EUROOPA PARLAMENT 2009–2014

*Istungidokument*

6.9.2013 B7-0386/2013

# RESOLUTSIOONI ETTEPANEK

komisjoni avalduse alusel

vastavalt kodukorra artikli 110 lõikele 2

Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum
(2013/2606(RSP))

**Malcolm Harbour, Andreas Schwab**
siseturu- ja tarbijakaitsekomisjoni nimel
**Elmar Brok, Tunne Kelam**
väliskomisjoni nimel

**B7-0386/2013**

**Euroopa Parlamendi resolutsioon Euroopa Liidu küberjulgeoleku strateegia kohta: avatud, ohutu ja turvaline küberruum**
**(2013/2606(RSP))**

*Euroopa Parlament*,

– võttes arvesse Euroopa Komisjoni ning liidu välisasjade ja julgeolekupoliitika kõrge esindaja 7. veebruari 2013. aasta ühisteatist „Euroopa Liidu küberjulgeoleku strateegia: avatud, ohutu ja turvaline küberruum” (JOIN(2013)1),

– võttes arvesse komisjoni 7. veebruari 2013. aasta ettepanekut võtta vastu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus (COM(2013)0048),

– võttes arvesse komisjoni 19. mai 2010. aasta teatist „Euroopa digitaalne tegevuskava” (COM (2010)0245) ja 18. detsembri 2012. aasta teatist „Euroopa digitaalarengu tegevuskava – Euroopa majanduskasvu kiirendamine digitaalsete vahenditega” (COM(2012)0784),

– võttes arvesse komisjoni 27. septembri 2012. aasta teatist „Pilvandmetöötluse võimaluste kasutamine Euroopas” (COM(2012)0529),

– võttes arvesse komisjoni 28. märtsi 2013. aasta teatist „Võitlus kuritegevusega digitaalajastul: küberkuritegevuse vastase võitluse Euroopa keskuse loomine” (COM(2012)0140) ja nõukogu 7. juuni 2012. aasta järeldusi selle kohta,

– võttes arvesse Euroopa Parlamendi ja nõukogu 12. augusti 2013. aasta direktiivi 2013/40/EL, milles käsitletakse infosüsteemide vastu suunatud ründeid ja millega asendatakse nõukogu raamotsus 2005/222/JSK[1],

– võttes arvesse nõukogu 8. detsembri 2008. aasta direktiivi 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta[2],

– võttes arvesse Euroopa Parlamendi ja nõukogu 13. detsembri 2011. aasta direktiivi 2011/92/EL, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust ja mis asendab nõukogu raamotsuse 2004/68/JSK[3],

– võttes arvesse Stockholmi programmi vabadusel, turvalisusel ja õiglusel rajaneval alal[4], komisjoni teatisi „Vabadusel, turvalisusel ja õigusel rajanev ala Euroopa kodanikele. Stockholmi programmi rakendamise tegevuskava” (COM(2010)0171) ja „ELi sisejulgeoleku strateegia toimimine: viis sammu turvalisema Euroopa suunas”

[1] ELT L 218, 14.8.2013, lk 8.
[2] ELT L 345, 23.12.2008, lk 75.
[3] ELT L 335, 17.12.2011, lk 1.
[4] ELT C 115, 4.5.2010, lk 1.

(COM(2010)0673) ja oma 22. mai 2012. aasta resolutsiooni Euroopa Liidu sisejulgeoleku strateegia kohta[1],

– võttes arvesse komisjoni ja kõrge esindaja ühisettepanekut, mis puudutab nõukogu otsust solidaarsusklausli liidupoolse rakendamise korra kohta (JOIN/2012/039),

– võttes arvesse nõukogu 28. mai 2001. aasta raamotsust 2001/413/JSK mittesularahaliste maksevahenditega seotud pettuste ja võltsimiste vastase võitluse kohta[2],

– võttes arvesse oma 12. juuni 2012. aasta resolutsiooni elutähtsate infoinfrastruktuuride kaitse kohta – saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas[3] ja nõukogu 27. mai 2011. aasta järeldusi komisjoni teatise „Elutähtsate infoinfrastruktuuride kaitse. „Saavutused ja edasised sammud: üleilmse küberjulgeoleku suunas”” kohta (COM(2011)0163),

– võttes arvesse oma 11. detsembri 2012. aasta resolutsiooni digitaalse ühtse turu rajamise lõpuleviimise kohta[4],

