Mnenje Evropskega ekonomsko-socialnega odbora o sporočilu Komisije Svetu, Evropskemu parlamentu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij — Strategija za varno informacijsko družbo — Dialog, partnerstvo ter povečanje vpliva in moči

COM(2006) 251 konč.

(2007/C 97/09)

Komisija je 31. maja 2006 sklenila, da v skladu s členom 262 Pogodbe o ustanovitvi Evropske skupnosti Evropski ekonomsko-socialni odbor zaprosi za mnenje o zgoraj omenjenem dokumentu.

Strokovna skupina za promet, energijo, infrastrukturo in informacijsko družbo, zadolžena za pripravo dela Odbora na tem področju, je mnenje sprejela 11. januarja 2007. Poročevalec je bil g. PEZZINI.

Evropski ekonomsko-socialni odbor je mnenje sprejel na 433. plenarnem zasedanju 15. in 16. februarja (seja z dne 16. februarja 2007) s 132 glasovi za in 2 vzdržanima glasovoma.

1. **Sklepi in priporočila**

1.1 Odbor je prepričan, da postaja informacijska varnost za podjetja, uprave, javne in zasebne organe ter posameznike vse večji problem.

1.2 Odbor se na splošno strinja z analizami in argumenti, ki zahtevajo novo strategijo, da bi povečali varnost omrežij in informacij pred napadi in vpadi, ki ne poznajo državnih mej.

1.3 Odbor meni, da bi si morala Komisija, upoštevajoč razsežnosti pojava in njegove gospodarske posledice ter posledice za zasebnost, še dodatno prizadevati za uresničitev inovativne in strukturirane strategije.

1.3.1 EESO poudarja tudi, da je Komisija pred kratkim objavila novo sporočilo o informacijski varnosti in da bi kmalu moral iziti nov dokument o tej problematiki. Odbor si pridržuje pravico, da v prihodnosti objavi bolj strukturirano mnenje, ki bo upoštevalo vsa sporočila kot celoto.

1.4 Odbor poudarja, da vprašanja informacijske varnosti nikakor ni mogoče obravnavati ločeno od krepitve varstva osebnih podatkov in varstva svoboščin, zajamčenih z Evropsko konvencijo o človekovih pravicah.

1.5 EESO se vprašuje, kakšna je zdaj dodana vrednost predloga v primerjavi s celostnim pristopom, sprejetim leta 2001, katerega namen je bil enak namenu, navedenem v tem Sporočilu ([1]).

1.5.1 Dokument Ocena vplivov *(Impact Assessment)* ([2]), priložen predlogu, vsebuje nekaj zanimivih posodobitev glede na stališče iz leta 2001, objavljen pa je bil samo v enem jeziku, torej ni dostopen številnim evropskim državljanom, ki svoje mnenje oblikujejo na podlagi uradnega dokumenta, izraženega v jezikih Skupnosti.

1.6 Odbor se sklicuje na sklepe svetovnega vrhunskega srečanja v Tunisu leta 2005 v zvezi z informacijsko družbo, ki jih je potrdila Skupščina OZN 27. marca 2006:

— načela nediskriminatorskega dostopa,

— spodbujanje informacijskih in komunikacijskih tehnologij (IKT) kot instrumenta miru,

— instrumenti za krepitev demokracije, kohezije in dobrega upravljanja,

— preprečevanje zlorab, ob spoštovanju človekovih pravic ([3]).

1.7 Odbor poudarja, da bi morala dinamična in celostna strategija Skupnosti, poleg dialoga, partnerstva in ozaveščanja, zajeti tudi:

— preprečevalne ukrepe,

— prehod z informacijske varnosti na informacijsko zavarovanje ([4]),

— vzpostavitev zanesljivega in priznanega pravnega, zakonodajnega in kazenskega okvira EU,

— krepitev tehnične standardizacije,

([1]) Glej: Mnenje EESO o *Sporočilu Komisije Svetu, Evropskemu parlamentu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o varnosti omrežij in informacij: predlog za evropski politični pristop*, UL C 48 z dne 21.2.2002, str. 33.

([2]) „Dokument o oceni vplivov“ nima enake teže, kot jo ima „dokument o strategiji“.

([3]) OZN 27.3.2006, priporočili št. 57 in 58. Zaključni dokument iz Tunisa št. 15.

