EUROPOS PARLAMENTAS 2009–2014

Plenarinio posėdžio dokumentas

A7-0335/2012

17.10.2012

PRANEŠIMAS

dėl kibernetinio saugumo ir gynybos
(2012/2096(INI))

Užsienio reikalų komitetas

Pranešėjas: Tunne Kelam

TURINYS

Puslapis

PASIŪLYMAS DĖL EUROPOS PARLAMENTO REZOLIUCIJOS

dėl kibernetinio saugumo ir gynybos

(2012/2096(INI))

Europos Parlamentas,

– atsižvelgdamas į Europos saugumo strategijos įgyvendinimo ataskaitą, kurią 2008 m. gruodžio 11 ir 12 d. patvirtino Europos Vadovų Taryba,

– atsižvelgdamas į Europos Tarybos konvenciją dėl elektroninių nusikaltimų (2004 m. lapkričio 23 d., Budapeštas),

– atsižvelgdamas į 2011 m. gegužės 27 d. Tarybos išvadas dėl ypatingos svarbos informacinės infrastruktūros apsaugos ir ankstesnes Tarybos išvadas dėl kibernetinio saugumo,

– atsižvelgdamas į 2010 m. gegužės 19 d. Komisijos Europos skaitmeninę darbotvarkę (COM(2010) 0245),

– atsižvelgdamas į 2008 m. gruodžio 8 d. Tarybos direktyvą 2008/114/EB dėl Europos ypatingos svarbos infrastruktūros objektų nustatymo ir priskyrimo jiems bei būtinybės gerinti jų apsaugą vertinimo[1],

– atsižvelgdamas į neseniai paskelbtą Komisijos komunikatą dėl Europos kovos su elektroniniu nusikalstamumu centro kūrimo laikantis vidaus saugumo strategijoje nurodyto prioriteto (COM(2012) 0140),

– atsižvelgdamas į savo 2010 m. kovo 10 d. rezoliuciją dėl Europos saugumo strategijos ir Bendros saugumo ir gynybos politikos įgyvendinimo[2],

– atsižvelgdamas į savo 2011 m. gegužės 11 d. rezoliuciją dėl bendros saugumo ir gynybos politikos plėtojimo įsigaliojus Lisabonos sutarčiai[3],

– atsižvelgdamas į savo 2012 m. gegužės 25 d. rezoliuciją dėl Europos Sąjungos vidaus saugumo strategijos[4],

– atsižvelgdamas į savo 2011 m. rugsėjo 27 d. rezoliuciją dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, iš dalies keičiančio Reglamentą (EB) Nr. 1334/2000, nustatantį Bendrijos dvejopo naudojimo objektų ir technologijų eksporto kontrolės režimą[5],

– atsižvelgdamas į savo 2012 m. birželio 12 d. rezoliuciją dėl ypatingos svarbos

[1] OL L 345, 2008 12 23, p. 75.
[2] Priimti tekstai, P7_TA(2010) 0061.
[3] Priimti tekstai, P7_TA(2011) 0228.
[4] Priimti tekstai, P7_TA(2012) 0207.
[5] Priimti tekstai, P7_TA(2011) 0406.

informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“[1],

– atsižvelgdamas į 2012 m. liepos 5 d. Jungtinių Tautų Žmogaus teisių tarybos rezoliuciją „Žmogaus teisių internete skatinimas, apsauga ir naudojimasis jomis“[2], kurioje pripažįstama žmogaus teisių apsaugos ir laisvo informacijos srauto internete svarba,

– atsižvelgdamas į 2012 m. gegužės 20 d. vykusio Čikagos aukščiausiojo lygio susitikimo išvadas,

– atsižvelgdamas į ES sutarties V antraštinę dalį,

– atsižvelgdamas į Darbo tvarkos taisyklių 48 straipsnį,

– atsižvelgdamas į Užsienio reikalų komiteto pranešimą (A7-0335/2012),

A. kadangi šiuolaikiniame globalizuotame pasaulyje ES ir jos valstybės narės tapo labai priklausomomis nuo saugios kibernetinės erdvės, saugaus naudojimosi informacinėmis bei skaitmeninėmis technologijomis ir lanksčių ir patikimų informacinių paslaugų bei susijusios infrastruktūros;

B. kadangi informacinės ir ryšių technologijos taip pat naudojamos kaip represijos priemonės; kadangi sąlygos, kuriomis naudojamos technologijos, didele dalimi lemia poveikį, kurį šios technologijos gali turėti kaip jėga, kuria siekiama teigiamų pokyčių arba represijų;