– võttes arvesse oma 22. novembri 2012. aasta resolutsiooni küberjulgeoleku ja -kaitse kohta[5],

– võttes arvesse oma 16. aprilli 2013. aasta seadusandlikku resolutsiooni ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus Euroopa Võrgu- ja Infoturbeameti (ENISA) kohta (COM(2010)521)[6], millega võeti vastu Euroopa Parlamendi seisukoht esimesel lugemisel,

– võttes arvesse oma 11. detsembri 2012. aasta resolutsiooni digitaalse vabaduse strateegia kohta ELi välispoliitikas[7],

– võttes arvesse Euroopa Nõukogu 23. novembri 2001. aasta küberkuritegevuse konventsiooni,

– võttes arvesse liidu rahvusvahelisi kohustusi, eelkõige neid, mis tulenevad teenuskaubanduse üldlepingust,

– võttes arvesse Euroopa Liidu toimimise lepingu artiklit 16 ja Euroopa Liidu põhiõiguste hartat, eriti selle artikleid 6, 8 ja 11[8],

– võttes arvesse Euroopa Liidu ja Ameerika Ühendriikide vahel Atlandi-ülese kaubandus- ja investeerimispartnerluse üle peetavaid läbirääkimisi,

– võttes arvesse kodukorra artikli 110 lõiget 2,

---

[1] Vastuvõetud tekstid, P7_TA(2012)0207.
[2] EÜT L 149, 2.6.2001, lk 1.
[3] Vastuvõetud tekstid, P7_TA(2012)0237.
[4] Vastuvõetud tekstid, P7_TA(2012)0468.
[5] Vastuvõetud tekstid, P7_TA(2012)0457.
[6] Vastuvõetud tekstid, P7_TA(2013)0103.
[7] Vastuvõetud tekstid, P7_TA(2012)0470.
[8] ELT C 83, 30.3.2010, lk 389.

A. arvestades, et järjest suurenevad kübervaldkonna probleemid, mis seisnevad üha keerukamates ohtudes ja rünnakutes, seavad tõsiselt ohtu liikmeriikide, erasektori ja laiema üldsuse julgeoleku, stabiilsuse ja majandusliku heaolu; arvestades, et ühiskonna ja majanduse kaitsmisel peame seetõttu arvestama pidevalt muutuvate oludega;

B. arvestades, et küberruum ja küberohutus peaksid ELi ja kõigi liikmesriikide puhul olema üheks julgeoleku- ja kaitsepoliitika strateegiliseks sambaks; arvestades, et küberruumis peab ka edaspidi olema võimalik ideid ja teavet vabalt levitada ja vabalt arvamust avaldada;

C. arvestades, et e-kaubanduses ja internetipõhistes teenustes väljendub internetis peituv võimas jõud ja need on vajalikud strateegia „Euroopa 2020" eesmärkide saavutamiseks, millest saavad kasu nii kodanikud kui ka erasektor; arvestades, et liit peab täielikult ära kasutama potentsiaali ja võimalused, mida internet ühtse turu, sh digitaalse ühtse turu edasise arengu jaoks pakub;

D. arvestades, et Euroopa Liidu küberjulgeoleku strateegiat käsitlevas ühisteatises sõnastatud strateegiliste prioriteetide kohaselt tuleb saavutada vastupidavus küberrünnakute suhtes, vähendada küberkuritegevust, töötada välja küberkaitsepoliitika ning ühise julgeoleku- ja kaitsepoliitikaga seotud kübersuutlikkus ja kehtestada ELi sidus rahvusvaheline küberruumipoliitika;

E. arvestades, et liidu võrgu- ja infosüsteemid on omavahel tihedalt seotud; arvestades, et kuna internet on oma olemuselt globaalne, siis ulatuvad paljud võrgu- ja infoturbega seotud juhtumid ühe riigi piiridest kaugemale ning võivad häirida siseturu toimimist ja vähendada tarbijate usaldust digitaalse ühtse turu vastu;

F. arvestades, et küberjulgeolek on liidus ja ka mujal maailmas ainult nii tugev kui on selle nõrgim lüli ja ühes sektoris või liikmesriigis esinevad häired võivad mõju avaldada muudele sektoritele ja liikmesriikidele, tekitades ülekanduva mõju kogu liidu majandusele;