([4]) Glej: *Emerging technologies in the context of security* (Nove tehnologije v kontekstu varnosti); CCR- Inštitut za varstvo in varnost državljanov, zvezek strateških raziskav, september 2005, Evropska komisija, http://serac.jrc.it.

— digitalno identifikacijo uporabnikov,

— vzpostavitev evropskih vaj informacijske varnosti na področju analize in predvidevanja *(foresight)* v razmerah multimodalnih tehnoloških konvergenc,

— krepitev evropskih in nacionalnih mehanizmov ocenjevanja tveganj,

— ukrepe za preprečevanje pojavljanja informacijskih monokultur,

— krepitev usklajevanja v okviru Skupnosti, na evropski in mednarodni ravni,

— ustanovitev nacionalne kontaktne točke za IKT (*ICT Security Focal Point)* med generalnimi direktorati,

— vzpostavitev Evropskega omrežja za varnost omrežij in informacij *(European Network and Information Security Network),*

— optimizacijo vloge evropskih raziskav na področju informacijske varnosti,

— uvedbo „evropskega dneva varnega računalnika“,

— pilotne ukrepe Skupnosti v šolah različnih vrst in stopenj na področjih informacijske varnosti.

1.8 Odbor meni, da je treba za zagotovitev dinamične in celostne strategije Skupnosti predvideti primerno finančno pomoč iz proračuna, z okrepljenimi pobudami in usklajevalnimi ukrepi na ravni Skupnosti, s katerimi bi bilo mogoče enotno predstavljati Evropo v svetu.

2. **Obrazložitev**

2.1 Varnost informacijske družbe je temeljnega pomena za zagotavljanje zaupanja in zanesljivosti omrežij in komunikacijskih storitev, ki so glavni dejavniki za razvoj gospodarstva in družbe.

2.2 Informacijska omrežja in sistemi morajo biti zaščiteni, da ohranjajo konkurenčne in komercialne zmogljivosti, da jamčijo neokrnjenost in kontinuiteto elektronskih komunikacij, da preprečujejo goljufije in zagotavljajo zakonsko varstvo zasebnosti.

2.3 Elektronske komunikacije in z njimi povezane storitve so največji segment celotnega sektorja telekomunikacij: leta 2004 je internet aktivno uporabljalo približno 90 % evropskih podjetij in 65 % jih je oblikovalo lastno spletno stran. Računajo, da internet redno uporablja približno polovica evropskega prebivalstva, 25 % gospodinjstev pa stalno uporablja širokopasovni dostop ([5]).

([5]) *i2010: Na poti k dinamičnemu pristopu k varni informacijski družbi.* Generalni direktorat za informacijsko družbo in medije, Factsheet 8 (junij 2006), http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-en.pdf.

2.4 Kljub hitrejši rasti vlaganj dosegajo izdatki za varnost samo 5 do 13 % celotnih vlaganj v informacijske tehnologije. Ti odstotki so veliko prenizki. Novejše študije so pokazale, da *„je v povprečju od 30 protokolov, ki jih skupno uporabljajo ključne strukture, 23 ranljivih za večprotokolne napade“* ([6]). Poleg tega računajo, da se vsak dan v povprečju prenese 25 milijonov elektronskih sporočil *spam* ([7]), zato Odbor pozdravlja nedavni predlog Komisije v zvezi s tem.

2.5 Na področju računalniških virusov ([8]) je hiter, množičen razvoj programov *worms* ([9]) in „*spyware* ([10])“ potekal vzporedno z vse hitrejšim razvojem sistemov in omrežij elektronskih komunikacij. Ti so postajali vse bolj zapleteni in obenem ranljivi, kar je bila tudi posledica konvergence multimedijev in sistemov GRID *infoware* ([11]): primeri izsiljevanja, DDoS (*Distributed denials of service*), internetne kraje identitete, *phishing* ([12]), *piratstvo* ([13]) itd. so izzivi za varnost informacijske družbe. Evropska skupnost je problem že obravnavala v enem svojih sporočil iz leta 2001 ([14]), o katerem je Odbor izrazil svoje mnenje ([15]) in ugotovil tri smeri ukrepanja:

— specifične varnostne ukrepe,

([6]) *Proceedings of the First International Conference on Availability, Reliability and Security* (ARES'06) (Poročila prve mednarodne konference o razpoložljivosti, zanesljivosti in varnosti) — Zvezek 00 ARES 2006, založnik IEEE Computer Society.

