



EUROOPA PARLAMENT

2009–2014

Istungidokument

A7-0167/2012

16.5.2012

RAPORT

Elutähtsate infoinfrastruktuuride kaitse – saavutused ja edasised sammud:
üleilmse küberjulgeoleku suunas
(2011/2284(INI))

Tööstuse, teadusuuringute ja energeetikakomisjon

Raportöör: Ivailo Kalfin

SISUKORD

Lk

EUROOPA PARLAMENDI RESOLUTSIOONI ETTEPANEK.....	3
SELETUSKIRI	11
KODANIKUVABADUSTE, JUSTIITS- JA SISEASJADE KOMISJONI ARVAMUS	13
PARLAMENDIKOMISJONIS TOIMUNUD LÕPPHÄÄLETUSE TULEMUS.....	17

EUROOPA PARLAMENDI RESOLUTSIOONI ETTEPANEK

**elutähtsate infoinfrastruktuuride kaitse kohta – saavutused ja edasised sammud:
üleilmse küberjulgeoleku suunas**

(2011/2284(INI))

Euroopa Parlament,

- võttes arvesse oma 5. mai 2010. aasta resolutsiooni Euroopa uue digitaalse tegevuskava kohta: 2015.eu¹,
 - võttes arvesse oma 15. juuni 2010. aasta resolutsiooni interneti haldamise järgmiste sammude kohta²,
 - võttes arvesse oma 6. juuli 2011. aasta resolutsiooni Euroopa lairibaühenduse kohta: investering digitaalvaldkonnale tuginevasse majanduskasvu³,
 - võttes arvesse kodukorra artiklit 48,
 - võttes arvesse tööstuse, teadusuuringute ja energeetikakomisjoni raportit ning kodanikuvabaduste, justiits- ja siseasjade komisjoni arvamust (A7-0167/2012),
- A. arvestades, et info- ja kommunikatsioonitehnoloogiate (IKT) võimalusi majanduse ja ühiskonna edendamisel suudetakse täielikult ära kasutada vaid siis, kui kasutajad usaldavad nende turvalisust ja vastupidavust ning kui internetikeskkonnas tagatakse tulemuslikult kehtivate õigusaktide täitmine küsimustes, nagu andmete puutumatus ja intellektuaalse omandi õigused;
- B. arvestades, et interneti ja IKT mõju kodanike elu eri aspektidele suureneb kiiresti, ning arvestades, et need on sotsiaalse suhtluse, kultuurilise rikastumise ja majanduskasvu peamiseks edasiviivaks jõuks;
- C. arvestades, et IKT- ja internetiturvalisus on ulatuslik kontseptsioon, millel on üleilmne mõju majanduslikele, sotsiaalsetele, tehnoloogilistele ja sõjalistele aspektidele, mis nõuab kohustuste selget määratlemist ja eristamist ning kindlat rahvusvahelise koostöö mehhanismi;
- D. arvestades, et ELi digitaalarengu tegevuskava juhtalgatuse eesmärk on edendada IKT tugevdamise alusel Euroopa konkurentsivõimet ning luua tingimused suure ja jõulise majanduskasvu ning tehnoloogiapõhiste töökohtade jaoks;
- E. arvestades, et erasektor on jätkuvalt peamine investor infoturbetoodetesse, -teenustesse, -rakendustesse ja infrastruktuuri ning on nende omanik ja haldaja, olles viimase kümnendi jooksul investerinud miljardeid eurosid; arvestades, et erasektori osalust tuleks

¹ ELT C 81E, 15.3.2011, lk 45.

² ELT C 236E, 12.8.2011, lk 33.

³ Vastuvõetud tekstid, P7_TA(2011)0322.

suurendada asjakohaste poliitiliste strateegiatega, et suurendada avaliku sektori, erasektori või avaliku ja erasektori omanduses olevate või nende hallatavate infrastruktuuride vastupidavust;

- F. arvestades, et IKT-võrkude, -teenuste ja -tehnoloogiate kõrgetasemelise turvalisuse ja vastupidavuse arendamine suurendab ELi majanduse konkurentsivõimet, parandades nii küberriskide hindamist ja maandamist kui varustades ELi majandust tervikuna tugevamate infoinfrastruktuuridega innovatsiooni ja majanduskasvu toetamiseks, mis loob ettevõtjatele uusi võimalusi tootlikkuse suurendamiseks;
- G. arvestades, et õiguskaitseorganite andmetest küberkuritegevuse kohta (mis hõlmavad küberrünnakuid, aga ka muud laadi internetikuritegevust) nähtub, et kuritegevus on mitmes Euroopa riigis märgatavalt suurenenud; arvestades siiski asjaolu, et nii õiguskaitseorganitelt kui ka infoturbeintsidentidega tegelevatelt rühmadelt (CERT) pärit statistiliselt representatiivseid andmeid küberrünnakute kohta on vähe ja neid tuleb tulevikus paremini koguda, sest see võimaldab õiguskaitseorganitel kogu ELis jõulisemalt reageerida ning pidevalt arenevatele küberohtudele paremini informeeritult õigusaktide abil reageerida;
- H. arvestades, et asjakohane infoturbe tase on kriitilise tähtsusega internetipõhiste teenuste jõuliseks kasvuks;
- I. arvestades, et hiljutised küberjuhtumid, häired ja rünnakud ELi institutsioonide, tööstuse ning liikmesriikide infoinfrastruktuuride vastu annavad tunnistust vajadusest luua vastupidav, innovaatiline ja tulemuslik elutähtsate infoinfrastruktuuride kaitse süsteem, mis põhineb täielikul rahvusvahelisel koostööl ja liikmesriikidele kehtivatel vastupidavuse miinimumstandarditel;
- J. arvestades, et IKT uute võimaluste, näiteks pilvandmetöötluse kiire arengu tõttu tuleb pöörata palju tähelepanu turvalisusele, et võimaldada tehnoloogilistest saavutustest täit kasu saada;
- K. arvestades, et Euroopa Parlament on korduvalt nõudnud, et andmete puutumatuse ja kaitse, võrgu neutraalsuse ning intellektuaalse omandi õiguste kaitse suhtes kohaldataks kõrgeid standardeid;