G. arvestades, et 2013. aasta aprilli seisuga olid riikliku küberjulgeoleku strateegia ametlikult vastu võtnud ainult 13 liikmesriiki; arvestades, et liikmesriikide valmisolek, julgeolek, strateegiakultuur ja riikliku küberjulgeoleku strateegia väljatöötamise ja rakendamise võime on endiselt väga erinev, ja arvestades, et neid erinevusi tuleks analüüsida;

H. arvestades, et julgeolekukultuuride erinevus ja õigusraamistiku puudumine põhjustab killustatust ja on digitaalsel ühtsel turul suur probleem; arvestades, et küberjulgeoleku ühtse käsitluse puudumine kujutab tõsist ohtu majanduslikule heaolule ja tehingute turvalisusele, ja arvestades, et seetõttu peavad valitsused, erasektor, õiguskaitse- ja luureasutused tegema kooskõlastatud pingutusi ja tihedamat koostööd;

I. arvestades, et küberkuritegevus on järjest kulukam rahvusvaheline probleem, sest sellega seotud kulu on ÜRO uimastite ja kuritegevuse vastu võitlemise büroo andmeil kogu maailmas kokku umbes 295 miljardit eurot aastas;

J. arvestades, et rahvusvaheline organiseeritud kuritegevus on tehnoloogia arengut ära kasutades suundumas üha enam küberruumi, milles tegusemise tõttu on organiseeritud

kuritegelike rühmituste traditsiooniline struktuur asendunud täiesti uuega; arvestades, et seetõttu on organiseeritud kuritegevus vähem kohalik ning pigem tegutsetakse üle kogu maailma eri piirkondades ja õigussüsteemides;

K. arvestades, et pädevatel asutustel takistavad küberkuritegevuse uurimist endiselt mitu tegurit, sealhulgas küberruumi tehingutes kasutatavad virtuaalsed vääringud, mida võidakse kasutada rahapesuks, territoriaalsuse probleemid ja õigussüsteemide piirid, puudulikud vahendid jälitusteabe jagamiseks, kvalifitseeritud personali vähesus ja ebaühtlane koostöö muude sidusrühmadega;

L. arvestades, et tehnoloogia on küberruumi arengu alus ning ELi küberruumi vastupidavuse ja ohutuse parandamiseks tuleb tehnoloogiliste muutustega pidevalt kaasas käia; arvestades, et tuleb võtta meetmeid, millega tagada, et õigusaktid oleksid tehnoloogia arengut arvestades ajakohased ning võimaldaksid küberkurjategijad kindlaks teha ja nende üle kohut mõista ning kaitsta küberkuritegevuse ohvreid;

1. tunneb heameelt Euroopa Liidu küberjulgeoleku strateegiat käsitleva ühisteatise üle ja ettepaneku üle võtta vastu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu liidus;

2. rõhutab, et internet ja küberruum on muutumas poliitiliste, majanduslike ja ühiskondlike toimingute jaoks veelgi tähtsamaks mitte ainult liidus, vaid ka seoses muude osalistega kogu maailmas;

3. rõhutab, et ELi küberjulgeoleku, küberkriisiolukordade, strateegiliste ülevaadete, avaliku ja erasektori koostöö ning üldsusele antavate hoiatuste ja soovituste kohta tuleb välja töötada strateegilise teabevahetuse poliitika;

4. tuletab meelde, et võrgu- ja infoturve peab kõrgel tasemel olema mitte ainult selle pärast, et säilitada teenused, mida on vaja ühiskonna ja majanduse tõrgeteta toimimiseks, vaid ka selleks, et kaitsta elutähtsa taristu tõhususe, töökindluse ja turvalisuse suurendamise kaudu kodanike füüsilist puutumatust; rõhutab, et ühelt poolt tuleb küll tegeleda võrgu- ja infoturbega, kuid teiselt poolt tuleb parandada ka füüsilist puutumatust; rõhutab, et taristu peaks vastu pidama nii tahtlike kui ka tahtmatute häirete puhul; rõhutab, et seetõttu tuleks küberjulgeoleku strateegias suuremat rõhku panna tahtmatute süsteemihäirete sagedastele põhjustele;

5. tuletab liikmesriikidele meelde, et kutsub üles viivitamata vastu võtma riikliku küberjulgeoleku strateegia, mis hõlmab tehnilisi, koordineerimis-, inimressursi ja rahalise eraldise aspekte ning sisaldab erasektori kaasamiseks selgeid eeskirju selle kohta, millist kasu see erasektorile annab ja millised on erasektori kohustused, ning kehtestama üksikasjaliku riskijuhtimise korra ja kaitsma õiguskeskkonda;

