EUROOPAN PARLAMENTTI 2009 - 2014

Istuntoasiakirja

A7-0167/2012

16.5.2012

MIETINTÖ

elintärkeiden tietoinfrastruktuureiden suojaamisesta – saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta
(2011/2284(INI))

Teollisuus-, tutkimus- ja energiavaliokunta

Esittelijä: Ivailo Kalfin

SISÄLTÖ

Sivu

EUROOPAN PARLAMENTIN PÄÄTÖSLAUSELMAESITYS

elintärkeiden tietoinfrastruktuureiden suojaamisesta – saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta
(2011/2284(INI))

Euroopan parlamentti, joka

– ottaa huomioon 5. toukokuuta 2010 antamansa päätöslauselman Euroopan uudesta digitaalisesta asialistasta: 2015.eu[1],

– ottaa huomioon 15. kesäkuuta 2010 antamansa päätöslauselman internetin hallinnosta tästä eteenpäin[2],

– ottaa huomioon 6. heinäkuuta 2011 antamansa päätöslauselman laajakaistasta Euroopassa: investointi digitaalivetoiseen kasvuun[3],

– ottaa huomioon työjärjestyksen 48 artiklan,

– ottaa huomioon teollisuus-, tutkimus- ja energiavaliokunnan mietinnön sekä kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnan lausunnon (A7-0167/2012),

A. ottaa huomioon, että tieto- ja viestintätekniikka (TVT) kykenee hyödyntämään täyttä valmiuttaan talouden ja yhteiskunnan edistämiseen vain, jos käyttäjät luottavat sen turvallisuuteen ja häiriönsietokykyyn ja jos esimerkiksi tietosuojakysymyksiä sekä teollis- ja tekijänoikeuksia koskeva lainsäädäntö pannaan tuloksekkaasti täytäntöön internet-ympäristössä;

B. ottaa huomioon, että internetin sekä TVT:n vaikutus eri näkökohtiin kansalaisten elämässä kasvaa nopeasti ja on ratkaiseva tekijä sosiaalisessa kanssakäymisessä, kulttuurin rikastamisessa ja talouskasvussa;

C. katsoo, että TVT:n ja internetin turvallisuus on laaja-alainen käsite, jolla on yleisesti vaikutusta taloudellisiin, sosiaalisiin, teknologisiin ja sotilaallisiin näkökohtiin, mikä edellyttää vastuualojen selkeää määrittämistä ja erittelyä sekä vankkaa kansainvälistä yhteistyömekanismia;

D. ottaa huomioon, että digitaalistrategiaa koskevassa EU:n lippulaivahankkeessa pyritään vahvistamaan Euroopan kilpailukykyä vahvistetun TVT:n perusteella ja luomalla edellytykset teknologian alan suurelle kasvulle ja työpaikkojen syntymiselle;

E. ottaa huomioon, että yksityinen sektori on edelleen ensisijainen investoija, omistaja ja hallinnoija tietoturvatuotteiden, palvelujen, sovellusten ja infrastruktuurin alalla, johon on viimeisen vuosikymmenen aikana investoitu miljardeja euroja; katsoo, että tätä osallisuutta olisi vahvistettava asianmukaisilla poliittisilla strategioilla julkisten,

[1] EUVL C 81E, 15.3.2011, s.45.
[2] EUVL C 236E, 12.8.2011, s. 33.
[3] Hyväksytyt tekstit, P7_TA(2011)0322.

yksityisten tai julkisten ja yksityisten yhdessä omistamien tai hallinnoimien infrastruktuurien häiriönsietokyvyn edistämiseksi;

F. katsoo, että TVT-verkkojen, palvelujen ja tekniikan erittäin korkean tason turvallisuuden ja häiriönsietokyvyn kehittämisen olisi lisättävä Euroopan talouden kilpailukykyä sekä parantamalla verkkoriskien arviointia ja hallinnointia että tarjoamalla EU:n taloudelle yleisesti entistä vankempia tietoinfrastruktuureja innovoinnin ja kasvun tukemiseksi ja antamalla yrityksille tilaisuuden parantaa tuottavuuttaan;

G. ottaa huomioon, että lainvalvontaviranomaisten verkkorikoksia – verkkohyökkäykset sekä muut verkossa tapahtuvat rikokset – koskevat tiedot osoittavat rikosten lisääntyneen suuresti Euroopan eri valtioissa; toteaa kuitenkin, että niin lainvalvontaviranomaisilta kuin kansallisilta tietoturvaryhmiltä (CERT) saadut tilastollisesti edustavat tiedot verkkohyökkäyksistä ovat edelleen niukkoja ja että niitä on yhdisteltävä vastaisuudessa paremmin, sillä näin lainvalvontaviranomaiset kaikkialla EU:ssa voivat puuttua niihin vahvemmin ja tiedottaa paremmin lainsäädännöllisistä toimista alati kehittyvien verkkouhkien osalta;

H. toteaa, että tietoturvan asianmukainen taso on elintärkeä internetpohjaisten palvelujen merkittävälle laajentumiselle;

I. katsoo, että viimeaikaiset verkkoturvallisuuspoikkeamat, häiriöt ja hyökkäykset EU:n toimielinten, teollisuuden ja jäsenvaltioiden tietoinfrastruktuuria vastaan osoittavat, että on luotava täysimääräiseen kansainväliseen yhteistyöhön ja jäsenvaltioiden välisiin sietokykyä koskeviin vähimmäisnormeihin perustuva vakaa, innovatiivinen ja toimiva järjestelmä elintärkeiden tietoinfrastruktuureiden suojaamiseksi;

J. katsoo, että etäresurssipalvelujen kaltaisten TVT:n uusien mahdollisuuksien nopea kehitys edellyttää voimakasta keskittymistä turvallisuuteen, jotta voidaan täysimääräisesti hyödyntää teknologisten saavutusten tarjoamat hyödyt;

K. toteaa vaatineensa toistuvasti tietosuojan ja tietoturvan, internetin riippumattomuuden sekä teollis- ja tekijänoikeuksien suojan tiukkojen standardien soveltamista;

I. Toimenpiteet elintärkeiden tietoinfrastruktuureiden suojan vahvistamiseksi kansallisella ja unionin tasolla

1. suhtautuu myönteisesti siihen, että jäsenvaltiot ovat toteuttaneet elintärkeiden tietoinfrastruktuureiden suojaamista koskevan eurooppalaisen ohjelman, elintärkeiden infrastruktuureiden varoitusjärjestelmän (CIWIN) perustaminen mukaan lukien;