I. Meetmed elutähtsate infoinfrastruktuuride kaitse tugevdamiseks riikide ja liidu tasandil

- 1. väljendab heameelt elutähtsate infoinfrastruktuuride kaitset käsitleva Euroopa tegevuskava rakendamise üle liikmesriikides, sealhulgas elutähtsate infrastruktuuridega seotud teabe vahetuse infosüsteemi (CIWIN) loomise üle;
- 2. on seisukohal, et elutähtsate infoinfrastruktuuride kaitse alased jõupingutused edendavad nii kodanike üldist julgeolekut kui parandavad ka kodanike arusaama julgeolekust ning usaldust valitsuse poolt nende kaitseks võetavate meetmete vastu;

3. tunnustab asjaolu, et komisjon kaalub nõukogu direktiivi nr 2008/114/EÜ¹ läbivaatamist, ning nõuab, et enne edasiste sammude astumist esitataks tõendeid direktiivi tulemuslikkuse ja mõju kohta; nõuab direktiivi rakendusala laiendamise kaalumist, eriti IKT-sektori ning finantsteenuste lisamisega; nõuab lisaks selliste valdkondade arvessevõtmist, nagu tervishoid, toidu ja vee tarnesüsteemid, tuumaenergia alased teadusuuringud ja tööstus (juhul kui neid ei käsitleta erisätetes); on seisukohal, et kõnealused sektorid peaksid saama samuti kasu CIWINi sektoriülesest lähenemisviisist (mis koosneb koostööst, hoiatussüsteemist ja parimate tavade vahetamisest);
4. toonitab, kui tähtis on luua ja tagada Euroopa teadustöö kestav integratsioon, et säilitada ja tugevdada Euroopa tipptaset elutähtsate infoinfrastruktuuride kaitse valdkonnas;
5. seoses sellega, et liikmesriikide ja Euroopa elutähtsad infoinfrastruktuurid on vastastikku seotud, üksteisest äärmiselt sõltuvad, tundlikud, strateegilised ja haavatavad, nõuab minimaalsete vastupidavuse standardite perioodilist ajakohastamist, et olla valmis ja reageerida häirete, vahejuhtumite, hävitamiskatsete või rünnakute korral, mis on põhjustatud näiteks liiga nõrgast infrastruktuurist või ebapiisavalt kindlustatud lõppterminalidest;
6. rõhutab infoturbestandardite ja -protokollide tähtsust ning toetab 2011. aasta otsust volitada Euroopa Standardikomiteed, Euroopa Elektrotehnika Standardikomiteed ja Euroopa Telekommunikatsioonistandardite Instituuti kehtestama turbestandardid;
7. eeldab, et elutähtsate infoinfrastruktuuride omanikud ja haldajad võimaldavad ja vajaduse korral aitavad kasutajatel rakendada asjakohaseid vahendeid enda kaitsmiseks pahatahtlike rünnakute ja/või häirete eest, vajadusel nii inimeste kui ka automaatseadmete juhendamisel;
8. toetab liidu tasandi koostööd avaliku ja erasektori sidusrühmade vahel ning ergutab nende pingutusi töötada välja ja rakendada turvalisuse ja vastupidavuse standardid riikliku ja Euroopa tasandi tsiviilotstarbeliste (kas avaliku sektori, erasektori või avaliku ja erasektori) elutähtsate infoinfrastruktuuride jaoks;
9. rõhutab, kui tähtsad on üleeuroopalised õppused ulatuslikele võrguturbeintsidentidele reageerimiseks ning ühtsete ohuhinnangu standardite kindlaksmääramine;
10. kutsub komisjoni koostöös liikmesriikidega hindama elutähtsate infoinfrastruktuuride kaitse tegevuskava rakendamist; nõuab tungivalt, et liikmesriigid looksid hästi toimivad riikide või valitsuste CERTid, töötaksid välja riiklikud küberjulgeoleku strateegiad, korraldaksid regulaarseid riiklikke ja üleeuroopalisi küberjuhtumite õppusi, töötaksid välja riiklikud küberjuhtumitega seotud situatsiooniplaanid ning osaleksid Euroopa küberjuhtumitega seotud situatsiooniplaanide väljatöötamisel 2012. aasta lõpuks;
11. soovitab kehtestada haldaja turvalisuse tagamise kavade või samaväärsed meetmed kõigis Euroopa elutähtsates infoinfrastruktuurides ning nimetada turvalisuse kontaktametnikud;

¹ ELT L 345, 23.12.2008, lk 75.