([7]) *Spam* = nezaželena komercialna sporočila po elektronski pošti. *Spam* je prvotno pomenil „spiced pork and ham“ (začinjeno svinjetino in šunko), nekakšno mesno konzervo v želatini, zelo priljubljeno v času druge svetovne vojne, ko je postala — tudi zato, ker ni bila več racionirana — eno glavnih živil za ameriške čete in angleško prebivalstvo. Zaradi dolgih let takšne diete je izraz dobil negativen pomen.

([8]) *Računalniški virus:* poseben računalniški program, ki se uvršča v kategorijo *malwarea* (škodljivih programov) in lahko, ko je izveden, okuži datoteke, da se lahko razmnožuje s kopiranjem samega sebe, praviloma tako, da uporabnik tega ne opazi. Virusi so lahko za operacijski sistem, ki jih gosti, bolj ali manj škodljivi, vendar tudi v najboljšem primeru povzročajo nepotrebno porabo virov: delovnega pomnilnika (RAM), procesorja (CPU) in prostora na trdem disku *(www. wikipedia.org/wiki/Virus_informatico)*.

([9]) *Worm* (črv) = škodljiv program, ki se je zmožen razmnoževati: *„e-mail worm“* (črv elektronskega sporočila) je uničujoč napad na omrežje, pri katerem črv zbere vse naslove elektronske pošte, vsebovane v lokalnem programu (recimo MS Outlook), potem pa na te naslove razpošlje na stotine elektronskih sporočil, ki vsebujejo črva kot nevidno prilogo.

([10]) *Spyware* (vohunski programi) = programi, ki beležijo, katere internetne strani uporabnik bere; namestijo se samodejno, brez obvestila uporabniku, brez njegove vednosti, privolitve in nadzora.

([11]) GRID *infoware* = omogoča souporabo, izbor in združevanje širokega razpona geografsko razporejenih virov za elektronsko obdelavo (recimo superračunalnikov, grozdov *(clusters)* računalnikov, sistemov za zapisovanje podatkov, virov podatkov, orodij in oseb), pri čemer jih predstavlja kot enoten, samostojen vir, namenjen najzahtevnejšim izračunom in posebno intenzivnim obdelavam podatkov.

([12]) *Phishing* = na informacijskem področju je „phishing“ opredeljen kot tehnika *crackinga*, ki se uporablja za pridobitev dostopa do osebnih in zaupnih podatkov z namenom kraje identitete s pomočjo uporabe ponarejenih elektronskih sporočil, ustrezno pripravljenih tako, da se zdijo pristna.

([13]) *Piracy* (piratstvo) = izraz, ki ga uporabljajo informacijski „pirati“ za programsko opremo, ki ji je bila odvzeta zaščita proti kopiranju in je na voljo za prenos z interneta.

([14]) COM(2001) 298 konč.

([15]) Glej opombo 1.

— zakonodajni okvir, vključno z varstvom podatkov in zasebnosti,

— boj proti kiberkriminalu.

2.6 Zaznavanje, identificiranje in preprečevanje informacijskih napadov v okviru omrežnega sistema so izzivi za iskanje primernih rešitev, spričo stalnih sprememb konfiguracij, raznolikosti omrežnih protokolov, ponujanih in razvitih storitev ter skrajno zapletene asinhrone narave napadov ([16]).

2.7 Žal pa sta slaba prepoznavnost obrestovanja vlaganj v varnost in dejstvo, da le malo uporabnikov prevzema odgovornost, privedla do podcenjevanja tveganj in do zmanjšanja pozornosti do razvoja varnostne kulture.

3. **Predlog Komisije**

3.1 S sporočilom o strategiji za varno informacijsko družbo ([17]) je Komisija želela izboljšati informacijsko varnost s pripravo dinamične in celostne strategije, temelječe na:

a) izboljševanju dialoga med javnimi organi in Komisijo, s *primerjalno analizo* nacionalnih politik in opredelitvi *najbolj učinkovitih praks elektronskih komunikacij* v varnem načinu;

b) boljšem ozaveščanju državljanov in malih ter srednje velikih podjetij glede učinkovitih varnostnih načinov, s tem, da bi morala Komisija imeti spodbujevalno vlogo, Evropsko agencijo za varnost omrežij in informacij (ENISA) pa bi bilo treba bolj vključiti;

c) dialog o instrumentih in predpisih za uravnoteženo razmerje med varnostjo in temeljnimi pravicami, vključno z varstvom zasebnosti.