2. katsoo, että elintärkeiden tietoinfrastruktuurien suojaamistoimien avulla lisätään kansalaisten yleistä turvallisuutta ja parannetaan myös kansalaisten käsitystä turvallisuudesta sekä vahvistetaan heidän luottamustaan toimenpiteisiin, joita hallitus toteuttaa heidän suojaamisekseen;

3. toteaa, että komissio harkitsee neuvoston direktiivin 2008/114/EY[1] tarkistamista, ja peräänkuuluttaa näytön esittämistä direktiivin tehokkuudesta ja sen vaikutuksista ennen lisäaskelten ottamista; peräänkuuluttaa direktiivin soveltamisalan laajentamista etenkin sisällyttämällä siihen TVT-ala ja rahoituspalvelut; edellyttää myös, että otetaan huomioon terveydenhuollon, elintarvikealan ja vesihuoltojärjestelmien, ydinalan tutkimuksen ja teollisuuden kaltaiset alat (siltä osin kuin erityissäännökset eivät kata niitä); katsoo, että näiden alojen pitäisi myös hyötyä eri alojen välisestä lähestymistavasta, joka on otettu käyttöön elintärkeiden infrastruktuureiden varoitusjärjestelmän myötä (käsittää yhteistyön, varoitusjärjestelmän ja parhaiden käytäntöjen vaihdon);

4. korostaa eurooppalaisen tutkimuksen jatkuvan integroinnin kehittämisen ja varmistamisen merkitystä eurooppalaisen huippuosaamisen ylläpitäjänä ja vahvistajana elintärkeiden tietoinfrastruktuureiden suojaamisessa;

5. vaatii sietokykyä koskevien vähimmäisnormien säännöllistä päivittämistä valmiuksien ja reagointikyvyn lisäämiseksi, jotta normit suojaisivat häiriöiltä, poikkeamilta, tuhoamisyrityksiltä tai hyökkäyksiltä, kuten liian heikoista infrastruktuureista tai riittämättömästi suojatuista päätekeskuksista johtuvilta hyökkäyksiltä, koska kansalliset ja EU:n elintärkeät tietoinfrastruktuurit ovat yhteydessä toisiinsa ja toisistaan erittäin riippuvaisia ja koska ne ovat arkaluonteisia, strategisia ja haavoittuvia;

6. korostaa tietoturvallisuusnormien ja -protokollien merkitystä ja suhtautuu myönteisesti CEN:lle, Cenelecille ja ETSI:lle vuonna 2011 annettuun toimeksiantoon luoda turvallisuusnormit;

7. odottaa, että elintärkeiden tietoinfrastruktuurien omistajat ja toiminnanharjoittajat antavat käyttäjille mahdollisuuden käyttää tarvittaessa asianmukaisia keinoja suojautuakseen vihamielisiltä hyökkäyksiltä ja/tai häiriöiltä ja tarvittaessa auttavat tässä niin ihmisten suorittaman kuin automaattisen valvonnan avulla;

8. kannattaa julkisten ja yksityisten sidosryhmien yhteistyötä unionin tasolla ja rohkaisee niitä kehittämään ja ottamaan käyttöön turvallisuus- ja häiriönsietokykynormeja kansallisten ja eurooppalaisten elintärkeiden tietoinfrastruktuurien osalta siviili- ja julkisalalla, yksityisalalla sekä yksityisen ja julkisen sektorin yhteisellä alalla;

9. korostaa yleiseurooppalaisten laajamittaisten verkkoturvallisuusharjoitusten sekä yhtenäisten uhka-arviota koskevien vaatimusten määrittämisen merkitystä;

10. pyytää komissiota arvioimaan yhteistyössä jäsenvaltioiden kanssa elintärkeiden tietoinfrastruktuurien suojaamista koskevan toimintasuunnitelman täytäntöönpanoa; kehottaa jäsenvaltioita perustamaan hyvin toimivia kansallisia/valtiollisia tietotekniikan kriisiryhmiä (CERT), kehittämään kansallisia verkkoturvallisuusstrategioita, järjestämään säännöllisiä kansallisia ja yleiseurooppalaisia verkkoturvallisuuspoikkeamaharjoituksia, kehittämään kansallisia verkkoturvallisuuspoikkeamavarautumissuunnitelmia ja edistämään osaltaan Euroopan verkkoturvallisuuspoikkeamavarautumissuunnitelman kehittämistä vuoden 2012 loppuun mennessä;

[1] EUVL L 345, 23.12.2008, s. 75.

11. suosittaa, että otetaan käyttöön operaattoreita koskevia turvallisuussuunnitelmia tai vastaavia toimia kaikkien elintärkeiden eurooppalaisten tietoinfrastruktuurien osalta ja että nimitetään turvallisuudesta vastaavia yhteyshenkilöitä;

12. on tyytyväinen tietojärjestelmiin kohdistuvista hyökkäyksistä tehdyn neuvoston puitepäätöksen 2005/222/YOS[1] hiljattaisen tarkistamiseen; panee merkille, että EU:n toimia suurten verkkohyökkäysten torjumiseksi on koordinoitava sisällyttämällä toimintaan Euroopan verkko- ja tietoturvavirasto ENISA, jäsenvaltioiden CERT-ryhmät ja tulevan eurooppalaisen CERT-ryhmän toimivalta;

13. katsoo, että ENISAlla voi olla tärkeä asema EU:n tasolla elintärkeiden tietoinfrastruktuureiden suojaamisessa, koska se voi tarjota teknistä asiantuntemusta jäsenvaltioille, EU:n toimielimille ja elimille sekä laatia raportteja ja analyysejä EU:n ja maailmanlaajuisten tietojärjestelmien turvallisuudesta;

II. EU:n lisätoimet internetin vankan turvallisuuden takaamiseksi

14. kehottaa ENISAa koordinoimaan ja toteuttamaan vuosittain internetiä koskevia EU:n turvallisuustietoisuuskuukausia, jotta jäsenvaltiot ja unionin kansalaiset kiinnittäisivät erityistä huomiota verkkoturvallisuuteen liittyviin kysymyksiin;