12. tervitab nõukogu raamotsuse 2005/222/JSK¹ (infosüsteemide vastu suunatud rünnete kohta) praegust läbivaatamist; märgib, et vaja on kooskõlastada ELi pingutused laiaulatuslike küberrünnakute tõrjumiseks, kaasates Euroopa Võrgu- ja Infoturbeameti (ENISA), liikmesriikide CERTide ja tulevase Euroopa CERTi pädevused;
13. on seisukohal, et ENISA võib etendada Euroopa tasandil elutähtsate infoinfrastruktuuride kaitsel kesket rolli liikmesriikidele ning Euroopa Liidu institutsioonidele ja asutustele tehniliste eriteadmiste andmise ning Euroopa ja üleilmsel tasandil infosüsteemide turvalisust käsitlevate aruannete ja analüüside koostamise kaudu;

II. ELi edasine tegevus internetiturvalisuse suurendamise nimel

14. nõuab tungivalt, et ENISA koordineeriks ja viiks igal aastal läbi ELi internetiturvalisuse teadlikkuse kuud, nii et küberjulgeolekuga seotud probleemid saaksid liikmesriikide ja ELi kodanike eritähelepanu osaliseks;
15. avaldab ENISA-le kooskõlas digitaalarengu tegevuskava eesmärkidega toetust selle võrgu- ja infoturbe seotud kohustuste täitmisel ning eelkõige liikmesriikide juhendamisel ja nõustamisel selles, kuidas saavutada nende CERTide põhipädevused, ning parimate tavade vahetamise toetamisel usaldusliku keskkonna väljaarendamise kaudu; kutsub ametit üles konsulteerima asjaomaste sidusrühmadega, eesmärgiga määratleda sarnased küberjulgeolekumeetmed eravõrkude ja -infrastruktuuride omanikele ja haldajatele, ning abistama vastavalt vajadusele komisjoni ja liikmesriike riikide ja Euroopa CERTide ning infrastruktuuri omanike ja haldajate seas infoturbe sertifitseerimiskavade, käitumisnormide ja koostöötavade väljatöötamises ja kasutuselevõttus tehnoloogiliselt neutraalsete ühiste miinimumstandardite määratlemise kaudu;
16. tervitab praegust ettepanekut ENISA volituste läbivaatamise kohta, eriti nende suurendamise ja ameti ülesannete laiendamise kohta; on arvamusel, et lisaks ENISA poolt liikmesriikidele pakutavatele teadmistele ja analüüsile peaks talle kuuluma mitu ELi tasandi täitevülesannet ning – koostöös USA vastavate asutustega – võrgu- ja infoturbeintsidendite ärahoidmise ja avastamisega seotud ülesanded ja liikmesriikidevahelise koostöö edendamine; juhib tähelepanu sellele, et ENISA määruse kohaselt võib ametile anda ka internetirünnakutele reageerimisega seotud lisakohustusi, eeldusel et ta lisab selgelt väärtust olemasolevatele riiklikele reageerimismehhanismidele;
17. tervitab 2010. ja 2011. aastal toimunud üleeuroopalisi küberjulgeolekuõppusi, mis viidi läbi üle kogu liidu ja mida vaatles ENISA, kelle eesmärk oli abistada liikmesriike üleeuroopalise situatsiooniplaani koostamisel, haldamisel ja testimisel; palub ENISA-l jätta sellised õppused oma tegevuskavva ja kaasata vastavalt vajadusele üha rohkem asjakohaseid erasektori ettevõtjaid, et suurendada Euroopa üldist internetiturvalisuse alast suutlikkust; ootab edasist laienemist rahvusvahelisel tasandil koos sarnaselt mõtlevate partneritega;
18. palub liikmesriikidel koostada riiklikud küberjuhtumitega seotud situatsiooniplaanid ning hõlmata neisse põhielemendid, nagu asjaomased kontaktpunktid ning sätted abi,

¹ ELT L 69, 16.3.2005, lk 67.

ohjeldamise ja parandamise kohta piirkondlikku, riiklikku või piiriülest tähtsust omavate küberhäirete või -rännakute korral; märgib, et samuti peaksid liikmesriigid looma riiklikul tasandil asjakohased koordineerimismehhanismid ja struktuurid, mis aitaksid parandada koordineerimist riigi pädevate asutuste vahel ning muuta nende võetud meetmed sidusamaks;