6. märgib, et kõrgel tasemel võrgu- ja infoturve on kogu liidus võimalik tagada ja ühtse turu turvalist ja tõrgeteta toimimist edendada ainult siis, kui liidu institutsioonid ja liikmesriigid täidavad ühiselt juhirolli ja kannavad poliitilist vastutust;

7. rõhutab, et liidu küberjulgeoleku poliitika peaks looma turvalise ja usaldusväärse digitaalse keskkonna, mis põhineb eri vabaduste kaitsmisel ja säilitamisel ning

põhiõiguste, eelkõige eraelu puutumatuse ja andmekaitse õiguse austamisel internetis, ja mille eesmärk on nimetatud vabadusi ja õigusi kaitsta, nagu on sätestatud ELi hartas ja Euroopa Liidu toimimise lepingu artiklis 16; on seisukohal, et erilist tähelepanu tuleks pöörata laste kaitsmisele internetis;

8. kutsub liikmesriike ja komisjoni üles tegema kõik vajaliku, et koostada koolitusprogrammid, mille eesmärk on suurendada digitaaloskuste omandamise raames Euroopa Liidu kodanike teadlikkust, oskusi ja teadmisi eelkõige isikliku julgeoleku osas juba varasest east alates; tunneb heameelt algatuse üle viia Euroopa Liidu Võrgu- ja Infoturbeameti (ENISA) toel ning koostöös avaliku sektori asutuste ja erasektoriga läbi Euroopa küberjulgeoleku kuu, mille eesmärk on suurendada teadlikkust probleemidest, mis kaasnevad võrgu- ja infosüsteemide kaitsmisega;

9. on seisukohal, et küberjulgeolekualane haridus suurendab Euroopa ühiskonna teadlikkust küberohtudest ja innustab küberruumi vastutustundlikult kasutama ning aitab suurendada pakutavate küberteadmiste hulka; tunnistab, et Europolil ja selle uuel küberkuritegevuse vastase võitluse Euroopa keskusel (EC3), ENISA-l ja Eurojustil on põhiroll ELi tasandil koolituse pakkumisel rahvusvahelise õiguskoostöövahendite kasutamise ja küberkuritegevuse eri aspektidega seotud õiguskaitse kohta;

10. kordab, et tuleb anda tehnilist nõu ja õigusalast teavet ning luua küberkuritegevuse ennetamise ja sellega võitlemise programmid; innustab koolitama küberinsenere, kes spetsialiseeruksid elutähtsa taristu ja infosüsteemide kaitsmisele, ning transpordikontrolli süsteemide ja liiklusjuhtimiskeskuste käitajaid; rõhutab, et avaliku sektori kõigi tasandite töötajate jaoks tuleb tingimata kehtestada korrapärase küberjulgeolekualase koolituse kavad;

11. kordab, et kui soovitakse piirata kodanike võimalusi kasutada kommunikatsiooni- ja infotehnoloogiavahendeid, tuleb seda teha ettevaatlikult, ja rõhutab, et liikmesriigid peaksid küberohtude ja -rünnakute vastaste meetmete väljatöötamisel igal juhul hoiduma kodanike õiguste ja vabaduste ohtu seadmisest ja neil peaksid tsiviil- ja militaartasandi küberjuhtumite eristamiseks olema asjakohased õiguslikud vahendid;

12. on seisukohal, et küberjulgeoleku alastes õigusaktides tuleks arvesse võtta riske, keskenduda elutähtsale taristule, mille toimimine on igati üldsuse huvides, ja tugineda turupõhistele pingutustele, mida ettevõtted teevad võrgu vastupidavuse tagamiseks; rõhutab, et praktilisel tasandil tuleb teha nii liidu kui ka liikmesriikide tasandil ja liidu strateegiliste partneritega koostööd, et tõhustada avaliku sektori asutuste ja erasektori vahel küberohtude alase teabe vahetamist, tagamaks võrgu- ja infoturbe, luues vastastikust usaldust, väärtusi ja pühendumust ning vahetades teadmisi; on seisukohal, et avaliku ja erasektori partnerlused peaksid põhinema võrkude ja tehnoloogia neutraalsusel ja keskenduma pingutustele, mille eesmärk on lahendada probleeme, mis avaldavad üldsusele suurt mõju; kutsub komisjoni üles innustama kõiki asjaomaseid turuosalisi näitama üles suuremat valvsust ja koostöötahet, et kaitsta teisi turuosalisi nende teenustele kahju tekitamise eest;