15. tukee ENISAa digitaalistrategian tavoitteiden mukaisesti sen toteuttaessa tehtäviään verkon tietoturvan osalta ja erityisesti sen tarjotessa ohjausta ja neuvonantoa jäsenvaltioille siitä, kuinka niiden CERT-ryhmien perusvalmiudet täytetään, sekä sen tukiessa parhaiden käytäntöjen vaihtoa luottamuksen ilmapiiriä kehittämällä; kehottaa virastoa kuulemaan asianomaisia sidosryhmiä vastaavanlaisten verkkoturvatoimenpiteiden määrittämiseksi yksityisten verkkojen ja infrastruktuurien omistajille/toiminnanharjoittajille sekä auttamaan komissiota ja jäsenvaltioita kansallisia ja Euroopan CERT-ryhmiä sekä infrastruktuurien omistajia/toiminnanharjoittajia koskevien tietoturvavarmentamisjärjestelmien, toimintanormien ja yhteistyökäytäntöjen kehittämisessä ja käyttöönotossa ja tarvittaessa määrittämään teknologianeutraaleja yhteisiä vähimmäisvaatimuksia;

16. on tyytyväinen nykyiseen ehdotukseen ENISAn toimivaltuuksien tarkistamisesta, erityisesti niiden laajentamisesta ja viraston tehtävien laajentamisesta; katsoo, että asiantuntemuksen ja analyysien muodossa jäsenvaltioille tarjoamansa avun lisäksi ENISAn olisi voitava hallinnoida useita toimeenpanotehtäviä EU:n tasolla ja yhteistyössä vastaavien yhdysvaltalaisten elinten kanssa verkko- ja tietoturvaloukkausten ehkäisemiseksi ja paljastamiseksi sekä jäsenvaltioiden välisen yhteistyön edistämiseksi; korostaa, että ENISAlle voitaisiin asetuksen nojalla antaa myös lisävastuuta internethyökkäyksiin reagoimista varten, sillä se lisäisi nykyisten kansallisten reagointimekanismien arvoa;

17. on tyytyväinen vuosien 2010 ja 2011 kaikkialle unionissa toteutettujen ja ENISA:n valvomien yleiseurooppalaisten verkkoturvallisuusharjoitusten tuloksiin, kun pyrittiin auttamaan jäsenvaltioita suunnittelemaan, ottamaan käyttöön ja testaamaan yleiseurooppalaista varautumissuunnitelmaa; kehottaa ENISA:a säilyttämään tällaiset

[1] EUVL L 69, 16.3.2005, s. 67.

harjoitukset suunnitelmissaan ja ottamaan tarvittaessa vaiheittain mukaan yksityisiä toiminnanharjoittajia yleisten verkkoturvavalmiuksien lisäämiseksi Euroopassa; toivoo toiminnan laajenevan kansainvälisesti samanhenkisiin kumppaneihin;

18. kehottaa jäsenvaltioita laatimaan kansallisia verkkoturvallisuutta koskevia varautumissuunnitelmia, joihin pitäisi sisällyttää keskeisiä tekijöitä, kuten asiaankuuluvat yhteyspisteet sekä avunantoa, rajoittamista ja korjaamista koskevat säännökset siltä varalta, että tapahtuu alueellisia, kansallisia tai rajat ylittäviä vaikutuksia aiheuttavia tietoverkkohäiriöitä tai -hyökkäyksiä; toteaa, että jäsenvaltioiden pitäisi myös ottaa käyttöön kansallisella tasolla asianmukaisia koordinointimekanismeja tai -rakenteita, jotka auttaisivat varmistamaan paremman koordinoinnin toimivaltaisten kansallisten viranomaisten välillä ja tekisivät niiden toimista johdonmukaisempia;

19. esittää, että komissio ehdottaisi EU:n verkkoturvallisuuspoikkeamavarautumissuunnitelman avulla sitovia toimenpiteitä kansallisten/hallitusten CERT-ryhmien teknisten tehtävien ja ohjaustehtävien koordinoimiseksi paremmin unionissa;

20. kehottaa komissiota ja jäsenvaltioita ryhtymään tarvittaviin toimenpiteisiin elintärkeiden infrastruktuureiden suojaamiseksi tietoverkkohyökkäyksiltä ja tarjoamaan keinoja, joiden avulla voidaan estää hermeettisesti pääsy elintärkeään infrastruktuuriin, mikäli suora tietoverkkohyökkäys uhkaisi vakavasti sen moitteetonta toimintaa;

21. odottaa EU:n CERT-ryhmän toiminnan täysimääräistä käynnistymistä, sillä se on merkittävä tekijä EU:n toimielimiin kohdistuvien tahallisten ja vihamielisten verkkohyökkäysten ehkäisemisessä, paljastamisessa, torjumisessa ja korjaamisessa;

22. suosittaa, että komissio ehdottaisi sitovia toimenpiteitä, joilla määrättäisiin vähimmäistason turvallisuus- ja häiriönsietokykynormit ja voitaisiin tehostaa kansallisten CERT-ryhmien välistä koordinointia;

23. kehottaa jäsenvaltioita ja EU:n toimielimiä varmistamaan hyvin toimivien CERT-ryhmien olemassaolon sekä sen, että niillä on hyväksyttyihin parhaisiin käytäntöihin perustuvat vähimmäistason turvallisuus- ja häiriönsietokykyvalmiudet; korostaa, että jäsenvaltioiden ja EU:n toimielimien on varmistettava hyvin toimivien CERT-ryhmien olemassaolo, ja että niillä on oltava tietyt ennalta määrätyt sitovat vähimmäistason turvallisuus- ja häiriönsietokykyvalmiudet; korostaa, että kansallisten CERT-ryhmien olisi oltava osa tehokasta verkostoa, jossa asiaankuuluvaa tietoa vaihdetaan tarvittavien luottamuksellisuutta koskevien vaatimusten mukaisesti; kehottaa perustamaan jokaisen jäsenvaltion osalta elintärkeitä tietoinfrastruktuureja koskevat jatkuvat 24/7-palvelut sekä laatimaan yhteisen eurooppalaisen hätätilaprotokollan, jota sovelletaan kansallisten yhteispisteiden välillä;

24. korostaa, että luottamuksen rakentaminen ja yhteistyön edistäminen jäsenvaltioiden välillä on ratkaisevan tärkeää tietojen, kansallisten verkkojen ja infrastruktuurien suojelemiseksi; kehottaa komissiota ehdottamaan yhteistä menettelyä yhteisen lähestymistavan määrittämiseksi ja laatimiseksi rajat ylittäviin TVT-uhkiin vastaamiseksi, edellyttäen että jäsenvaltiot toimittavat komissiolle geneeristä tietoa elintärkeiden tietoinfrastruktuuriensa riskeistä, uhista ja haavoittuvuudesta;

