus;

— imtis veiksmų, kurie padėtų išvengti informacinių monokultūrų, naudojančių lengvai „piratuojamus“ produktus, atsiradimo. Remti įvairias daugiakultūres naujoves siekiant sukurti bendrą informacinę Europos erdvę (SEIS, *Single European Information Space*).

4.3.2 Komitetas mano, kad reikėtų sukurti centrą „IRT saugumas“, skirtą generalinių direktoratų ryšiams palaikyti ([23]). Šis centras galėtų plėtoti veiklą:

— Komisijos vidaus tarnybų lygiu;

— valstybių lygiu: parengus horizontaliai taikomus sprendimus, susijusius su sąveikumo, tapatybės valdymo, privataus gyvenimo apsaugos, laisvos prieigos prie paslaugų ir informacijos aspektais bei minimaliais saugumo reikalavimais;

— tarptautiniu lygiu: kad Europa galėtų pareikšti vieningą nuomonę JTO, G8, Ekonominio bendradarbiavimo ir plėtros organizacijoje, Tarptautinėje standartizacijos organizacijoje.

4.4 *Stiprinti ES atsakingo koordinavimo priemones*

4.4.1 Komiteto įsitikinimu, taip pat labai svarbu sukurti Europos tinklų ir informacijos saugumo tinklą, kuris padėtų skatinti apklausas, tyrimus ir seminarus apie saugumo mechanizmus ir jų sąveikumą, apie pažangią kriptografiją ir privatumo apsaugą.

4.4.2 Komiteto nuomone, siekiant optimizuoti Europos mokslinių tyrimų vaidmenį šiame ypatingai pažeidžiamame sektoriuje, reikėtų parengti naudingą šios informacijos santrauką:

— Europos saugumo mokslinių tyrimų programos (ESRP) ([24]), įtrauktos į 7-ąją MTTPD pagrindų programą,

([21]) Žr. 19 išnašos trečią įtrauką.

([22]) ETSI (Europos telekomunikacijų standartų institutas), žr. visu pirma 2006 m. sausio 16-17 d. seminarą. Be to, ETSI parengė specifikacijas dėl neteisėto kišimosi (TS 102 232; 102 233; 102 234), interneto prieigos prie belaidžio LAN (TR 102 519) ir elektroninių parašų, taip pat parengė saugumo algoritmus GSM, GPRS ir UMTS.

([23]) Šis centras ryšiams tarp GD palaikyti galėtų būti finansuojamas remiantis TSI specialiosios bendradarbiavimo programos pagal Septintąją bendrąją mokslinių tyrimų, technologinės plėtros ir demonstracinės veiklos programą arba ES saugumo mokslinių tyrimo programos (PERS) prioritetais.

([24]) Žr. 7-ąją MTTPD programą. Specialioji bendradarbiavimo programa; teminiam saugumo prioritetui 2007-2013 m. laikotarpiui skirtas 1.35 mlrd. eurų biudžetas.

— *Safer Internet Plus* programos ir

— Europos programos dėl ypatingos svarbos infrastruktūros objektų apsaugos (EPCIP) ([25]).

4.4.3 Be to, siūloma paskelbti Europos informacijos saugumo dieną, kurią remtų nacionalinės švietimo kampanijos mokyklose ir informacijos kampanijos, skirtos naudotojams ir susijusios su IT informacijos apsaugos procedūromis, aišku, nekalbant apie informaciją, susijusią su technologine pažanga plačioje ir nuolat kintančioje kompiuterių srityje.

4.4.4 Komitetas ne kartą yra pabrėžęs, kad „nuo elektroninės prekybos saugumo lygio priklauso įmonių apsisprendimas savo veikloje naudoti IRT. Nuo elektroninių sandorių saugumo lygio taip pat labai priklauso vartotojų pasiryžimas interneto tinklalapyje paskelbti savo kreditinės kortelės duomenis“ ([26]).

4.4.5 Komitetas yra įsitikinęs, kad, atsižvelgiant į didžiulį sektoriaus augimo potencialą, reikia sukurti jam skirtą politiką, o esamą politiką pritaikyti prie naujų pokyčių. Būtina sukurti integruotą informacijos saugumo strategiją, sujungiančia visas Europos iniciatyvas ir panaikinančią ribas tarp sektorių bei užtikrinančią tolygią ir saugią IRT sklaidą visuomenėje.

4.4.6 Komitetas mano, kad tokios svarbios strategijos, kaip šiuo metu nagrinėjama, įgyvendinamos itin lėtai dėl valstybių narių biurokratinių ir kultūrinių kliūčių, kurios trukdo priimti būtinus sprendimus Bendrijos lygiu.

4.4.7 Komitetas taip pat mano, kad Bendrijos išteklių nepakanka daugeliui prioritetinių projektų, kurie konkrečiai padėtų išspręsti naujas su globalizacija susijusias problemas tik tuomet, jei būtų įgyvendinami Bendrijos lygiu.

4.5 *Siekti didesnių Bendrijos garantijų vartotojų apsaugos srityje*

4.5.1 Komitetas supranta, kad valstybės narės technologines saugumo priemones ir saugumo valdymo procedūras ėmėsi įgyvendinti atsižvelgdamos į savo pačių poreikius ir dėmesį skiria skirtingiems aspektams. Tai viena iš priežasčių, kodėl sunku rasti bendrą ir veiksmingą saugumo problemų sprendimą. Nors saugumo klausimų įvairios valstybės narės atskirai spręsti negali, išskyrus kai kuriuos administracinius tinklus, tarp valstybių narių sistemingas bendradarbiavimas nevyksta.