C. kadangi labai sparčiai daugėja kibernetinės erdvės problemų, pavojų ir išpuolių joje, todėl kyla didelė grėsmė valstybių ir privačiojo sektoriaus saugumui, gynybai, stabilumui ir konkurencingumui; kadangi dėl šios priežasties tokie pavojai neturėtų būti laikomi ateities problemomis; kadangi dauguma labai akivaizdžių ir trikdančių kibernetinės erdvės incidentų dabar yra pagrįsti politiniais motyvais; kadangi didžioji dauguma kibernetinių incidentų yra primityvūs, o grėsmė ypatingos svarbos objektams tampa vis sudėtingesnė, todėl reikia nuodugnios apsaugos sistemos;

D. kadangi visame pasaulyje beveik du milijardus naudotojų siejanti kibernetinė erdvė tapo viena galingiausių ir veiksmingiausių priemonių skleisti demokratines idėjas ir suburti žmones, siekiančius įgyvendinti laisvės troškimus ir kovoti su diktatoriškais režimais; kadangi naudojant kibernetinę erdvę nedemokratinių ir autoritarinių režimų valdomose šalyse kyla vis didesnis pavojus asmens teisėms į saviraiškos ir asociacijų laisvę; kadangi dėl to labai svarbu užtikrinti, kad kibernetinė erdvė išliktų atvira laisvam idėjų, informacijos ir saviraiškos srautui;

E. kadangi ES ir jos valstybėse narėse susiduriama su daugybe politinių, teisėkūros ir organizacinių kliūčių, siekiant sukurti visapusišką ir vieningą kibernetinės gynybos ir kibernetinio saugumo metodą; kadangi jautrioje ir pažeidžiamoje kibernetinio saugumo srityje trūksta bendrų apibrėžčių, standartų ir priemonių;

[1] Priimti tekstai, P7_TA(2012) 0237.
[2] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

F. kadangi dalijimasis ir koordinavimas ES institucijose, su valstybėmis narėmis ir tarp jų, taip pat su išorės partneriais, vis dar nepakankamas;

G. kadangi ES ir tarptautiniu lygmenimis nesusitarta dėl aiškių suderintų kibernetinio saugumo ir kibernetinės gynybos sąvokų apibrėžčių; kadangi įvairiose šalyse kibernetinis saugumas ir kiti svarbūs terminai suprantami labai skirtingai;

H. kadangi ES dar neparengė darnios ypatingos svarbos informacinės infrastruktūros apsaugos politikos, kuriai reikia taikyti daugiadisciplinį metodą, tuo pat metu stiprinant saugumą ir gerbiant pagrindines teises;

I. kadangi ES pasiūlė įvairių kovos su civilinio lygmens elektroniniais nusikaltimais iniciatyvų, įskaitant naująjį Europos kovos su elektroniniu nusikalstamumu centrą, tačiau jai trūksta konkretaus plano, kurį būtų galima taikyti saugumo ir gynybos lygmeniu;

J. kadangi kovojant su elektroniniais nusikaltimais labai svarbu didinti privačiojo sektoriaus, teisėsaugos institucijų, gynybos ir kitų kompetentingų institucijų tarpusavio pasitikėjimą ir patikimumą;

K. kadangi valstybinių ir nevalstybinių subjektų tarpusavio pasitikėjimas yra patikimo kibernetinio saugumo sąlyga;

L. kadangi dėl informacijos konfidencialumo ir galimos žalos susijusių įmonių įvaizdžiui apie daugumą viešojo ir privačiojo sektoriaus kibernetinių incidentų nepranešama;

M. kadangi daugelis kibernetinių incidentų įvyksta dėl privačiojo ir viešojo sektoriaus tinklo infrastruktūros atsparumo ir stiprumo trūkumo, menkai apsaugotų duomenų bazių ir kitų ypatingos svarbos informacinės infrastruktūros trūkumų; kadangi tik kelios valstybės narės savo tinklų ir informacinių sistemų bei susijusių duomenų apsaugą laiko atitinkamos pareigos vykdyti priežiūrą dalimi, o tuo paaiškinama, kodėl trūksta investicijų į modernias saugumo technologijas, mokymus ir atitinkamų gairių rengimą; kadangi daug valstybių yra priklausomos nuo trečiųjų šalių saugumo technologijų ir turėtų labiau stengtis šią priklausomybę sumažinti;