13. tunnistab, et küberjulgeoleku intsidentide tuvastamine ja nendest teatamine on hädavajalik, et edendada liidus vastupidavust küberrünnakute suhtes; usub, et peaksid kehtima proportsionaalsed ja vajalikud avalikustamisnõuded, et märkimisväärseid

julgeolekurikkumisi hõlmavatest intsidentidest teavitataks pädevaid riiklikke asutusi, mis võimaldaks küberkuritegevuse juhtumeid paremini jälgida ning hõlbustaks kõikidel tasanditel teadlikkust tõsta;

14. ergutab komisjoni ja teisi osapooli kehtestama küberjulgeolekut ja vastupidavust küberrünnakute suhtes käsitlevat poliitikat, mis hõlmaks majanduslikke stiimuleid kõrgetasemelise küberjulgeoleku ja vastupidavuse edendamiseks;

***Vastupidavus küberrünnakute suhtes***

15. märgib, et eri sektorites ja liikmesriikides on erinevad võimalused ja oskused ning see takistab usaldusliku koostöö arengut ning pärsib ühtse turu toimimist;

16. on seisukohal, et nõuded väikestele ja keskmise suurusega ettevõtjatele peaksid lähtuma proportsionaalsest ja riskipõhisest lähenemisviisist;

17. nõuab tungivalt, et arendataks elutähtsa taristu vastupidavust küberrünnakute suhtes, ning tuletab meelde, et tulevane kord solidaarsusklausli (ELi toimimise lepingu artikkel 222) rakendamiseks peaks arvestama liikmesriigi vastu suunatud küberrünnaku ohtu; palub komisjonil ja kõrgel esindajal võtta seda ohtu arvesse ühiste terviklike ohu- ja riskihindamisaruannete puhul, mida tuleb alates 2015. aastast esitada;

18. rõhutab, et eelkõige elutähtsate teenuste usaldusväärsuse, kättesaadavuse ja konfidentsiaalsuse tagamiseks peab elutähtsa taristu loetelu ja jaotus olema ajakohane ning peavad olema kehtestatud minimaalsed turvanõuded nende võrgu- ja infosüsteemide jaoks;

19. märgib, et ettepanekus võtta vastu direktiiv meetmete kohta, millega tagada võrgu- ja infoturbe ühtlaselt kõrge tase kogu Euroopa Liidus, nähakse ette infoühiskonna teenuste osutajatele ja elutähtsa taristu operaatoritele minimaalsed turvanõuded;

20. palub liikmesriikidel ja liidul kehtestada sobivad raamistikud kiiretele kahesuunalistele teabevahetussüsteemidele, mis tagavad erasektori jaoks anonüümsuse ning annavad avalikule sektorile pidevalt ajakohast teavet, ning pakkuda vajaduse korral erasektorile abi;

21. väljendab heameelt komisjoni idee üle luua seoses küberjulgeolekuga riskijuhtimiskultuur ning nõuab tungivalt, et liikmesriigid ja liidu institutsioonid lisaksid küberkriiside ohjamise kiiresti oma kriisiohjamiskavadesse ja riskianalüüsidesse; lisaks sellele palub liikmesriikide valitsustel ja komisjonil ergutada erasektori osalejaid lisama küberkriisi ohjamise oma juhtimiskavadesse ja riskianalüüsidesse ning koolitama oma töötajaid küberjulgeoleku valdkonnas;

22. palub, et kõik liikmesriigid ja liidu institutsioonid looksid hästi toimivate, infoturbeintsidentidega tegelevate rühmade (CERTide) võrgustiku, mis toimib 24 tundi päevas ja 7 päeva nädalas; juhib tähelepanu, et riikide CERTid peaksid kuuluma tõhusasse võrgustikku, milles vahetatakse asjakohast teavet kooskõlas vajalike usaldus- ja konfidentsiaalsusstandarditega; märgib, et CERTe ja muid asjaomaseid turvaorganeid ühendavad katusalgatused võivad aidata luua usaldust piiri- ja sektoriüleses kontekstis;

tunnistab CERTide ja õiguskaitseasutuste tõhusa ja tulemusliku koostöö tähtsust võitluses küberkuritegevuse vastu;