3.2 Sporočilo poleg tega predvideva zaupno partnerstvo agencije ENISA, s primernim okvirom za zbiranje podatkov o kršitvah varnosti, o ravneh zaupnosti uporabnikov in o razvoju varnostne industrije:

a) z državami članicami,

b) s potrošniki in uporabniki,

c) z industrijo informacijske varnosti in

d) z zasebnim sektorjem.

Vzpostaviti bi bilo treba večjezični spletni portal EU za obveščanje in opozarjanje na tveganja, s ciljem strateškega partnerstva med zasebnim sektorjem, državami članicami in raziskovalci.

3.2.1 Sporočilo nadalje predvideva močnejše ozaveščanje zainteresiranih strani o varnostnih potrebah in tveganjih.

3.2.2 Kar se tiče mednarodnega sodelovanja in sodelovanja s tretjimi državami, „globalna razsežnost varnosti omrežij in informacij od Komisije zahteva, da na mednarodni ravni in v sodelovanju z državami članicami poveča svoja prizadevanja za spodbujanje globalnega sodelovanja za VOI“ (varnost omrežij in informacij) ([18]), vendar ta ugotovitev ni vključena v dejavnosti dialoga, partnerstva ter povečanja vpliva in moči.

4. **Ugotovitve**

4.1 Odbor se strinja z analizami in argumenti, ki upravičujejo celostno in dinamično evropsko strategijo za varnost omrežij in informacij; meni, da je vprašanje varnosti bistvenega pomena za spodbujanje odnosa, ki bi bil uporabi informacijskih tehnologij bolj naklonjen, in za krepitev zaupanja v te tehnologije. Svoja stališča je EESO predstavil v številnih mnenjih ([19]).

4.1.1 Odbor vnovič poudarja ([20]), da so „omrežje interneta in nove tehnologije komuniciranja po omrežju (npr. mobilna telefonija ali osebni digitalni pomočniki/dlančniki/z multimedijskimi funkcijami, zmožni povezovanja v mrežo in zdaj v polnem razmahu) orodja temeljnega pomena za razvoj gospodarstva znanja, e-gospodarstva in omrežne uprave.“

([16]) *Multivariate Statistical Analysis for Network Attacks Detection* (Multivariabilna statistična analiza za odkrivanje omrežnih napadov). Guangzhi Qu, Salim Hariri* —2005 ZDA, Arizona
Internet Technology Laboratory, ECE Department, The University of Arizona, www.ece.arizona.edu/~hpdc,
Mazin Yousif, Intel Corporation, ZDA — Delo je delno podprl svet za raziskave in razvoj informacijskih tehnologij pri družbi Intel.

([17]) COM(251) 2006 z dne 31.5.2006.

([18]) Glej COM 251/2006, predzadnji odstavek poglavja 3.

([19]) Glej naslednje dokumente:
— mnenje EESO o *predlogu direktive Evropskega parlamenta in Sveta o hrambi podatkov, obdelanih v zvezi z zagotavljanjem javnih elektronskih komunikacijskih storitev, in spremembi Direktive 2002/58/ES-* UL C 69 z dne 21.3.2006, str. 16;
— mnenje EESO o *sporočilu Komisije Svetu, Evropskemu parlamentu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij — i2010 — Evropska informacijska družba za rast in zaposlovanje-* UL C 110 z dne 9.5.2006, str. 83;
— mnenje EESO o *predlogu Evropskega parlamenta in Sveta o uvedbi večletnega programa Skupnosti za spodbujanje varnejše uporabe interneta in novih spletnih tehnologij* — UL C 157 z dne 28.6.2005, str. 136;
— mnenje EESO 1474o *sporočilu Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij Varnost omrežij in varnost informacij: predlog za evropski strateški pristop* — UL C 48 z dne 21.2.2002, str. 33.

([20]) Glej opombo 19, alinejo 3.

4.2 *Za večjo veljavnost predlogov Komisije*

4.2.1 Vendar pa Odbor meni, da je pristop, ki ga predlaga Komisija in ki predvideva utemeljevanje te celostne in dinamične strategije na odprtem in vključujočem dialogu, skupaj z okrepljenim partnerstvom in okrepljenim povečanjem vpliva in moči, med vsemi zainteresiranimi stranmi in zlasti z uporabniki, mogoče še razširiti.