N. kadangi dauguma aukšto lygio kibernetinių išpuolių, keliančių grėsmę nacionaliniam ar tarptautiniam saugumui bei gynybai, vykdytojų niekada nebūna nustatomi ir patraukiami baudžiamojon atsakomybėn; kadangi tarptautiniu mastu nėra nei susitarta dėl atsako į valstybės remiamus kibernetinius išpuolius prieš kitą valstybę, nei nuspręsta, ar tokie veiksmai galėtų būti traktuojami kaip *casus belli*;

O. kadangi teikdama kibernetinio saugumo strategijos rengimo, įgyvendinimo ir išlaikymo rekomendacijas Europos tinklų ir informacijos apsaugos agentūra (ENISA) padeda valstybėms narėms remti dalijimąsi gerąja patirtimi kibernetinio saugumo srityje ir atlieka pagalbinį vaidmenį įgyvendinant nacionalines kibernetinio saugumo strategijas, nacionalinius nenumatytų atvejų planus, organizuojant Europos ir tarptautinius ypatingos svarbos informacinės infrastruktūros apsaugos (YSIIA) pratybas ir rengiant nacionalinių pratybų scenarijus;

P. kadangi iki 2012 m. birželio mėn. tik dešimt ES valstybių narių oficialiai priėmė

nacionalinę kibernetinio saugumo strategiją;

Q. kadangi kibernetinė gynyba yra vienas svarbiausių Europos gynybos agentūros (EGA) prioritetų; įgyvendindama Pajėgumų plėtojimo planą ji įsteigė kibernetinio saugumo projektų grupę, kurioje dauguma valstybių narių kartu kaupia patirtį ir teikia rekomendacijas;

R. kadangi siekiant didinti ir išlaikyti aukštą kibernetinio saugumo ir gynybos lygį labai svarbu investuoti į kibernetinio saugumo ir gynybos mokslinius tyrimus ir technologinę plėtrą; kadangi moksliniams tyrimams ir technologinei plėtrai skirtos gynybos išlaidos ne padidintos iki sutartų 2 proc. visų gynybos išlaidų, bet sumažintos;

S. kadangi informuotumo didinimas ir piliečių švietimas kibernetinio saugumo klausimais turėtų būti kiekvienos išsamios kibernetinio saugumo strategijos pagrindas;

T. kadangi reikia nustatyti aiškią saugumo priemonių ir piliečių teisių pagal SESV, pvz., teisės į privatų gyvenimą, duomenų apsaugą ir saviraiškos laisvę, pusiausvyrą; nė vienas iš šių elementų neturėtų būti aukojamas dėl kito;

U. kadangi didėja poreikis labiau gerbti ir ginti asmens teisę į privatų gyvenimą, kaip nustatyta ES pagrindinių teisių chartijoje ir SESV 16 straipsnyje; kadangi institucijų ir gynybos įstaigų poreikis apsaugoti ir ginti kibernetinę erdvę nacionaliniu lygmeniu, nors ir svarbus, niekada jokiu būdu neturėtų būti naudojamas kaip pretekstas kibernetinėje ir informacinėje erdvėje apriboti teises ir laisves;

V. kadangi dėl pasaulinio ir sienų nepaisančio interneto pobūdžio reikia naujų tarptautinio valdymo ir bendradarbiavimo su įvairiomis suinteresuotosiomis šalimis formų;

W. kadangi vyriausybės, siekdamos užtikrinti savo ypatingos svarbos infrastruktūros saugumą, vis labiau pasitiki privačiojo sektoriaus subjektais;

X. kadangi Europos išorės veiksmų tarnyba (EIVT) kibernetinio saugumo aspekto dar nėra aktyviai įtraukusi į santykius su trečiosiomis šalimis;

Y. kadangi stabilumo priemonė kol kas yra vienintelė ES programa, skirta reaguoti į neatidėliotinas krizes arba pasaulines ir (arba) tarpregionines saugumo problemas, įskaitant kibernetinio saugumo pavojus;

Z. kadangi bendras ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupės atsakas į kibernetinio saugumo pavojus yra vienas iš ES ir JAV santykių prioritetų;

Veiksmai ir koordinavimas Europos Sąjungoje

1. pažymi, kad ES ir pasaulyje sparčiai didėja ir vis dažniau pasitaiko kibernetinių pavojų grėsmė ir daugėja išpuolių prieš vyriausybines, administracines, karines bei tarptautines įstaigas ir kad yra akivaizdus pagrindas susirūpinti, jog valstybiniai ir nevalstybiniai subjektai, visų pirma teroristinės ir nusikalstamos grupuotės, gali atakuoti ES institucijų ir valstybių narių ypatingos svarbos informacines ir ryšių struktūras bei infrastruktūrą ir taip

gali padaryti didelės žalos, įskaitant kinetinį poveikį;