23. toetab ENISAt tema kohustuste täitmisel seoses võrgu- ja infoturbega, eriti liikmesriikide nõustamisel ja juhendamisel, aga ka parimate tavade vahetamise toetamisel ning usaldusliku keskkonna loomisel;

24. rõhutab, et tööstus peab transpordivõrkudes ja infosüsteemides kasutatavate IKT toodete puhul rakendama kogu väärtusahela ulatuses sobivaid küberjulgeolekualaseid nõudeid, asjakohaselt riske ohjama, võtma vastu turvastandardid ja -lahendused, ning arendama parimate tavade ja teabe vahetamist, eesmärgiga tagada küberrünnakute vastu kaitstud transpordisüsteemid;

***Tööstuslikud ja tehnoloogilised ressursid***

25. on seisukohal, et võrgu- ja infoturbe kõrge taseme tagamine on kesksel kohal turvalahenduste pakkujate ja kasutajate konkurentsivõime suurendamisel liidus; on seisukohal, et ehkki liidu IT-julgeolekutööstusel on märkimisväärne hulk kasutamata potentsiaali, ei ole avaliku ja erasektori ega ärikasutajaid sageli teadlikud küberjulgeolekusse investeerimise kuludest ja sellest saadavast kasust ning seetõttu on nad kahjulike küberrünnakute suhtes haavatavad; rõhutab, et CERTide rakendamine on sellega seoses oluline tegur;

26. on veendunud, et tugev pakkumine ja nõudlus küberturbelahenduste valdkonnas eeldab IKT küsimustega tegelevate riiklike asutuste poolt piisavaid investeeringuid akadeemilistesse vahenditesse, teadus- ja arendustegevusse ning teadmiste ja võimekuse suurendamisse, et edendada innovatsiooni ning saavutada piisav teadlikkus võrgu- ja infoturberiskidest, mis on samm Euroopa ühtse julgeolekutööstuse suunas;

27. palub liidu institutsioonidel ja liikmesriikidel võtta vajalikud meetmed, et luua küberjulgeoleku ühtne turg, kus kasutajad ja tarnijad saavad innovatsiooni, sünergiat ja kombineeritud oskusi parimal viisil ära kasutada ning mis on avatud VKEdele;

28. ergutab liikmesriike kaaluma ühiste investeeringute tegemist Euroopa küberjulgeolekutööstusse, nagu on tehtud teiste tööstusharude puhul, nt lennundussektoris;

***Küberkuritegevus***

29. on seisukohal, et kuritegevus küberruumis võib olla ühiskonna heaolule niisama kahjulik nagu kuritegevus füüsilises maailmas ning et need kuritegevuse vormid sageli soodustavad teineteist, nagu võib näha näiteks laste seksuaalse ärakasutamise, organiseeritud kuritegevuse ja rahapesu puhul;

30. märgib, et mõnel juhul on seaduslik ja ebaseaduslik äritegevus omavahel seotud; rõhutab olulist seost (mida hõlbustab internet) terrorismi rahastamise ja raske organiseeritud kuritegevuse vahel; rõhutab, et üldsus peab aru saama, kui tõsised tagajärjed on küberkuritegevuses osalemisel, ning mõistma, et see, mis esmapilgul võib tunduda „ühiskondlikult aktsepteeritava” kuriteona – nt filmide ebaseaduslik allalaadimine –,

tekitab sageli suuri rahasummasid rahvusvahelistele kuritegelikele sündikaatidele;

31. nõustub komisjoniga, et samad normid ja põhimõtted, mis kehtivad füüsilises maailmas, kehtivad ka internetis, ning seetõttu tuleks võitlust küberkuritegevuse vastu tõhustada ajakohaste õigusaktide ja tegutsemisvõimega;

32. on seisukohal, et küberkuritegevuse piirideta olemust arvestades on eriti tähtsad üksikute liikmesriikide tasandist kõrgemal, st liidu tasandil tehtavad ühised jõupingutused ja pakutavad eksperditeadmised ning et Eurojustile, Europoli EC3-le, CERTidele, ülikoolidele ja teaduskeskustele tuleb seetõttu anda piisavad vahendid ja võimalused, et toimida ekspertiisi-, koostöö- ja teabejagamiskeskustena;