25. suhtautuu myönteisesti komission aloitteeseen, joka koskee eurooppalaisen tiedonjako- ja hälytysjärjestelmän kehittämistä vuoteen 2013 mennessä;

26. suhtautuu myönteisesti komission alulle panemiin, internetin turvallisuutta ja elintärkeiden tietoinfrastruktuureiden suojaamista koskeviin sidosryhmien kuulemisiin, kuten sietokykyä käsittelevän eurooppalaisen julkis-yksityisen kumppanuuden; tunnustaa TVT:n myyjien jo nyt merkittävän osallistumisen ja sitoutumisen näihin toimiin ja kannustaa komissiota jatkamaan ponnisteluja kannustaakseen tiedemaailmaa ja TVT:n käyttäjien järjestöjä toimimaan aktiivisemmin; kannustaa komissiota myös edistämään verkkoturvallisuuskysymyksiä koskevaa sidosryhmien välistä rakentavaa vuoropuhelua; kannattaa digitaalistrategian yleiskokouksen kehittämistä edelleen elintärkeiden tietoinfrastruktuureiden suojaamisen hallintokehyksenä;

27. suhtautuu myönteisesti Euroopan jäsenvaltiofoorumin tähän mennessä tekemään työhön laadittaessa toimialakohtaisia kriteerejä elintärkeiden EU:n infrastruktuurien määrittelemiseksi erityisesti kiinteiden ja matkaviestintäverkkojen osalta ja käsiteltäessä internetin sietokykyä ja vakautta koskevia EU:n periaatteita ja suuntaviivoja; odottaa innokkaasti yksimielisyyden rakentamisen jatkamista jäsenvaltioiden välillä ja kannustaa tässä yhteydessä foorumia täydentämään nykyistä aineelliseen omaisuuteen keskittyvää lähestymistapaa pyrkimyksillä kattaa myös loogiset infrastruktuurivarat, jotka virtualisaation ja etäteknologian kehittyessä tulevat yhä merkittävämmiksi elintärkeiden tietoinfrastruktuureiden tehokkaan suojaamisen kannalta;

28. ehdottaa, että komissio käynnistäisi julkisen yleiseurooppalaisen koulutusaloitteen, jossa keskityttäisiin niin yksityisten kuin yritysten loppukäyttäjien koulutukseen ja tietoisuuden lisäämiseen internetin ja kannettavien TVT-laitteiden mahdollisista uhista kaikilla käyttäjäketjun kaikilla tasoilla sekä edistämään turvallisempaa toimintaa verkossa; palauttaa tämän osalta mieleen vanhentuneisiin laitteisiin ja ohjelmistoihin liittyvät riskit;

29. kehottaa jäsenvaltioita komission tuella vahvistamaan tietoturvaopetusta ja -koulutusta koskevia kansallisille lainvalvontaviranomaisille ja oikeusviranomaisille sekä asianomaisille EU:n virastoille suunnattuja ohjelmia;

30. kannattaa eurooppalaisen opinto-ohjelman luomista tietoturva-alan akateemisille asiantuntijoille, koska sillä olisi myönteinen vaikutus EU:n asiantuntemukseen ja valmiuksiin alati kehittyvän kyberavaruuden ja siihen liittyvien uhkien osalta;

31. kannattaa verkkoturvallisuuskoulutusta (tohtoriopiskelijoiden harjoittelut, korkeakouluopinnot, työpajat, opintoharjoittelut jne.) ja erityisiä koulutusharjoituksia elintärkeiden tietoinfrastruktuureiden suojaamisesta;

32. kehottaa komissiota ehdottamaan vuoden 2012 loppuun mennessä selkeään terminologiaan perustuvaa kattavaa internetin turvallisuutta koskevaa unionin strategiaa; katsoo, että internetin turvallisuusstrategian pitäisi tähdätä suojatun ja sietokykyisen infrastruktuurin ja avoimien standardien tukemana sellaisen kyberavaruuden luomiseen, joka edistää innovointia ja vaurautta vapaan tietovirran kautta samalla kun varmistetaan yksityisyyden ja muiden kansalaisvapauksien vankka suoja; katsoo, että strategiassa pitäisi esittää yksityiskohtaisesti tarvittavat periaatteet, tavoitteet, menetelmät, välineet ja toimintatavat (sekä sisäiset että ulkoiset) kansallisten ja unionin ponnistelujen

virtaviivaistamiseksi ja vahvistaa häiriönsietokykyä koskevat vähimmäisnormit jäsenvaltioissa, jotta varmistetaan turvallinen, keskeytymätön, vakaa ja sietokykyinen palvelu riippumatta siitä, liittyykö se elintärkeään infrastruktuuriin vai yleiseen internetin käyttöön;

33. korostaa, että komission tulevassa "internetin turvallisuusstrategiassa" olisi otettava erityisesti huomioon elintärkeiden tietoinfrastruktuureiden suojaamista koskeva työ ja pyrittävä tietoverkkoturvallisuuden osalta kokonaisvaltaiseen ja järjestelmälliseen lähestymistapaan sisällyttämällä strategiaan ennaltaehkäiseviä toimenpiteitä, kuten turvatoimia koskevat vähimmäisstandardit tai yksittäisten käyttäjien, yritysten ja julkisten laitosten opettaminen, ja reaktiivisia toimenpiteitä, kuten rikosoikeudellisia, siviilioikeudellisia ja hallinnollisia seuraamuksia;

34. pyytää komissiota ehdottamaan vankkaa mekanismia internetin turvallisuusstrategian täytäntöönpanon koordinoimiseksi ja säännölliseksi päivittämiseksi; katsoo, että mekanismia olisi tuettava riittävin hallinnollisin resurssein, asiantuntijaresurssein ja taloudellisin varoin ja että sillä olisi oltava valmiudet helpottaa EU:n kantojen laatimista suhteissa niin kansallisiin kuin kansainvälisiin sidosryhmiin internetin turvallisuuteen liittyvissä asioissa;