2. todėl pabrėžia, kad šias problemas reikia spręsti ES lygmeniu taikant visuotinį koordinuotą požiūrį, parengiant išsamią ES kibernetinio saugumo strategiją, kurioje reikėtų pateikti bendrą kibernetinio saugumo ir gynybos apibrėžtį, taip pat apibrėžtį, kas sudaro su gynyba susijusį kibernetinį išpuolį, bendrą veiklos viziją ir reikėtų atsižvelgti į papildomą esamų agentūrų ir įstaigų naudą, taip pat į gerąją praktiką tose valstybėse narėse, kurios jau turi nacionalines kibernetinio saugumo strategijas; pabrėžia, kad siekiant padėti derinti įvairias karines ir civilines iniciatyvas, programas ir veiklą labai svarbu Sąjungos lygmeniu koordinuoti veiklą ir kurti sąveiką; pabrėžia, kad tokia strategija reikėtų užtikrinti lankstumą ir kad ją reikėtų reguliariai atnaujinti pritaikant prie greitai kintančios kibernetinės erdvės;

3. primygtinai ragina Komisiją ir Sąjungos vyriausiąją įgaliotinę užsienio reikalams ir saugumo politikai savo būsimame pasiūlyme dėl solidarumo sąlygos įgyvendinimo tvarkos (SESV 222 straipsnis) apsvarstyti rimto kibernetinio išpuolio prieš kurią nors valstybę narę galimybę; be to, laikosi nuomonės, kad nors kibernetiniai išpuoliai, keliantys grėsmę nacionaliniam saugumui, vis dar turi būti apibrėžti taikant bendrą terminologiją, jiems galėtų būti taikoma abipusės gynybos sąlyga (ES sutarties 42 straipsnio 7 dalis) nepažeidžiant proporcingumo principo;

4. pabrėžia, jog BSGP privaloma užtikrinti, kad vykdant ES karines operacijas ir civilines misijas pajėgos būtų apsaugotos nuo kibernetinių išpuolių; pabrėžia, kad kibernetinė gynyba turėtų tapti aktyviu BSGP pajėgumu;

5. pabrėžia, kad visas ES kibernetinio saugumo politikos kryptis reikėtų grįsti ir kurti taip, kad būtų užtikrinta didžiausia įmanoma skaitmeninių laisvių apsauga bei išsaugojimas ir pagarba žmogaus teisėms internete; mano, kad siekiant stiprinti šias pastangas internetas ir IRT turėtų būti integruotos į ES užsienio ir saugumo politikos kryptis;

6. ragina Komisiją ir Tarybą vienareikšmiškai pripažinti skaitmenines laisves pagrindinėmis teisėmis ir privalomomis sąlygomis siekiant naudotis visuotinėmis žmogaus teisėmis; pabrėžia, kad valstybės narės, kurdamos savo atsakus į kibernetines grėsmes ir išpuolius, turėtų siekti niekada nesukelti grėsmės piliečių teisėms ir laisvėms, o jų teisės aktuose turėtų būti nustatyti atitinkami civilinio ir karinio lygmens kibernetinių incidentų skirtumai; ragina apdairiai taikyti apribojimus piliečių gebėjimui pasinaudoti ryšių ir informacinių technologijų priemonėmis;

7. ragina Tarybą ir Komisiją kartu su valstybėmis narėmis parengti baltąją knygą dėl kibernetinės gynybos, kurioje būtų pateiktos aiškios apibrėžtys ir kriterijai, pagal kuriuos, remiantis motyvais ir padariniais, atskiriami kibernetinių išpuolių civilinėje ir karinėje erdvėje lygiai, taip pat reagavimo lygiai, įskaitant tyrimą, nusikaltėlių nustatymą ir baudžiamąjį persekiojimą;

8. mano, kad reikia atnaujinti Europos saugumo strategiją, siekiant nustatyti ir rasti persekiojimo ir baudžiamojo persekiojimo priemonių, taikomų pavieniams, su tinklu susijusiems ir valstybės remiamiems kibernetiniams užpuolėjams;