33. väljendab suurt heameelt EC3 loomise üle ning ergutab edasi arendama seda ametit ja tema tähtsat rolli teabe ja eksperditeadmiste õigeaegse ja tõhusa piiriülese vahetamise koordineerijana küberkuritegevuse ennetamise, avastamise ja uurimise toetuseks;

34. palub liikmesriikidel tagada, et kodanikud pääseksid kergesti ligi teabele küberohtude ja nende vastu võitlemise kohta; on veendunud, et need suunised peaksid hõlmama teavet selle kohta, kuidas kasutajad saavad internetis oma privaatsust kaitsta, kuidas tuvastada seksuaalsuhte eesmärgil kontakti otsimise juhtumeid ja neist teada anda, kuidas paigaldada tarkvara ja tulemüüre, kuidas hallata salasõnu ning kuidas panna tähele andmepüüki, andmelõikust ja muid rünnakuid;

35. nõuab tungivalt, et liikmesriigid, kes ei ole veel ratifitseerinud Euroopa Nõukogu Budapesti konventsiooni küberkuritegevuse kohta, teeksid seda viivitamata; väljendab heameelt Euroopa Nõukogu seisukohtade üle vajaduse kohta ajakohastada konventsiooni tehnoloogilise arengu valguses, et tagada selle jätkuv tõhusus küberkuritegevuse vastu võitlemisel, ning palub komisjonil ja liikmesriikidel selles arutelus osaleda; ergutab jõupingutusi konventsiooni ratifitseerimise edendamiseks teistes riikides ning palub komisjonil seda väljaspool liitu aktiivselt propageerida;

***Küberkaitse***

36. rõhutab, et küberprobleemid, -ohud ja -rünnakud seavad ohtu liikmesriikide kaitsealased ja riikliku julgeolekuga seotud huvid ning et tsiviil- ja sõjaline lähenemisviis elutähtsa taristu kaitsmisele peaksid andma sünergia kaudu kasu mõlemale;

37. seepärast palub liikmesriikidel tõhustada koostööd Euroopa Kaitseagentuuriga (EDA), et töötada välja ettepanekud ja algatused küberkaitsevõimekuse kohta, lähtudes uuematest algatustest ja projektidest; rõhutab vajadust suurendada teadus- ja arendustegevust, muu hulgas vahendite ühendamise ja jagamise abil;

38. kordab, et terviklik ELi küberjulgeoleku strateegia puhul tuleks arvesse võtta olemasolevate ametite ja organite lisaväärtust, samuti nende liikmesriikide häid tavasid, kes on juba vastu võtnud riiklikud küberjulgeoleku strateegia;

39. palub asepresidendil ja kõrgel esindajal lisada küberkriiside ohjamine kriisiohjekavadesse, ning rõhutab, et liikmesriigid peaksid koostöös EDAga töötama välja kavad, kuidas kaitsta ÜVJP missioone ja operatsioone küberrünnakute eest; palub neil koondada Euroopa

küberkaitsejõu;

40. juhib tähelepanu NATOga küberjulgeoleku valdkonnas tehtavale heale praktilisele koostööle ning vajadusele seda koostööd tõhustada, eriti parema koordineerimise abil kavandamise, tehnoloogia, koolituse ja varustuse valdkonnas;

41. nõuab, et liit teeks jõupingutusi arutelu alustamiseks rahvusvaheliste partneritega, sh NATOga, et määrata kindlaks koostöövaldkonnad, vältida topelttööd ning täiendada igal võimalusel üksteise tegevust;

***Rahvusvaheline poliitika***

42. on veendunud, et rahvusvaheline koostöö ja arutelu mängivad väga olulist rolli usalduse ja läbipaistvuse loomisel ning kõrgetasemelise suhtluse ja teabevahetuse edendamisel ülemaailmsel tasandil; seepärast palub komisjonil ja Euroopa välisteenistusel luua küberdiplomaatia meeskond, kelle kohustuste hulka kuuluks arutelu edendamine sarnaselt meelestatud riikide ja organisatsioonidega; nõuab ELi aktiivsemat osalemist mitmesugustel küberjulgeolekut käsitlevatel kõrgetasemelistel rahvusvahelistel konverentsidel;

43. on seisukohal, et tuleb leida tasakaal piiriülese andmeedastuse, andmekaitse ja küberjulgeoleku vastandlike eesmärkide vahel kooskõlas liidu rahvusvaheliste kohustustega, eelkõige teenuskaubanduse üldlepingu raames;