19. soovitab komisjonil esitada ELi küberjuhtumitega seotud situatsiooniplaani kaudu siduvad meetmed riikide ja valitsuste CERTide tehniliste ja juhtimisega seotud ülesannete paremaks koordineerimiseks ELi tasandil;
20. palub komisjonil ja liikmesriikidel võtta vajalikke meetmeid, et kaitsta elutähtsaid infrastruktuure küberrännakute eest ja pakkuda mooduseid elutähtsale infrastruktuurile juurdepääsu hermeetiliseks katkestamiseks, kui otsene küberrünnak ohustab tõsiselt selle nõuetekohast toimimist;
21. ootab, et täielikult hakkaks toimima ELi CERT, millest saab olulisim tegur ELi institutsioonide vastu suunatud tahtlike ja pahatahtlike küberrännakute ärahoidmisel, avastamisel, neile reageerimisel ja nendest taastumisel;
22. soovitab komisjonil pakkuda välja siduvad meetmed, mille eesmärk on kehtestada minimaalsed turva- ja vastupidavusstandardid ning parandada koordineerimist liikmesriikide CERTide vahel;
23. palub liikmesriikidel ja ELi institutsioonidel tagada selliste hästi toimivate CERTide olemasolu, millel on kokkulepitud parimatel tavadel põhinevad minimaalsed pädevused turvalisuse ja vastupidavuse vallas; juhib tähelepanu, et riikide CERTid peaksid kuuluma tulemuslikku võrgustikku, milles vahetatakse asjakohast teavet kooskõlas vajalike konfidentsiaalsusstandarditega; nõuab ööpäevaringselt tegutseva elutähtsate infoinfrastruktuuride kaitse teenuse loomist igas liikmesriigis ning riikide kontaktpunktide suhtes kohaldatava ühise Euroopa hädaolukordade protokollide koostamist;
24. rõhutab, et andmete ning riiklike võrkude ja infrastruktuuride kaitsmiseks on ülioluline luua usaldus ja edendada liikmesriikide vahelist koostööd; palub komisjonil soovitada ühist menetlust ühise lähenemisviisi kindlaksmääramiseks ja kasutuselevõtuks, et võidelda piiriüleste IKT-ohtudega, eeldades et liikmesriigid esitavad komisjonile üldteavet oma elutähtsate infoinfrastruktuuride riskide, ohtude ja haavatavuse kohta;
25. väljendab heameelt komisjoni algatuse üle töötada 2013. aastaks välja Euroopa teabe jagamise ja hoiatussüsteem;
26. väljendab heameelt erinevate komisjoni algatatud konsultatsioonide üle sidusrühmadega internetiturvalisuse ja elutähtsate infoinfrastruktuuride kaitse teemal, nagu vastupidavust käsitlev Euroopa avaliku ja erasektori partnerlus; tunnustab IKT-müüjate juba märkimisväärset osalemist ja pühendumust selles valdkonnas, innustab komisjoni tegema edasisi pingutusi akadeemiliste ringkondade ja IKT-kasutajate ühenduste julgustamisel, et nad oleksid aktiivsemad, ning konstruktiivse, paljusid sidusrühmi kaasava dialoogi tugevdamisel küberjulgeoleku probleemide teemal; toetab digitaalse assamblee kui elutähtsate infoinfrastruktuuride kaitse haldusraamistiku edasiarendamist;

27. väljendab heameelt Euroopa liikmesriikide foorumi seni tehtud töö üle sektoripõhiste kriteeriumide kehtestamisel, et määrata kindlaks Euroopa elutähtsad infrastruktuurid, keskendudes tava- ja mobiilsidele, ning interneti vastupidavust ja stabiilsust käsitlevate ELi põhimõtete ja suuniste arutamisel; loodab liikmesriikide jätkuvalle üksmeele saavutamisele ja julgustab sellega seoses foorumit täiendama praegust füüsilise varale keskendunud käsitusviisi jõupingutustega hõlmata ka loogilise infrastruktuuri vara, mis muutub virtualiseerimis- ja pilvandmetöötlustehnoloogia edasiarendamisel üha olulisemaks elutähtsate infoinfrastruktuuride kaitse tõhususe seisukohast;
28. soovib komisjonil alata avalik üleeuroopaline hariduskampaania, mis on suunatud nii erakasutajate kui ka ettevõtjatest lõppkasutajate harimisele ja teadlikkuse tõstmisele võimalike ohtude kohta internetis ning paiksete ja mobiilsete IKT-seadmete kohta kasutusahela igas osas kui ka üksikisikute turvalisema internetikäitumise edendamisele; tuleb sellega seoses meelde aegunud IT-seadmete ja tarkvaraga seotud riske;
29. kutsub liikmesriike üles komisjoni toetusel tugevdama infoturbe alaseid koolitus- ja haridusprogramme, mis on suunatud riiklikele õiguskaitseorganitele ja õigusasutustele ning asjaomastele ELi ametitele;
30. toetab teadusekspertidele ELi õppekava loomist infoturbe valdkonnas, sest see mõjuks hästi ELi teadmiste ja valmisolekule seoses pidevalt areneva küberruumi ja selle ohtudega;
31. toetab elutähtsate infoinfrastruktuuride kaitse valdkonnas küberjulgeoleku alase hariduse (doktorantide praktika, ülikoolikursused, seminarid, üliõpilaste koolitamine jne) ja eriväljaõppe kursuste edendamist;
32. palub komisjonil esitada 2012. aasta lõpuks ettepaneku liidu laiahaardelise internetiturvalisuse strateegia kohta, mis põhineb selgel terminoloogial; on seisukohal, et internetiturvalisuse strateegia eesmärk peaks olema sellise küberruumi loomine (mida toetavad turvaline ja vastupidav infrastruktuur ning avatud standardid), mis toetab innovatsiooni ja heaolu teabe vaba liikumise kaudu, kaitstes samas kindlalt eraelu puutumatust ja muid kodanikuvabadusi; on jätkuvalt seisukohal, et strateegias tuleks üksikasjalikult määratleda põhimõtted, eesmärgid, meetodid, vahendid ja poliitika (nii liidusisene kui -väline), mis on vajalikud liikmesriikide ja ELi pingutuste sujuvamaks muutmiseks ning liikmesriikide seas minimaalsete vastupidavusstandardite kehtestamiseks, et tagada ohutu, pidev, tugev ja vastupidav teenus, olgu see seotud elutähtsa infrastruktuuri või üldise internetikasutusega;
33. toonitab, et komisjoni tulevases internetiturvalisuse strateegias tuleks keskseks lähtepunktiks võtta töö elutähtsate infoinfrastruktuuride kaitsel ning seada eesmärgiks terviklik ja süstemaatiline lähenemine küberjulgeolekule, mis hõlmab nii ennetavaid meetmeid, nagu turvameetmete miinimumstandardite kehtestamine või üksikkasutajate, ettevõtete ja avalik-õiguslike asutuste koolitamine, kui ka reageerivaid meetmeid, nagu kriminaal- ning tsiviilõiguslikud ja halduskaristused;
34. nõuab, et komisjon teeks ettepaneku tugeva mehhanismi kohta, et kooskõlastada internetiturvalisuse strateegia rakendamist ja regulaarset ajakohastamist; on seisukohal, et mehhanismi tuleks toetada piisavate haldus- ja finantsressurssidega ja ekspertide

kogemustega ning et see peaks olema pädev hõlbustama internetiturvalisusega seotud ELi seisukohtade väljakujundamist suhetes nii liidusiseste kui ka rahvusvaheliste sidusrühmadega;