ES lygmuo

9. pabrėžia horizontalaus ES institucijų ir agentūrų vidaus ir tarpusavio bendradarbiavimo ir kibernetinio saugumo veiklos koordinavimo svarbą;

10. pabrėžia, kad taikant naujas technologijas metamas iššūkis metodams, pagal kuriuos vyriausybės įgyvendina įprastus svarbiausius uždavinius; dar kartą patvirtina, kad už gynybos ir saugumo politikos kryptis, įskaitant atitinkamą demokratinę priežiūrą, galiausiai atsakinga vyriausybė; atkreipia dėmesį į vis svarbesnį privačiojo sektoriaus veikėjų vaidmenį įgyvendinant saugumo ir gynybos uždavinius, kuriuos atliekant dažnai trūksta skaidrumo ir atskaitomybės arba demokratinės priežiūros priemonių;

11. pabrėžia, kad vyriausybės, taikydamos naujas technologijas saugumo ir gynybos politikos srityje, turi tvirtai laikytis pagrindinių tarptautinės viešosios ir humanitarinės teisės principų, pvz., pagarbos valstybės suverenitetui ir žmogaus teisėms; atkreipia dėmesį į vertingą ES valstybių narių, pvz., Estijos, patirtį apibrėžiant ir kuriant kibernetinio saugumo politiką ir kibernetinę gynybą;

12. pripažįsta, kad reikia įvertinti bendrą kibernetinių išpuolių prieš ES informacines sistemas ir infrastruktūrą grėsmės lygį; atsižvelgdamas į tai pabrėžia, kad reikia nuolat vertinti, kaip ES institucijos pasirengusios atremti galimus kibernetinius išpuolius; ypač pabrėžia, kad būtina stiprinti ypatingos svarbos informacinę infrastruktūrą;

13. taip pat pabrėžia, kad būtina teikti informaciją apie pažeidžiamumą, pranešimus ir įspėjimus, susijusius su informacinėms sistemoms kylančiomis naujomis grėsmėmis;

14. pažymi, kad neseniai įvykdžius kibernetinius išpuolius prieš Europos informacinius tinklus ir vyriausybių informacines sistemas padaryta didelė žala ekonomikai ir saugumui, kurios mastas tinkamai neįvertintas;

15. ragina visas ES institucijas kuo skubiau parengti kibernetinio saugumo strategijas ir su savo sistemomis susijusius nenumatytų atvejų planus;

16. ragina visas ES institucijas į savo rizikos analizę ir krizių valdymo planus įtraukti kibernetinių krizių valdymo klausimą; be to, ragina visas ES institucijas visiems savo darbuotojams rengti informuotumo didinimo mokymus kibernetinio saugumo klausimais; siūlo kartą per metus panašiai kaip avarines pratybas rengti kibernetines pratybas;

17. pabrėžia, kad svarbu veiksmingai plėtoti ES kompiuterinių incidentų tyrimo tarnybą (ES CERT) ir nacionalines CERT, taip pat parengti nacionalinius nenumatytų atvejų planus, kuriais būtų galima naudotis, jei prireiktų imtis veiksmų; palankiai vertina tai, kad iki 2012 m. gegužės mėn. visos ES valstybės narės įsteigė nacionalines CERT; primygtinai ragina toliau plėtoti nacionalines ir ES CERT, kurias prireikus būtų galima panaudoti per 24 valandas; pabrėžia, kad reikia įvertinti šios srities viešojo ir privačiojo sektorių partnerysčių galimybes;

18. pripažįsta, kad „Cyber Europe 2010” – pirmosios europinės ypatingos svarbos informacinės infrastruktūros apsaugos pratybos, kuriose dalyvavo įvairios valstybės narės ir kurioms vadovavo ENISA, buvo naudingos ir tapo gerosios patirties pavyzdžiu; taip pat pabrėžia, kad būtina kuo greičiau sukurti Europos lygmens Ypatingos svarbos infrastruktūros objektų įspėjamąjį informacinį tinklą;

19. pabrėžia, kad svarbu imtis Europos masto veiksmų dėl pasirengimo didelių tinklo saugumo incidentų atveju ir apibrėžti bendrą pavojaus vertinimo standartų rinkinį;

20. ragina Komisiją ištirti būtinybę ir galimybes įsteigti ES kibernetinio koordinavimo pareigybę;