44. palub, et asepresident ja kõrge esindaja süvalaiendaks küberjulgeoleku mõõdet ELi välistegevusse, eriti suhetes kolmandate riikidega, et tõhustada koostööd ning kogemuste ja teabe vahetamist küberjulgeoleku valdkonnas;

45. nõuab, et liit teeks jõupingutusi arutelu alustamiseks rahvusvaheliste partneritega, et määrata kindlaks koostöövaldkonnad, vältida topelttööd ning täiendada igal võimalusel üksteise tegevust; palub, et asepresident ja kõrge esindaja ning komisjon tegutseksid rahvusvahelistes organisatsioonides ennetavalt ning koordineeriksid liikmesriikide seisukohti küsimustes, kuidas kübervaldkonnas lahendusi ja poliitikat tõhusalt edendada;

46. on seisukohal, et tuleks teha jõupingutusi tagamaks, et olemasolevaid rahvusvahelisi õiguslikke instrumente, eriti Euroopa Nõukogu küberkuritegevuse konventsiooni küberruumis jõustatakse; on seepärast seisukohal, et praegu puudub vajadus luua uusi rahvusvahelise tasandi instrumente; väljendab aga heameelt rahvusvahelise koostöö üle küberruumi käitumisnormide väljatöötamisel, mis toetab küberruumis õigusriigi põhimõtete järgimist; on seisukohal, et tuleks kaaluda olemasolevate õiguslike instrumentide ajakohastamist, et võtta arvesse tehnoloogia arengut; on seisukohal, et jurisdiktsiooniga seotud küsimused nõuavad põhjalikku arutelu õiguskoostöö ning süüdistuse esitamise üle rahvusvahelistes kriminaalasjades;

47. on seisukohal, et eelkõige ELi ja USA küberjulgeoleku ja küberkuritegevuse töörühm peaks aitama ELil ja USA-l vahetada vajaduse korral küberjulgeolekupoliitika parimaid tavasid; märgib sellega seoses, et tulevastel läbirääkimistel Atlandi-ülese kaubandus- ja investeerimispartnerluse üle käsitletakse ka küberjulgeolekuga seotud valdkondi, nt teenuseid, mis sõltuvad võrgu- ja infosüsteemide turvalisest toimimisest;

48. märgib, et küberjulgeolekuga seotud oskused ning võime ennetada, tuvastada ja tõhusalt kõrvaldada ohte ja pahatahtlikke rünnakuid, on maailmas ebavõrdselt arenenud; rõhutab, et jõupingutused vastupidavuse suurendamiseks küberrünnakute suhtes ja võitluseks küberohtude vastu ei tohi piirduda sarnaselt meelestatud partneritega, vaid need peaksid hõlmama ka vähem arenenud võimaluste, tehnilise taristu ja õigusraamistikuga piirkondi; on veendunud, et selles küsimuses on CERTide koordineerimine ülioluline; palub komisjonil hõlbustada ja vajaduse korral toetada kolmandate riikide jõupingutusi oma küberjulgeolekualase võimekuse arendamiseks, kasutades selleks sobivaid vahendeid;

***Rakendamine***

49. nõuab riiklike küberjulgeoleku strateegiate tõhususe regulaarset hindamist kõige kõrgemal poliitilisel tasandil, et tagada nende kohandamine uute globaalsete ohtudega ning tagada ühesugune küberjulgeoleku tase eri liikmesriikides;

50. palub komisjonil koostada selge tegevuskava, milles määratakse kindlaks küberjulgeoleku strateegia liidu tasandi eesmärkide saavutamise ja hindamise ajakava; palub liikmesriikidel leppida kokku sarnases kavas strateegia riiklike meetmete jaoks;

51. nõuab komisjonilt, liikmesriikidelt, Europolilt ja äsja asutatud EC3-lt, Eurojustilt ning ENISA-lt regulaarseid aruandeid, milles hinnatakse küberjulgeoleku strateegias seatud eesmärkide saavutamisel tehtud edusamme, sh tähtsamaid tulemuslikkuse näitajaid, mis mõõdavad rakendamist;

52. teeb presidendile ülesandeks edastada käesolev resolutsioon nõukogule, komisjonile, liikmesriikide valitsustele ja parlamentidele, Europolile, Eurojustile ning Euroopa Nõukogule.