35. palub komisjonil esitada ettepaneku ELi raamistiku kohta turvarikkumistest teatamiseks elutähtsates sektorites, nagu energeetika, transport, vee- ja toidutarned, ning IKT- ja finantsteenuste sektoris, et tagada liikmesriikide asjaomaste asutuste ja kasutajate teavitamine küberjuhtumitest, -rünnakutest või -häiretest;
36. nõuab tungivalt, et komisjon parandaks statistiliselt esinduslike andmete kättesaadavust ELis, liikmesriikides ja tööstuses (eriti finantsteenuste ja IKT-sektoris) toimunud küberrünnakute maksumuse kohta, suurendades 2013. aastaks kavandatud Euroopa küberkuritegevuse keskuse, CERTide ja komisjoni teiste algatuste, nagu Euroopa teabe jagamise ja hoiatussüsteem, andmekogumisvõimet, et tagada süstemaatiline aruandlus ja andmevahetus küberrünnakute ning Euroopa tööstust ja liikmesriike mõjutava küberkuritegevuse muude vormide kohta ning tugevdada õiguskaitset;
37. toetab tihedat suhtlust ja koostööd liikmesriikide erasektorite ning ENISA vahel, et teavitada riikide/valitsuste CERTe Euroopa teabe jagamise ja hoiatussüsteemi (EISAS) arengust;
38. juhib tähelepanu sellele, et peamiseks internetiturvalisuse suurendamiseks loodud tehnoloogiate arendamise ja kasutamise taga olevaks edasiviivaks jõuks on IKT-tööstus; tuletab meelde, et ELi poliitika peab ettevõtluse ning avaliku ja erasektori partnerluste võimaluste täielikuks ärakasutamiseks vältima Euroopa internetimajanduse kasvu takistamist ja sisaldama vajalikke stiimuleid; soovib uurida täiendavaid stiimuleid tööstusele, et töötada välja jõulisemad haldaja turvalisuse tagamise kavad kooskõlas direktiiviga 2008/114/EÜ;
39. kutsub komisjoni üles esitama seadusandliku ettepaneku küberrünnakute (s.o suunatud andmepüük (spear-phishing), internetipettus jne) tõsisemaks kuriteoks tunnistamise kohta;

III. Rahvusvaheline koostöö

40. tuletab meelde, et rahvusvaheline koostöö on tulemuslike küberjulgeoleku meetmete rakendamise põhiline vahend; tunnistas, et praegu ei ole EL aktiivselt ja püsivalt kaasatud küberjulgeolekuga seotud rahvusvahelise koostöö protsessi ja dialoogidesse; kutsub komisjoni ja Euroopa välisteenistust üles alustama kõigi sarnaselt mõtleivate riikidega konstruktiivset dialoogi, et kujundada välja ühised arusaamad ja poliitika eesmärgiga suurendada interneti ja elutähtsate infrastruktuuride vastupidavust; on jätkuvalt seisukohal, et samal ajal peaks EL lisama internetiturvalisuse probleemid püsivalt oma välissuhete temaatikasse, muu hulgas mitmesuguste rahastamisvahendite väljatöötamisel või selliste rahvusvaheliste lepingute allkirjastamisel, mis hõlmavad tundlike andmete vahetust ja säilitamist;
41. võtab teadmiseks Euroopa Nõukogu 2001. aasta küberkuritegevuse vastase Budapesti konventsiooni häid saavutusi; juhib siiski tähelepanu, et julgustades rohkem riike konventsiooni allkirjastama ja ratifitseerima, peaks Euroopa välisteenistus sõlmima sarnaselt mõtleivate rahvusvaheliste partneritega ka kahe- ja mitmepoolsed lepingud

interneti turvalisuse ja vastupidavuse kohta;