4.5.2 Be to, Komitetas pastebi, kad Taryba savo pamatiniu sprendimu 2005/222/JAI pateikė teisminių institucijų ir kitų kompetentingų institucijų bendradarbiavimo pagrindines nuostatas, kuriomis, suartinus nacionalines baudžiamosios teisės nuostatas dėl atakų prieš informacines sistemas, siekiama užtikrinti vienodą valstybių narių požiūrį į:

— neteisėtą prieigą prie informacinių sistemų;

— neteisėtą įsikišimą į sistemą siekiant sukelti tyčinį rimtą informacinės sistemos veikimo sutrikdymą ar nutraukimą;

— neteisėtą įsikišimą į informacinėje sistemoje esančius kompiuterinius duomenis siekiant juos ištrinti, sugadinti, pažeisti, pakeisti, nuslėpti arba užkirsti prieigą prie jų;

— kurstymą, bendrininkavimą ir pasikėsinimą, susijusį su pirmiau išvardytais nusikaltimais.

4.5.3 Pamatiniame sprendime taip pat patikslinami kriterijai, leidžiantys nustatyti juridinių asmenų atsakomybę ir galimas sankcijas, kurios taikomos atsakomybę nustačius.

4.5.4 Kalbant apie dialogą su valstybių narių institucijomis, Komitetas pritaria Komisijos pasiūlymui, kad šios valdžios institucijos turėtų palyginti valstybių narių tinklų ir informacijos saugumo politiką, įskaitant ir konkrečiai viešajam sektoriui skirtą saugumo politiką. Šis pasiūlymas jau buvo pateiktas 2001 m. EESRK nuomonėje ([27]).

4.6 *Siekti bendresnės saugumo kultūros*

4.6.1 Siekiant apginti klientų teisę į privatumo apsaugą ir konfidencialumą, reikia įtraukti informacijos saugumo pramonę, kuri užtikrintų, kad jų įrenginių priežiūrai naudojamos sistemos ir duomenų kodavimas neatsilieka nuo technologijų pažangos ([28]).

([25]) 2005 m. lapkričio 17 d. COM (2005) 576.
([26]) Žr. 19 išnašos antrą įtrauką.
([27]) Žr. 19 išnašos ketvirtą įtrauką.
([28]) Žr. Direktyvą 97/66/EB dėl asmens duomenų tvarkymo telekomunikacijų srityje (OL L 24/1998).

4.6.2 Didesnio visuomenės informavimo kampanijų klausimu Komitetas mano, kad būtina sukurti tikrą „saugumo kultūrą“, kuri visiškai neprieštarautų informacijos, komunikacijos ir išraiškos laisvei. Daugelis naudotojų nežino apie riziką, susijusią su skaitmeniniu piratavimu, o daugelis operatorių, pardavėjų ir tiekėjų nepajėgūs įvertinti, ar sistema turi trūkumų ir kokio jie masto.

4.6.3 Nors privatumo ir asmens duomenų apsauga yra prioritetiniai tikslai, vartotojai taip pat turi teisę į tikrai veiksmingą apsaugą nuo netinkamo asmens profiliavimo „šnipukais“ ir „riktais“ (angl. *spyware* ir *web bugs*) ar kitais būdais. Su tuo dažnai susijęs elektroninių pašto šiukšlių (daugybė nepageidaujamų žinučių ([29])) siuntinėjimas taip pat turėtų būti sustabdytas. Nuo tokių įsibrovimų kenčia su tuo susiję asmenys ([30]).

4.7 *Siekti, kad Europos agentūra būtų stipresnė ir aktyvesnė*

4.7.1 Komitetas pritaria veiksmingesniam ir stipresniam Europos tinklų ir informacijos saugumo agentūros (ETISA) vaidmeniui skleidžiant informaciją ir ypač informuojant bei rengiant operatorius ir naudotojus, kaip jis nurodė savo neseniai parengtoje nuomonėje ([31]) dėl viešųjų elektroninių ryšių paslaugų teikimo.

4.7.2 Galiausiai, siūlomos iniciatyvos dėl visų suinteresuotų subjektų grupių didesnės atsakomybės turi būti įgyvendinamos griežtai laikantis subsidiarumo principo. Iš tikrųjų, šis uždavinys turėtų tekti valstybėms narėms ir privačiam sektoriui atsižvelgiant į jų konkrečias kompetencijos sritis.

4.7.3 ENISA turėtų gauti Europos tinklų ir informacijos saugumo tinklo (angl. *European Network and Information Security Network*) paramą imantis bendrų veiksmų ir turėti galimybę naudotis įvairiomis kalbomis parengtu Bendrijos portalu, skelbiančiu apie informacijos saugumo pavojus, skirtu teikti asmenišką, sąveikią ir vartotojui palankią informaciją, ir orientuotu į visų amžiaus grupių individualius naudotojus bei mažas ir vidutines įmones.

2007 m. vasario 16 d., Briuselis.

Europos ekonomikos ir socialinių reikalų komiteto
pirmininkas
Dimitris DIMITRIADIS

([29]) Angl. *spamming*.

([30]) Žr. EESRK nuomones dėl elektroninių ryšių tinklų (OL C 123, 2001 4 25, p. 50), dėl elektroninės prekybos (OL C 169, 1999 6 16, p. 36) ir dėl elektroninės prekybos poveikio bendrajai rinkai (OL C 123, 2001 4 25, p. 1).

([31]) Žr. 19 išnašos pirmą įtrauką.