4.2.2 To stalšče je bilo poudarjeno v prejšnjih mnenjih: „Da bi bil učinkovit, mora ta program neposredno vključevati vse uporabnike interneta, ki morajo biti usposobljeni in seznanjeni z varnostnimi ukrepi in sredstvi, ki jih je treba uporabljati za preprečitev sprejemanja škodljivih ali nezaželenih vsebin, ali pa za preprečitev tega, da bi bili uporabniki uporabljeni kot posredniki takšnih vsebin. Po mnenju Odbora mora del programa, ki zadeva usposabljanje in seznanjanje, torej nameniti absolutno prednost vključevanju uporabnikov“ ([21]).

4.2.3 Vključevanje uporabnikov in državljanov pa mora po mnenju Odbora potekati tako, da združuje potrebno zaščito informacij in omrežij z državljanskimi svoboščinami ter pravico uporabnikov do varnega dostopa in zmernih cen.

4.2.4 Treba je upoštevati, da pomeni prizadevanje za informacijsko varnost strošek za potrošnika, tudi zaradi časa, ki je potreben za odstranjevanje ovir ali za to, da se jim izognemo. Odbor meni, da bi bilo treba določiti, da mora biti vsak računalnik obvezno opremljen s sistemom protivirusne zaščite. Uporabnik bi odločal, ali ga aktivira, vendar bi bil sistem že od vsega začetka v izdelku.

4.3 *Za bolj dinamično in inovativno strategijo EU*

4.3.1 Poleg tega bi si Unija po mnenju Odbora morala zastavljati bolj ambiciozne cilje in sprejeti inovativno, celostno in dinamično strategijo z novimi pobudami, npr.:

— mehanizme, ki omogočajo digitalno identifikacijo posameznih uporabnikov, od katerih se prepogosto zahteva, naj zavrnejo lastne matične podatke;

— ukrepe, izvedene v okviru ETSI ([22]), ki bi zagotavljali varno uporabo IKT in ponujali hitre, točne rešitve, določene s skupnim varnostnim pragom v vsej EU;

— preprečevalne ukrepe z vključevanjem minimalnih varnostnih zahtev v informacijske in omrežne sisteme ter izvajanje pilotnih ukrepov prek tečajev o varnosti v šolah vseh vrst in stopenj;

— vzpostavitev zanesljivega in priznanega pravnega in zakonodajnega okvira na ravni EU; ta okvir, uporabljen za informacijsko tehnologijo in omrežja, bi omogočil prehod z informacijske varnosti na informacijsko zavarovanje;

— okrepitev evropskih in nacionalnih mehanizmov ocenjevanja tveganj in večjo zmogljivost uporabe zakonodajnih in urejevalnih predpisov, da bi onemogočili storilce informacijskih kaznivih dejanj, storjenih na področju zasebnosti in zbirk podatkov;

— ukrepe, namenjene preprečevanju pojavljanja informacijskih monokultur, ki jih je lažje „piratizirati“; podporo diverzificiranim večkulturnim inovacijam, namenjenim uresničevanju Enotnega evropskega informacijskega prostora *(SEIS, Single European Information Space)*.

4.3.2 EESO meni, da bi bilo primerno vzpostaviti nacionalno kontaktno točko za varnost IKT med direktorati *(ICT-Security Focal Point, inter DG)* ([23]). Kontaktna točka bi omogočala delovanje:

— na notranji ravni služb Komisije;

— na ravni posameznih držav, z večsektorskimi rešitvami za vidike interoperabilnosti, upravljanja identitete, varstva zasebnosti, svobode dostopa do informacij in storitev, kar so minimalne varnostne zahteve;

— na mednarodni ravni, da bi lahko v različnih kontekstih — npr. OZN, G8, OVSE, ISO — zagotovili enotno, evropsko stališče.

4.4 *Za okrepljene in odgovorne ukrepe usklajevanja na ravni EU*

4.4.1 EESO namenja velik pomen tudi vzpostavitvi Evropskega omrežja za varnost omrežij in informacij *(European Network and Information Security Network)*, prek katerega bi bilo mogoče spodbujati raziskave, študije in delavnice o varnostnih mehanizmih in o njihovi interoperabilnosti, o napredni kriptografiji in varstvu zasebnosti.

4.4.2 EESO meni, da bi bilo treba za ta sektor, ki je zelo občutljiv, čim bolj izboljšati vlogo evropskih raziskav, in sicer s primernim povzetkom vsebine:

— *Evropskega programa raziskav varnosti* (ESRP) ([24]), ki je del *Sedmega okvirnega programa raziskav, tehnološkega razvoja in predstavitev*;

([21]) Glej opombo 19, alinejo 3.