35. kehottaa komissiota ehdottamaan EU:n puitteita ilmoituksille, jotka koskevat elintärkeillä aloilla, kuten energia-, liikenne-, vesi- ja elintarvikehuoltoaloilla sekä TVT-alalla ja rahoituspalveluissa tapahtuneita turvallisuusrikkomuksia, jotta jäsenvaltioiden toimivaltaiset viranomaiset ja käyttäjät saavat tiedon verkkoturvallisuuspoikkeamista, verkkohyökkäyksistä ja häiriöistä;

36. kehottaa komissiota parantamaan tilastollisesti edustavien tietojen saatavuutta verkkohyökkäysten aiheuttamista kustannuksista EU:ssa, jäsenvaltioissa ja teollisuudessa (erityisesti rahoituspalveluissa ja TVT-alalla) vahvistamalla tietoverkkorikollisuutta käsittelevän eurooppalaisen keskuksen, joka on määrä perustaa vuoteen 2013 mennessä, CERT-ryhmien ja muiden komission aloitteiden, kuten eurooppalaisen tiedonjako- ja hälytysjärjestelmän tietojenkeruuvalmiuksia, jotta voidaan varmistaa järjestelmällinen raportointi ja tietojen jakaminen verkkohyökkäyksistä ja muista verkkorikollisuuden muodoista, jotka haittaavat eurooppalaista teollisuutta ja jäsenvaltioita, ja tehostaa lainvalvontaa;

37. kannattaa kansallisten yksityisten sektorien ja ENISAn tiivistä yhteistyötä ja vuorovaikutusta, jotta kansalliset/valtiolliset CERT-ryhmät voidaan kytkeä eurooppalaisen tiedonjako- ja hälytysjärjestelmän (EISAS) kehittämiseen;

38. huomauttaa, että tärkein internetin turvallisuutta lisäävän tekniikan kehittämisen ja käytön vauhdittaja on TVT-ala; muistuttaa, että EU:n politiikassa on vältettävä Euroopan internettalouden kasvun haittaamista ja että politiikkaan on sisällyttävä tarvittavat kannustimet, jotta liike-elämän sekä julkisen ja yksityisen sektorin kumppanuuksien potentiaali saadaan hyödynnettyä täysimääräisesti; suosittaa tutkimaan muita teollisuudelle tarjottavia kannustimia, jotta se kehittäisi entistä vankempia direktiivin 2008/114/EY mukaisesti operaattoreita koskevia vankkoja turvallisuussuunnitelmia;

39. kehottaa komissiota esittämään lainsäädäntöehdotuksen yhä uusien verkkohyökkäyksen muotojen kriminalisoimiseksi (mm. tiedon tuulastaminen (spear-phishing), sähköiset petokset jne.);

III. Kansainvälinen yhteistyö

40. muistuttaa, että kansainvälinen yhteistyö on tärkein väline toimivien verkkoturvallisuustoimenpiteiden käyttöönotossa; myöntää, että tällä hetkellä EU ei ole aktiivisesti ja jatkuvasti mukana verkkoturvallisuuteen liittyvissä kansainvälisissä yhteistyöprosesseissa ja vuoropuhelussa; kehottaa komissiota ja Euroopan ulkosuhdehallintoa (EUH) käynnistämään rakentavan vuoropuhelun kaikkien samoin ajattelevien maiden kanssa yhteisen näkökulman ja toimintatapojen kehittämiseksi, jotta internetin ja elintärkeän infrastruktuurin häiriönsietokykyä saadaan parannettua; katsoo, että samalla EU:n pitäisi sisällyttää internetin turvallisuutta koskevat kysymykset pysyvästi ulkosuhteidensa soveltamisalaan muun muassa suunniteltaessa erilaisia rahoitusvälineitä tai sitouduttaessa kansainvälisiin sopimuksiin, joihin liittyy arkaluonteisten tietojen vaihtoa tai varastointia;

41. panee merkille vuonna 2001 tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen myönteiset saavutukset; korostaa, että Euroopan ulkosuhdehallinnon olisi sekä rohkaistava useampia valtioita allekirjoittamaan ja ratifioimaan yleissopimus että luotava kahdenvälisiä ja monenvälisiä sopimuksia internetin turvallisuudesta ja sietokyvystä samanhenkisten kansainvälisten kumppanien kanssa;

42. huomauttaa, että useiden kansainvälisten ja EU:n toimielinten, elinten ja virastojen sekä jäsenvaltioiden monet meneillään olevat toimet edellyttävät koordinointia päällekkäisen työn välttämiseksi, minkä vuoksi on syytä harkita koordinaatiosta vastaavan viranomaisen nimittämistä, mahdollisesti nimittämällä EU:n verkkoturvallisuuskoordinaattori;

43. korostaa, että kriittisen tietoteknisen infrastruktuurin suojaamiseen osallistuvien EU:n ja Yhdysvaltojen tärkeimpien toimijoiden ja lainsäädäntövallan käyttäjien on käytävä jäsenneltyä vuoropuhelua päästäkseen yhteisymmärrykseen oikeudellisesta ja hallinnollisesta järjestelmästä ja saadakseen niitä varten yhteiset tulkinnat ja kannat;

44. suhtautuu myönteisesti marraskuussa 2010 pidetyssä EU:n ja Yhdysvaltojen huippukokouksessa tapahtuneeseen EU:n ja Yhdysvaltojen verkkoturvallisuus- ja -rikollisuustyöryhmän perustamiseen ja tukee sen ponnisteluja internetin turvallisuutta koskevien asioiden sisällyttämiseksi transatlanttiseen poliittiseen vuoropuheluun; on tyytyväinen siihen, että komissio laatii Yhdysvaltojen kanssa EU:n ja Yhdysvaltojen verkkoturvallisuus- ja -rikollisuustyöryhmän alaisuudessa vuosiksi 2012/2013 yhteisen ohjelman ja etenemissuunnitelman yhteisiä/yhteensovitettuja mannertenvälisiä verkkoturvallisuusharjoituksia varten;

45. ehdottaa EU:n ja Yhdysvaltojen lainsäätäjien välisen jäsennellyn vuoropuhelun aloittamista internetiin liittyvien kysymysten käsittelemiseksi osana pyrkimystä saavuttaa yhteinen näkökulma, tulkinta ja kannat;

46. kehottaa Euroopan ulkosuhdehallintoa ja komissiota varmistamaan Euroopan jäsenvaltiofoorumin tekemän työn pohjalta aktiivisen toiminnan asianomaisilla kansainvälisillä foorumeilla muun muassa koordinoimalla jäsenvaltioiden kantoja EU:n ydinarvojen, tavoitteiden ja toimintatapojen edistämiseksi internetin turvallisuuden ja sietokyvyn alalla; toteaa, että kyseisiä foorumeja ovat esimerkiksi Nato, YK (erityisesti Kansainvälisen televiestintäliiton ja Internetin hallintofoorumin kautta), internetosoitteita ja verkkotunnuksia hallinnoiva ICANN-järjestö (Internet Corporation for Assigned Names and Numbers), internetiin liittyvien nimien ja osoitteiden keskusrekisteri IANA (Internet Assigned Numbers Authority), ETYJ, OECD ja Maailmanpankki;

47. kannustaa komissiota ja ENISAa osallistumaan merkittävien sidosryhmien vuoropuheluihin kyperavaruuden teknisten ja oikeudellisten normien määrittämiseksi kansainvälisellä tasolla;

48. kehottaa puhemiestä välittämään tämän päätöslauselman neuvostolle ja komissiolle.