42. juhib tähelepanu sellele, et eri rahvusvaheliste ja ELi institutsioonide, organite ja ametite ning liikmesriikide üliarvukaid tegevusi on vaja dubleerimise vältimiseks kooskõlastada, mistõttu tasub kaaluda mõtet määrata kooskõlastamise eest vastutav ametiisik, tõenäoliselt ELi küberjulgeoleku koordinaatori ametikoha loomisega;
43. rõhutab, et elutähtsate infoinfrastruktuuride kaitsega tegelevate ELi ja USA peamiste asjaosaliste ja seadusandjate vaheline struktureeritud dialoog on eriti tähtis ühiste arusaamade loomiseks ning õigus- ja juhtimisraamistike ühesuguseks tõlgendamiseks ja nende suhtes ühesugustele seisukohtadele jõudmiseks;
44. väljendab heameelt 2010. aasta novembris toimunud ELi–USA tippkohtumisel loodud ELi ja USA küberjulgeoleku ja küberkuritegevuse vastase võitluse töörühma üle ning toetab selle pingutusi kaasata Atlandi-ülesesse poliitilisse dialoogi internetiturvalisuse küsimused; väljendab heameelt selle üle, et komisjon ja USA valitsus koostasid ELi ja USA töörühma raames koos ühise programmi ja tegevuskava, et korraldada 2012./2013. aastal ühised / samal ajal toimuvad mandritevahelised küberõppused;
45. teeb ettepaneku luua ELi ja USA seadusandjate vaheline struktureeritud dialoog internetiga seotud probleemide arutamiseks, et püüda leida ühised arusaamad, tõlgendused ja seisukohad;
46. nõuab tungivalt, et Euroopa välisteenistus ja komisjon kindlustaksid Euroopa liikmesriikide foorumi tehtud töö põhjal aktiivse seisukoha asjaomastes rahvusvahelistes foorumites, koordineerides muu hulgas liikmesriikide seisukohti ELi põhiliste väärtuste, eesmärkide ja poliitikate edendamiseks interneti turvalisuse ja vastupidavuse valdkonnas; märgib, et sellisteks foorumiteks on NATO, ÜRO (eelkõige Rahvusvahelise Telekomunikatsiooni Liidu ja Interneti Haldamise Foorumi kaudu), Interneti nimede ja numbrite määramise korporatsioon, internetiaadresse haldav organisatsioon IANA, OSCE, OECD ning Maailmapank;
47. julgustab komisjoni ja ENISAt osalema peamiste sidusrühmade dialoogides, et määratleda rahvusvahelisel tasandil küberruumi tehnilised ja õigusnormid;
48. teeb presidendile ülesandeks edastada käesolev resolutsioon nõukogule ja komisjonile.

SELETUSKIRI

Tehnoloogia osakaal on kõigis meie igapäevaelu aspektides jätkuvalt suurenenud, ulatudes kommunikatsioonist rahanduse ja panganduseni, transpordist energeetikani, kultuurist ja meelelahutusest tervishoiuni.

Tänapäeval, kus kasutatakse üha rohkem interneti ja arvutipõhiseid tehnoloogiaid, on interneti turvalisus Euroopa Liidu ja ülejäänud maailma üks tähtsamaid poliitilisi prioriteete. 2010. aastal käivitatud ELi 2020. aasta strateegias on juhtalgatuseks ELi digitaalne tegevuskava, mis seab Euroopa Liidu tehnoloogilisele arengule ambitsioonikad eesmärgid. Innovaatiliste IKT-tehnoloogiate, nagu kiire ja ülikiire paikne ja mobiilne internet ning mobiilside võrgud, arukad võrgud, aga ka internetiteenuste, nagu pilvandmetöötlus ja asjade internet, kasvav kasutamine ja rakendamine põhineb ühel lihtsal, kuid olulisel aspektil: turvalisus, vastupidavus ja usaldus.

2006. aasta detsembris võttis komisjon vastu teatise Euroopa elutähtsate infrastruktuuride kaitse Euroopa programmi (EPCIP) kohta. Selles kehtestatakse üldine raamistik elutähtsate infrastruktuuride kaitse alasele tegevusele ELi tasandil. Kaks aastat hiljem võttis nõukogu vastu direktiivi nr 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta. Esimeses etapis keskenduti direktiivis energeetika- ja transpordisektorile. Selles käsitleti ainult neid infrastruktuure, mille häired mõjutaksid kahte või enamat ELi liikmesriiki.

Direktiivis 2008/114 määratleti IKT-sektor kui tulevane esmatähtis sektor, kuigi seda ei liigitatud kriitiliseks infrastruktuuriks. Sellele vaatamata on komisjon 2005. aastast alates rõhutanud pingutuste koordineerimise vajadust elektroonilise kommunikatsiooni suhtes usalduse ja kindlustunde loomisel¹. Selleks võeti 2006. aastal vastu turvalise infoühiskonna strateegia², mille peamised koostisosid toetati nõukogu resolutsioonis nr 2007/068/01.

2009. aastal võttis komisjon vastu teatise pealkirjaga „Euroopa kaitsmine laiaulatuslike küberrünnakute ja häirete eest: valmisoleku, turvalisuse ja vastupidavuse suurendamine”³. Selle teatisega kehtestas komisjon elutähtsate infoinfrastruktuuride kaitse tegevuskava, mille eesmärgiks on soodustada ja toetada elutähtsate infoinfrastruktuuride turvalisust nii liikmesriikide kui ka liidu tasandil. Tegevuskavas määratletakse komisjoni, ENISA, liikmesriikide ja tööstusharu konkreetne roll. IKT-infrastruktuuride turvalisuse ja vastupidavuse suurendamise probleemi käsitleti veelgi intensiivsemalt Euroopa digitaalarengu tegevuskavas⁴ ja sellega seotud nõukogu järeldustes⁵, ettepanekus võtta vastu direktiiv infosüsteemide vastu suunatud rünnete kohta⁶, ning samuti komisjoni ettepanekus anda tugevdatud ja kaasajastatud ENISA-le uued volitused⁷.

¹ COM(2005) 229.

² COM(2006) 251.

³ COM(2009) 149.

⁴ COM(2010) 245.

⁵ Nõukogu 31. mai 2010. aasta järeldused.

⁶ COM(2010) 517.

⁷ COM(2010) 521.

2011. aasta märtsis avaldas komisjon teatise elutähtsate infoinfrastruktuuride kaitse kohta: „Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas”¹. Selles dokumendis vaatleb komisjon 2009. aastast pärineva elutähtsate infoinfrastruktuuride kaitse tegevuskava rakendamise tulemusi ja kirjeldab järgmisi võetavaid samme, pöörates enam tähelepanu ELi piiridest kaugemale ulatuvale rahvusvahelisele koostööle.