([22]) ETSI = Evropski inštitut za telekomunikacijske standarde *(European Telecomunications Standards Institute)*; glej zlasti delavnico z dne 16. in 17. januarja 2006. ETSI je med drugim pripravil tudi specifikacije o nezakonitih prisluškovanjih (TS 102 232; 102 233; 102 234, o dostopu do interneta prek brezžičnih omrežij Wireless LAN (TR 102 519), o elektronskih podpisih, in razvil varnostne algoritme za GSM, GPRS in UMTS.

([23]) To *kontaktno točko med generalnimi direktorati* bi lahko financirali v okviru prednostne naloge IST specifičnega programa *Sodelovanje* 7. okvirnega programa raziskav, tehnološkega razvoja in predstavitev, ali pa v okviru *Evropskega programa raziskav varnosti* (ESRP).

([24]) Glej: Sedmi okvirni program raziskav, tehnološkega razvoja in predstavitev ES, posebni program sodelovanja; tematska prednost raziskave varnosti s proračunom 1,35 milijarde eurov za obdobje 2007-2013.

— programa *Safer Internet Plus*

— in *Evropskega programa za zaščito kritičnih infrastruktur*, (EPCIP) ([25]).

4.4.3 Tem predlogom bi lahko dodali uvedbo „evropskega dneva varnega računalnika“, podprtega z nacionalnimi kampanjami vzgoje v šolah in z informacijami, namenjenimi potrošnikom, o postopkih za zaščito informacij prek računalnikov, ter seveda o tehnološkem napredku na širokem in nenehno spreminjajočem se področju računalništva.

4.4.4 Odbor je večkrat poudaril, da je „pripravljenost podjetij za uporabo IKT odvisna od tega, za kako varno ocenijo elektronsko poslovanje. Podobno je tudi pripravljenost uporabnikov, da na spletno stran vnesejo številko kreditne kartice, močno odvisna od njihove ocene varnosti transakcij“ ([26]).

4.4.5 Odbor je prepričan, da je zaradi velikanskega potenciala rasti tega sektorja treba izvajati specifične ukrepe, sedanje pa prilagoditi novim dogajanjem. Evropske pobude na področju varnosti informacij je treba povezati s pomočjo celostne strategije, odpraviti meje med sektorji in zagotavljati homogeno ter varno širjenje IKT v družbi.

4.4.6 Odbor meni, da nekatere pomembne strategije, kakršna je ta, napredujejo prepočasi zaradi birokratskih in kulturnih težav, ki jih države članice povzročajo, ko gre za nujne odločitve, ki jih je treba sprejeti na ravni Skupnosti.

4.4.7 Odbor meni tudi, da viri Skupnosti ne zadoščajo za uresničitev številnih, nujnih projektov, ki lahko dajo otipljive odgovore na nove probleme globalizacije samo, če so uresničeni na ravni Skupnosti.

4.5 *Za večje jamstvo EU pri varstvu potrošnikov*

4.5.1 Odbor je seznanjen s tem, da so države članice sprejele tehnološke varnostne ukrepe in postopke za upravljanje varnosti v skladu z lastnimi zahtevami ter da se osredotočajo na različne vidike. Tudi zato je na vprašanja v zvezi z varnostjo težko dati enopomenski in učinkovit odgovor. Z izjemo nekaterih upravnih omrežij ni sistematičnega čezmejnega sodelovanja med državami članicami, čeprav se vprašanj varnosti posamezne države ne morejo lotevati neodvisno druga od druge.

4.5.2 Odbor nadalje opozarja, da je Svet — z okvirnim sklepom 2005/222/PNZ — sprejel okvir za sodelovanje med pravosodnimi in drugimi pristojnimi oblastmi, za zagotovitev koherentnega pristopa držav članic s približevanjem njihovih kazenskih zakonodaj na področju napadov na informacijske sisteme pri:

— nezakonitem dostopu do informacijskih sistemov,

— nezakonitem poseganju v informacijski sistem, z namernim resnim oviranjem ali prekinitvijo njegovega delovanja,

— nezakonitem poseganju v računalniške podatke v informacijskem sistemu, z njihovim namernim brisanjem, poškodovanjem, poslabšanjem, spremembo ali odstranitvijo, ali tako, da se onemogoči dostop,

— nagovarjanju, spodbujanju ali soudeležbi pri omenjenih kaznivih dejanjih.