PERUSTELUT

Tekniikka on yhä tärkeämmässä asemassa jokapäiväisessä elämässämme sen kaikilla osa-alueilla – viestinnästä rahoitus- ja pankkialaan, liikenteestä energiaan, kulttuurista ja viihteestä terveydenhuoltoon.

Nykyisin internetin ja tietokonepohjaisen tekniikan lisääntyvän käytön myötä internetin turvallisuus on yksi Euroopan unionin ja muun maailman tärkeimmistä poliittisista painopisteistä. Vuonna 2010 julkistettu Eurooppa 2020 -strategia sisälsi lippulaiva-aloitteena Euroopan digitaalistrategian, jossa asetettiin kunnianhimoisia tavoitteita Euroopan unionin tekniselle kehitykselle. Innovatiivisen tieto- ja viestintätekniikan, kuten nopeiden ja ultranopeiden kiinteiden ja matkaviestintään perustuvien internetyhteyksien ja matkaviestinverkkojen, älykkäiden sähköverkkojen sekä internetpalvelujen, kuten pilvipalvelujen ja esineiden internetin, lisääntyvä käyttö ja hyödyntäminen perustuu yhteen yksinkertaiseen, mutta ratkaisevan tärkeään näkökohtaan – turvallisuuteen, sietokykyyn ja luottamukseen.

Joulukuussa 2006 komissio hyväksyi Euroopan elintärkeiden infrastruktuureiden suojaamisohjelmaa (EPCIP) koskevan tiedonannon. Siinä määritellään yleiset puitteet elintärkeän infrastruktuurin suojaamistoimille EU:n tasolla. Kaksi vuotta myöhemmin neuvosto hyväksyi direktiivin 2008/114/EY Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista. Ensimmäisessä vaiheessa direktiivi keskittyi energia- ja liikennealaan. Siinä käsitellään yksinomaan infrastruktuureita, joiden toiminnan keskeytyminen vaikuttaisi vähintään kahteen EU:n jäsenvaltioon.

Direktiivissä 2008/114/EY tieto- ja viestintätekniikka-ala määriteltiin tulevaksi painopistealaksi, vaikka sitä ei luokiteltu elintärkeäksi infrastruktuuriksi. Siitä huolimatta komissio on vuodesta 2005 korostanut tarvetta koordinoida ponnisteluja luottamuksen parantamiseksi sähköistä viestintää kohtaan[1]. Tätä varten vuonna 2006 hyväksyttiin turvallisen tietoyhteiskunnan strategia[2], jonka keskeiset tekijät vahvistettiin neuvoston päätöslauselmassa 2007/068/01.

Vuonna 2009 komissio hyväksyi tiedonannon "Euroopan suojaaminen laajoilta tietoverkkohyökkäyksiltä ja häiriöiltä: valmiuden, turvallisuuden ja sietokyvyn parantaminen"[3]. Tässä tiedonannossa komissio esitti "elintärkeiden tietoinfrastruktuureiden suojaamista koskevan toimintasuunnitelman", jonka tavoitteena on kannustaa ja tukea kriittisten tietoinfrastruktuureiden turvallisuutta sekä kansallisella että unionin tasolla. Suunnitelmassa määritellään komission, ENISA:n, jäsenvaltioiden ja alan erityisroolit. TVT-infrastruktuurien turvallisuuden ja sietokyvyn lisäämistä käsiteltiin entistä pontevammin Euroopan digitaalistrategiassa[4] ja siihen liittyvissä neuvoston päätelmissä[5], ehdotuksessa

1 COM(2005)0229.
2 COM(2006)0251.
3 COM(2009)0149.
4 COM(2010)0245.
5 Neuvoston päätelmät, 31. toukokuuta 2010.

direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä[1] sekä komission ehdotuksessa vahvistetun ja uudistetun ENISA:n uudeksi toimikaudeksi[2].

Maaliskuussa 2011 komissio antoi tiedonannon elintärkeiden tietoinfrastruktuureiden suojaamisesta: "saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta"[3] . Komissio tarkastelee asiakirjassa elintärkeiden tietoinfrastruktuurien suojaamista koskevan toimintasuunnitelman toteuttamisen tuloksia vuodesta 2009 ja kuvailee seuraavia vaiheita keskittyen entistä enemmän EU:n rajojen ulkopuoliseen kansainväliseen yhteistyöhön.

Koko tämä muutaman vuoden aikana tapahtunut kehitys, joka ei lopeta ponnisteluja kyberavaruuden turvallisuuden lisäämiseksi unionissa, osoittaa, että internetin turvallisuus on tärkeä kysymys. On selvää, että internet on elintärkeä infrastruktuuri ja että sen toimintahäiriöt saattavat johtaa huomattaviin menetyksiin ja turvallisuusriskeihin, jotka vaikuttavat todella useisiin Euroopan kansalaisiin ja yrityksiin. Lisäksi tekniikan nopea kehitys edellyttää, että internethyökkäysten estämisen, korjaustoimien ja maailmanlaajuisen verkon sietokyvyn pitäisi perustua kattaviin, ennaltaehkäiseviin, joustaviin, innovatiivisiin ja pitkän aikavälin puitteisiin. Näiden puitteiden on varmistettava, että hallitusten, yritysten, yksilöiden ja kaikkien muiden sidosryhmien välinen vuorovaikutus on tehokasta. Lopuksi todettakoon, että internetin sietokyvyn lisääminen on mahdollista vain, kun toiminnassa on tehokas kansainväliseen yhteistyöhön ja kansainvälisiin normeihin perustuva järjestelmä.