Kõik need mõne aasta jooksul toimunud muutused, millega liidu küberruumi turvalisuse suurendamise pingutused ei ole veel lõppenud, näitavad, et internetiturvalisuse probleem on püsiv. On ilmne, et internet on elutähtis infrastruktuur ning et internetikatkestus võib põhjustada ulatuslikke kahjusid ja turvariske, mis mõjutavad väga paljusid Euroopa kodanikke ja ettevõtteid. Lisaks nõuab tehnoloogia kiire areng, et internetirünnete ärahoidmine, korrektiivsed meetmed ja ülemaailmse võrgu vastupidavus põhineks laiahaardelisel, reageerimisvõimelisel, paindlikul, innovaatilisel ja pikaajalisel raamistikul. See raamistik peab tagama tõhusa suhtluse valitsuste, ettevõtete, üksikisikute ja kõigi muude sidusrühmade vahel. Lõpetuseks tuleks mainida, et interneti suurem vastupidavus on võimalik vaid juhul, kui on kehtestatud tõhus rahvusvahelise koostöö ja rahvusvaheliste normide süsteem.

¹ COM(2011) 163 final.

22.3.2012

KODANIKUVABADUSTE, JUSTIITS- JA SISEASJADE KOMISJONI ARVAMUS

tööstuse, teadusuuringute ja energeetikakomisjonile

elutähtsate infoinfrastruktuuride kaitse kohta. Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas
(2011/2284(INI))

Arvamuse koostaja: Ágnes Hankiss

ETTEPANEKUD

Kodanikuvabaduste, justiits- ja siseasjade komisjon palub vastutaval tööstuse, teadusuuringute ja energeetikakomisjonil lisada oma resolutsiooni ettepanekusse järgmised ettepanekud:

1. on seisukohal, et elutähtsate infoinfrastruktuuride kaitse nõuab interdistsiplinaarset lähenemist, mis peab hõlmama kodanikuvabaduste ning justiits- ja siseasjade selliseid olulisi aspekte, nagu sisejulgeolek, isikuandmete kaitse ning õigus konfidentsiaalsusele ja eraelule, nii et koos julgeoleku tugevdamisega respektieritaks põhiõigusi;
2. tuletab meelde, et elutähtsate infoinfrastruktuuride kaitse on lisatud ELi sisejulgeoleku strateegiasse seoses küberruumi turvalisuse taseme tõstmisega kodanike ja ettevõtjate jaoks;
3. nõuab tungivalt Euroopa elutähtsate infrastruktuuride kindlaksmääramise lõpuleviimist ja pidevat ajakohastamist komisjoni järelevalve all kooskõlas nõukogu direktiiviga 2008/114 Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta¹; rõhutab ühtlasi vajadust luua Euroopa tasandil võimalikult kiiresti elutähtsate infrastruktuuridega seotud teabe vahetuse infosüsteem; rõhutab, et arvestades avalik-õiguslike asutuste, ettevõtete ja kodumajapidamiste suurt sõltuvust info- ja kommunikatsioonitehnoloogiast (IKT), tuleks läbi vaadata nõukogu direktiiv 2008/114/EÜ, et tunnustada ka IKTd elutähtsa valdkonnana;
4. kutsub liikmesriike üles töötama välja riiklikku strateegiat ja tagama usaldusväärne poliitikakujundus ja õiguskeskkond, igakülgsed riskijuhtimismenetlused ning asjakohased

¹ ELT L 345, 23.12.2008, lk 75.

ettevalmistavad meetmed ja mehhanismid; nõuab tungivalt, et liikmesriigid, kus veel oma riiklikku infoturbeintsidentidega tegelevat rühma (CERT) asutatud ei ole, selle õigeaegselt asutaksid, kasutades vajaduse korral Euroopa Võrgu- ja Infoturbeameti (ENISA) abi;