4.5.3 Okvirni sklep nadalje navaja merila za opredelitev odgovornosti pravnih oseb in morebitne kazni, ki jih je mogoče uporabiti, če je ugotovljena odgovornost ([27]).

4.5.4 V okviru dialoga z organi oblasti držav članic Odbor podpira predlog Komisije, da ti organi začnejo z vajo primerjalne ocene lastnih nacionalnih politik, povezanih z varnostjo omrežij in informacijskih sistemov, vključno s specifičnimi politikami za javni sektor. Ta predlog je naveden že v mnenju EESO iz leta 2001.

4.6 *Za bolj razširjeno varnostno kulturo*

4.6.1 Glede vključevanja industrije informacijske varnosti, mora ta — za varstvo pravic svojih odjemalcev do zasebnosti in zaupnosti — dejansko jamčiti, da so uporabljeni sistemi stvarnega nadzora njenih instalacij in šifriranja sporočil v skladu z doseženim tehnološkim razvojem ([28]).

([25]) COM(2005) 576 z dne 17.11.2005.
([26]) Glej opombo 19, alinejo 2.
([27]) Glej opombo 19, alinejo 4.
([28]) Glej: direktivo 97/66/ES o ravnanju z osebnimi podatki na telekomunikacijskem področju (UL L 24 z dne 30.1.1998).

4.6.2 V zvezi s kampanjami ozaveščanja Odbor meni, da je temeljnega pomena vzpostavitev resnične „varnostne kulture“, ki bo v celoti v skladu s svobodo obveščanja, komuniciranja in izražanja. Številni uporabniki se ne zavedajo vseh tveganj, povezanih z računalniškim piratstvom, mnogi ponudniki storitev, prodajalci ali dobavitelji pa niso zmožni oceniti obstoja in obsega ranljivih vidikov.

4.6.3 Čeprav je prednostni cilj varstvo zasebnosti in osebnih podatkov, imajo potrošniki tudi pravico, da so zares učinkovito zaščiteni pred nedopustnim zbiranjem podatkov o njih s pomočjo „vohunskih“ računalniških programov (*spyware* in *web bug*) ali na druge načine. Treba bi bilo tudi zavreti *spamming* (množično razpošiljanje nezaželenih elektronskih sporočil) ([29]), ki pogosto izhaja iz teh nedopustnih dejanj. Ti vdori svojim žrtvam namreč povzročajo stroške ([30]).

4.7 *Za močnejšo in dejavnejšo agencijo EU*

4.7.1 Odbor je naklonjen bolj izostreni in okrepljeni vlogi *Evropske agencije za varnost omrežij in informacij* (ENISA), tako glede ozaveščanja kot tudi — in predvsem — delovanja pri obveščanju in usposabljanju ponudnikov in uporabnikov, kot je sicer EESO pred kratkim že navedel v enem svojih mnenj o zagotavljanju javnih storitev elektronskih komunikacij ([31]).

4.7.2 Kar se tiče predlagane dejavnosti za ozaveščanje vseh skupin zainteresiranih, se zdi, da so te dejavnosti usmerjene k strogemu upoštevanju načela subsidiarnosti. Zanje so namreč odgovorne države članice in zasebni sektor, odvisno od posebnih odgovornosti.

4.7.3 ENISA bi lahko s pridom uporabljala prispevke, ki jih ponuja evropsko omrežje *European Network and Information Security Network*, za organiziranje povezanih dejavnosti, tako kot večjezični spletni portal Skupnosti za opozarjanje na področju informacijske varnosti, za posameznikom prilagojene in interaktivne informacije s poenostavljenim jezikom, predvsem ko gre za posamezne uporabnike različnih starosti ter za mala in srednjevelika podjetja.

V Bruslju, 16. februarja 2007.

Predsednik

Evropskega ekonomsko-socialnega odbora

Dimitris DIMITRIADIS

([29]) V franc.: *pollu postage*.

([30]) Glej: mnenja EESO o *Omrežjih za elektronske komunikacije* (UL C 123 del 25.4.2001, str. 50), *Elektronsko trgovanje* (UL C 169 z dne 16.6.1999, str. 36) in *Posledice elektronskega trgovanja za skupni trg* (UL C 123 z dne 25.4.2001, str. 1).

([31]) Glej opombo 19, alinejo 1.