1 COM(2010)0517.
2 COM(2010)0521.
3 COM(2011)0163 lopullinen.

22.3.2012

KANSALAISVAPAUKSIEN SEKÄ OIKEUS- JA SISÄASIOIDEN VALIOKUNNAN LAUSUNTO

teollisuus-, tutkimus- ja energiavaliokunnalle

elintärkeiden tietoinfrastruktuureiden suojaamisesta – saavutukset ja seuraavat vaiheet: kohti maailmanlaajuista verkkoturvallisuutta
(2011/2284(INI))

Valmistelija: Ágnes Hankiss

EHDOTUKSET

Kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunta pyytää asiasta vastaavaa teollisuus-, tutkimus- ja energiavaliokuntaa sisällyttämään seuraavat ehdotukset päätöslauselmaesitykseen, jonka se myöhemmin hyväksyy:

1. ottaa huomioon, että elintärkeiden tietoinfrastruktuureiden suojaaminen vaatii monialaisen lähestymistavan, jonka on sisällettävä kansalaisvapauksien sekä oikeus- ja sisäasioiden tärkeät näkökohdat, joita ovat esimerkiksi sisäinen turvallisuus, henkilötietojen suojaaminen sekä oikeus luottamuksellisuuteen ja yksityiselämään, millä tehostetaan turvallisuutta ja huolehditaan perusoikeuksien kunnioittamisesta;

2. muistuttaa, että elintärkeiden tietoinfrastruktuureiden suojaaminen sisältyy EU:n sisäisen turvallisuuden strategiaan, kun parannetaan kansalaisten ja yritysten turvallisuutta verkkoympäristössä;

3. korostaa, että Euroopan elintärkeän infrastruktuurin määrittäminen on saatettava päätökseen ja sitä on päivitettävä jatkuvasti komission valvonnassa (Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista annetun) neuvoston direktiivin 2008/114/EY[1] mukaisesti; painottaa myös tarvetta luoda elintärkeiden infrastruktuureiden varoitusjärjestelmä EU:n tasolla mahdollisimman pian; edellyttää, että neuvoston direktiiviä 2008/114/EY olisi tarkasteltava uudelleen, jotta myös tieto- ja viestintätekniikan ala luokitellaan elintärkeäksi alaksi, sillä julkisyhteisöt, yritykset ja yksityiset kotitaloudet ovat siitä hyvin riippuvaisia;

[1] EUVL L 345, 23.12.2008, s. 75.

4. kehottaa jäsenvaltioita laatimaan kansallisia strategioita ja varmistamaan niille vakaan päätöksenteko- ja sääntely-ympäristön, monipuoliset kansalliset riskinhallintatoimet ja tarvetta vastaavat valmiustoimet ja -mekanismit; kehottaa jäsenvaltioita, jotka eivät ole vielä perustaneet kansallisia tietotekniikan kriisiryhmiä (CERT), perustamaan ne ajoissa turvautuen tarvittaessa Euroopan verkko- ja tietoturvaviraston (ENISA) apuun;

5. katsoo, että mitä tahansa laaja-alaista tietojärjestelmää, joka koskee esimerkiksi EU:n, jäsenvaltioiden hallitusten tai finanssi- ja terveydenhuoltolaitosten luottamuksellisia henkilötietoja, tulisi pitää osana elintärkeää tietoinfrastruktuuria, ja tällaisten tietojen suojaaminen olisi varmistettava korkeimpien mahdollisten standardien mukaisesti;

6. kehottaa komissiota ja jäsenvaltioita ryhtymään tarvittaviin toimenpiteisiin elintärkeiden infrastruktuureiden suojaamiseksi tietoverkkohyökkäyksiltä ja tarjoamaan keinoja, joiden avulla voidaan estää pääsy elintärkeään infrastruktuuriin, mikäli suora tietoverkkohyökkäys uhkaisi vakavasti sen moitteetonta toimintaa;

7. korostaa yleiseurooppalaisten laajamittaisten verkkoturvallisuusharjoitusten sekä yhtenäisten uhka-arviota koskevien vaatimusten määrittämisen merkitystä;

8. katsoo, että ENISAlla voi olla tärkeä asema EU:n tasolla elintärkeiden tietoinfrastruktuureiden suojaamisessa, koska se voi tarjota teknistä asiantuntemusta jäsenvaltioille, EU:n toimielimille ja elimille sekä antaa raportteja ja analyysejä EU:n ja maailmanlaajuisten tietojärjestelmien turvallisuudesta;

9. uskoo, että EU:n ulkopuolelle ulottuva kansainvälinen yhteistyö on välttämätöntä, sillä tietoverkkouhkat ovat luonteeltaan maailmanlaajuisia, ja ne vaativat kansainvälisen oikeuden määräysten mukaisia maailmanlaajuisia ratkaisuja; painottaa lisäksi, että kaikkien arkaluonteisten tietojen vaihtoa sisältävien kansainvälisten sopimusten tekemisessä tulisi ottaa huomioon tiedonsiirron ja -varastoinnin turvallisuus;

10. korostaa, että komission tulevassa "internetin turvallisuusstrategiassa" olisi otettava erityisesti huomioon elintärkeiden tietoinfrastruktuureiden suojaamista koskeva työ ja pyrittävä tietoverkkoturvallisuuden osalta kokonaisvaltaiseen ja järjestelmälliseen lähestymistapaan sisällyttämällä strategiaan ennaltaehkäiseviä toimenpiteitä, kuten turvatoimia koskevat vähimmäisstandardit tai yksittäisten käyttäjien, yritysten ja julkisten laitosten opettaminen, ja reaktiivisia toimenpiteitä, kuten rikosoikeudellisia, siviilioikeudellisia ja hallinnollisia seuraamuksia;

11. uskoo, että yhteistyötä EU:ssa tulisi vahvistaa ja lisätä ennen kaikkea siviili- ja sotilastoimijoiden välillä sekä sellaisten oikeusviranomaisten ja muiden toimivaltaisten viranomaisten välillä, jotka estävät ja torjuvat tietojärjestelmiin kohdistuvia hyökkäyksiä ja määräävät niistä rangaistuksia, mukaan luettuina jäsenvaltioiden poliisivoimat ja muut lainvalvontaviranomaiset sekä EU:n erillisvirastot, kuten Eurojust, Europol ja ENISA;