5. on seisukohal, et elutähtsa infoinfrastruktuuri osaks tuleb pidada kõiki suuremahulisi andmebaase, milles käsitletakse delikaatseid isikuandmeid, näiteks ELi, liikmesriikide valitsuste ning finants- ja tervishoiuasutuste andmebaase, ja et kõnealuste andmete kaitse peab vastama kõrgeimatele standarditele;
6. kutsub komisjoni ja liikmesriike üles võtma vajalikke meetmeid elutähtsate infrastruktuuride kaitseks küberrünnakute eest ja tagada vahendid, millega katkestada juurdepääs elutähtsale infrastruktuurile, kui otsene küberrünnak tõsiselt selle ohustab nõuetekohast toimimist;
7. rõhutab, kui tähtsad on ulatuslikele võrguturbeintsidentidele reageerimiseks üleeuroopalised õppused ning ühtsete ohuhinnangu standardite kindlaksmääramine;
8. on seisukohal, et ENISA võib Euroopa tasandil olla elutähtsate infoinfrastruktuuride kaitsel keskne roll liikmesriikidele ning Euroopa Liidu institutsioonidele ja asutustele tehniliste eriteadmiste andmise kaudu ning Euroopa ja üleilmsel tasandil infosüsteemide turvalisust käsitlevate aruannete ja analüüside koostamise teel;
9. arvab, et EList kaugemale ulatuv rahvusvaheline koostöö on hädavajalik, sest küberohud on oma olemuselt üleilmsed ning nõuavad üleilmset reageerimist vastavalt rahvusvahelise õiguse normidele; rõhutab ühtlasi, et kõigis tundlike andmete vahetamist käsitlevates rahvusvahelistes lepingutes tuleks arvesse võtta andmete edastamise ja säilitamise turvalisust;
10. toonitab, et komisjoni tulevases interneti julgeoleku strateegias tuleks keskseks lähtepunktiks võtta töö elutähtsate infoinfrastruktuuride kaitsel ning seada eesmärgiks terviklik ja süstemaatiline lähenemine küberjulgeolekule, mis hõlmab nii ennetavaid meetmeid, nt julgeolekumeetmete miinimumstandardite kehtestamist või üksikkasutajate, ettevõtete ja avalik-õiguslike asutuste koolitamist, kui ka reageerivaid meetmeid, nt kriminaal- ning tsiviilõiguslikke ja halduskaristusi;
11. on seisukohal, et ELi-sisest kooskõlastamist infosüsteemide vastaste rünnakute ennetamisel, nende vastu võitlemisel ja nende eest karistamisel tuleb tugevdada ja laiendada, eelkõige tsiviil- ja sõjaväeliste osapoolte vahel ning ka kohtu- ja muude pädevate asutuste, sealhulgas liikmesriikide politsei- ja muude õiguskaitseasutuste vahel ning samuti selliste Euroopa tasandi asutuste vahel nagu Eurojust, Europol ja ENISA;
12. rõhutab avaliku ja erasektori vahelise tugeva koostöö tähtsust, sest nende sektorite erinevad tugevad küljed peaksid üksteist vastastikku täiendades toetama infrastruktuuri kaitseks tehtavaid pingutusi ning seega Euroopa kodanike elu ja eraelu puutumatust; palub komisjonil rajada Euroopa avaliku ja erasektori partnerlus vastupidavuse nimel, mis integreeritaks ENISA ja Euroopa valitsuste infoturbeintsidentidega tegelevate rühmade (CERT) tööga;
13. juhib tähelepanu sellele, et eri rahvusvaheliste ja ELi institutsioonide, organite ja ametite

ning liikmesriikide üliarvukaid tegevusi on vaja kattumise vältimiseks kooskõlastada, mistõttu tasub kaaluda mõtet määrata kooskõlastamise eest vastutav ametiisik, tõenäoliselt ELi küberturbekoordinaatori ametikoha loomisega;

14. on seisukohal, et elutähtsate infoinfrastruktuuride kaitse parandab lisaks kodanike üldise julgeoleku tugevdamisele ka kodanike arusaama julgeolekust ning usaldust nende kaitseks võetavate valitsuse meetmete vastu;
15. toonitab, kui tähtis on luua ja tagada Euroopa teadustöö kestav integratsioon, et säilitada ja tugevdada Euroopa tipptaset elutähtsate infoinfrastruktuuride kaitse valdkonnas;
16. rõhutab toimiva teadusuuringute kava tähtsust küberjulgeoleku valdkonnas;
17. toetab elutähtsate infoinfrastruktuuride kaitse valdkonnas küberjulgeoleku alase hariduse (doktorantide praktika, ülikoolikursused, seminarid, üliõpilaste koolitamine jne) ja eriväljaõppe kursuste edendamist;
18. toetab tihedat suhtlust ja koostööd liikmesriikide erasektorite ning ENISA vahel, et teavitada riikide/valitsuste infoturbeintsidendidega tegelevaid rühmi (CERT) Euroopa teabe jagamise ja hoiatussüsteemi (EISAS) arengust;
19. rõhutab, kui tähtis meetmete ja vajalike vahendite seisukohalt on ühine Euroopa küberjulgeoleku strateegia ja selle määratlemise ajakava kehtestamine;
20. toonitab elutähtsate infoinfrastruktuuride kaitsega tegelevate peamiste ELi ja USA asjaosaliste ja seadusandjate vahelise struktureeritud dialoogi tähtsust vastastikuse mõistmise ning õigus- ja juhtimisraamistike ühesuguse tõlgendamise ning nende suhtes ühesugustele seisukohtadele jõudmise jaoks.

PARLAMENDIKOMISJONIS TOIMUNUD LÕPPHÄÄLETUSE TULEMUS

Vastuvõtmise kuupäev	21.3.2012
Lõpphääletuse tulemus	+: 45 –: 0 0: 2
Lõpphääletuse ajal kohal olnud liikmed	Roberta Angelilli, Edit Bauer, Arkadiusz Tomasz Bratkowski, Philip Claey's, 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
Lõpphääletuse ajal kohal olnud asendusliige/asendusliikmed	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
Lõpphääletuse ajal kohal olnud asendusliige/asendusliikmed (kodukorra art 187 lg 2)	Luis de Grandes Pascual

PARLAMENDIKOMISJONIS TOIMUNUD LÕPPHÄÄLETUSE TULEMUS

Vastuvõtmise kuupäev	8.5.2012
Lõpphääletuse tulemus	+: 51 –: 7 0: 0
Lõpphääletuse ajal kohal olnud liikmed	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
Lõpphääletuse ajal kohal olnud asendusliige/asendusliikmed	Ioan Enciu, Françoise Grossetête, Takis Hadjigeorgiou, Roger Helmer, Jolanta Emilia Hibner, Bernd Lange, Werner Langen, Zofija Mazej Kukovič, Silvia-Adriana Țicău, Inês Cristina Zuber
Lõpphääletuse ajal kohal olnud asendusliige/asendusliikmed (kodukorra art 187 lg 2)	Anne E. Jensen, Nicole Kiil-Nielsen, Norica Nicolai