12. korostaa julkisen ja yksityisen sektorin välisen vahvan yhteistyön merkitystä, sillä sektoreiden eri vahvuuksien pitäisi toisiaan täydentäen tukea infrastruktuureiden suojaamiseksi tehtyjä toimia ja siten Euroopan kansalaisten elämää ja yksityisyyttä; kehottaa komissiota perustamaan suojaustoimien varmistamiseksi Euroopan julkisen ja

yksityisen sektorin kumppanuuden, joka toimii yhteistyössä ENISAn ja Euroopan hallitusten CERT-ryhmän kanssa;

13. huomauttaa, että useiden kansainvälisten ja EU:n toimielinten, elinten ja virastojen sekä jäsenvaltioiden monet meneillään olevat toimet edellyttävät koordinointia päällekkäisen työn välttämiseksi, minkä vuoksi on syytä harkita koordinaatiosta vastaavan viranomaisen nimittämistä, mahdollisesti nimittämällä EU:n verkkoturvallisuuskoordinaattori;

14. katsoo, että elintärkeiden tietoinfrastruktuureiden suojaamistoimien avulla lisätään kansalaisten yleistä turvallisuutta ja parannetaan myös kansalaisten käsitystä turvallisuudesta ja heidän luottamustaan toimenpiteisiin, joita hallitus toteuttaa heidän suojaamisekseen;

15. korostaa eurooppalaisen tutkimuksen jatkuvan integroinnin kehittämisen ja varmistamisen merkitystä eurooppalaisen huippuosaamisen ylläpitäjänä ja vahvistajana elintärkeiden tietoinfrastruktuureiden suojaamisen alalla;

16. korostaa verkkoturvallisuusalan tutkimuksen aktiivisen etenemissuunnitelman merkitystä;

17. kannattaa verkkoturvallisuuskoulutusta (tohtoriopiskelijoiden harjoittelut, korkeakouluopinnot, työpajat, opintoharjoittelut jne.) ja erityisiä koulutusharjoituksia elintärkeiden tietoinfrastruktuureiden suojaamisesta;

18. kannattaa kansallisten yksityisten sektorien ja ENISAn tiivistä yhteistyötä ja vuorovaikutusta, jotta kansalliset/valtiolliset CERT-ryhmät voidaan kytkeä eurooppalaisen tiedonjako- ja hälytysjärjestelmän (EISAS) kehittämiseen;

19. Korostaa, että on tärkeää laatia yhteinen eurooppalainen verkkoturvallisuusstrategia ja esittää aikataulu siihen liittyvien toimien ja tarvittavien resurssien määrittämiseksi;

20. korostaa, että kriittisen tietoteknisen infrastruktuurin suojaamiseen osallistuvien EU:n ja Yhdysvaltojen tärkeimpien toimijoiden ja lainsäädäntövallan käyttäjien on käytävä jäsenneltyä vuoropuhelua päästäkseen yhteisymmärrykseen oikeudellisesta ja hallinnollisesta järjestelmästä ja saadakseen niitä varten yhteiset tulkinnat ja kannat.

VALIOKUNNAN LOPULLISEN ÄÄNESTYKSEN TULOS

Hyväksytty (pvä)	21.3.2012
Lopullisen äänestyksen tulos	+: 45 –: 0 0: 2
Lopullisessa äänestyksessä läsnä olleet jäsenet	Roberta Angelilli, Edit Bauer, Arkadiusz Tomasz Bratkowski, Philip Claeys, Carlos Coelho, Rosario Crocetta, Frank Engel, Cornelia Ernst, Tanja Fajon, Kinga Göncz, Nathalie Griesbeck, Sylvie Guillaume, Anna Hedh, Salvatore Iacolino, Lívia Járóka, Teresa Jiménez-Becerril Barrio, Juan Fernando López Aguilar, Monica Luisa Macovei, Svetoslav Hristov Malinov, Véronique Mathieu, Anthea McIntyre, Jan Mulder, Antigoni Papadopoulou, Judith Sargentini, Csaba Sógor, Renate Sommer, Rui Tavares, Kyriacos Triantaphyllides, Wim van de Camp, Renate Weber, Josef Weidenholzer, Cecilia Wikström
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Vilija Blinkevičiūtė, Andrew Henry William Brons, Michael Cashman, Anna Maria Corazza Bildt, Ana Gomes, Nadja Hirsch, Stanimir Ilchev, Iliana Malinova Iotova, Franziska Keller, Wolfgang Kreissl-Dörfler, Mariya Nedelcheva, Hubert Pirker, Zuzana Roithová, Kārlis Šadurskis
Lopullisessa äänestyksessä läsnä olleet sijaiset (187 art. 2 kohta)	Luis de Grandes Pascual

VALIOKUNNAN LOPULLISEN ÄÄNESTYKSEN TULOS

Hyväksytty (pvä)	8.5.2012
Lopullisen äänestyksen tulos	+: 51 –: 7 0: 0
Lopullisessa äänestyksessä läsnä olleet jäsenet	Amelia Andersdotter, Josefa Andrés Barea, Jean-Pierre Audy, Zigmantas Balčytis, Ivo Belet, Bendt Bendtsen, Jan Březina, Maria Da Graça Carvalho, Giles Chichester, Jürgen Creutzmann, Pilar del Castillo Vera, Dimitrios Droutsas, Adam Gierek, Norbert Glante, Robert Goebbels, András Gyürk, Fiona Hall, Edit Herczog, Kent Johansson, Romana Jordan, Krišjānis Kariņš, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Vittorio Prodi, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Paul Rübig, Salvador Sedó i Alabart, Francisco Sosa Wagner, Konrad Szymański, Britta Thomsen, Evžen Tošenovský, Ioannis A. Tsoukalas, Claude Turmes, Marita Ulvskog, Vladimir Urutchev, Kathleen Van Brempt, Alejo Vidal-Quadras, Henri Weber
Lopullisessa äänestyksessä läsnä olleet varajäsenet	Ioan Enciu, Françoise Grossetête, Takis Hadjigeorgiou, Roger Helmer, Jolanta Emilia Hibner, Bernd Lange, Werner Langen, Zofija Mazej Kukovič, Silvia-Adriana Ţicău, Inês Cristina Zuber
Lopullisessa äänestyksessä läsnä olleet sijaiset (187 art. 2 kohta)	Anne E. Jensen, Nicole Kiil-Nielsen, Norica Nicolai