21. mano, kad atsižvelgiant į aukštą gebėjimų lygį, kurio reikia tiek atitinkamai kibernetinių sistemų ir infrastruktūros gynybai, tiek vykdyti išpuolius prieš jas, turėtų būti apsvarstyta galimybė Komisijai, Tarybai ir valstybėms narėms sukurti kompiuterių saugumo užtikrinimo strategiją; pažymi, kad tokiais atvejais galimas didelis protų nutekėjimas ir kad ypač už tokius išpuolius nuteisti nepilnamečiai turi daug galimybių reabilituotis ir būti integruoti į gynybos agentūras ir įstaigas;

Europos gynybos agentūra (EGA)

22. palankiai vertina naujausias iniciatyvas ir projektus, susijusius su kibernetine gynyba, visų pirma su svarbių kibernetinio saugumo ir gynybos duomenų rinkimu ir problemų bei poreikių nustatymu, ir primygtinai ragina valstybes nares kibernetinės gynybos srityje daugiau bendradarbiauti su EGA, taip pat ir kariniu lygmeniu;

23. pabrėžia, kad valstybėms narėms plėtojant nacionalinius kibernetinės gynybos pajėgumus svarbu glaudžiai bendradarbiauti su EGA; mano, kad, siekiant užtikrinti veiksmingą kibernetinę gynybą Europos ir nacionaliniu lygmenimis, svarbu Europos lygmeniu kurti sąveiką, kaupti informaciją ir ja dalytis;

24. ragina EGA stiprinti bendradarbiavimą su NATO, nacionaliniais ir tarptautiniais kompetencijos centrais, Europos kovos su elektroniniu nusikalstamumu centru Europole, prisidedančiu prie greitesnio reagavimo į kibernetinius išpuolius, ir ypač su Bendros kibernetinės gynybos mokymo centru (CCDCOE) ir sutelkti dėmesį į gebėjimų stiprinimą, mokymą, keitimąsi informacija ir dalijimąsi patirtimi;

25. susirūpinęs pažymi, kad iki 2010 m. tik vienos valstybės narės gynybos moksliniams tyrimams ir technologinei plėtrai skirtų išlaidų lygis siekė 2 proc. ir kad 2010 m. penkios valstybės narės mokslinių tyrimų ir technologinės plėtros išlaidų nepatyrė; primygtinai ragina EGA kartu su valstybėmis narėmis sutelkti išteklius ir veiksmingai investuoti į bendruosius mokslinius tyrimus ir technologinę plėtrą, ypatingą dėmesį skiriant kibernetiniam saugumui ir gynybai;

Valstybės narės

26. ragina visas valstybes nares plėtoti ir nedelsiant baigti rengti atitinkamą nacionalinę kibernetinio saugumo ir gynybos strategiją ir užtikrinti patikimą politikos formavimo bei reguliavimo aplinką, išsamias rizikos valdymo procedūras ir atitinkamas parengiamąsias priemones bei mechanizmus; ragina ENISA padėti valstybėms narėms; reiškia paramą ENISA, rengiančiai gerosios patirties vadovą, kuriame bus nurodyta geroji patirtis ir pateiktos rekomendacijos, kaip rengti, įgyvendinti ir išsaugoti kibernetinio saugumo strategiją;

27. ragina visas valstybes nares savo karinėje struktūroje sukurti specialius kibernetinio

saugumo ir kibernetinės gynybos padalinius, kad būtų galima bendradarbiauti su panašiomis kitų ES valstybių narių įstaigomis;

28. ragina valstybes nares regionų mastu diegti specializuotus teismus, kurie turėtų užtikrinti, jog už išpuolius prieš informacines sistemas būtų veiksmingiau baudžiama; pabrėžia, kad būtina skatinti derinti nacionalinę teisę siekiant užtikrinti, kad ji būtų pritaikyta prie technikos ir praktikos raidos;

29. ragina Komisiją toliau formuoti darnų ir veiksmingą europinį požiūrį siekiant išvengti nereikalingų iniciatyvų, skatinti ir remti valstybių narių pastangas kurti bendradarbiavimo mechanizmus ir gerinti keitimąsi informacija; mano, kad reikia nustatyti būtiniausią privalomo valstybių narių bendradarbiavimo ir dalijimosi ištekliais lygį;

30. primygtinai ragina valstybes nares parengti nacionalinius nenumatytų atvejų planus ir į krizių valdymo planus bei rizikos analizę įtraukti kibernetinių krizių valdymą; taip pat pabrėžia, kad svarbu tinkamai mokyti visus viešųjų įstaigų darbuotojus esminiais kibernetinio saugumo klausimais, ypač organizuoti tinkamą teisminių ir saugumo institucijų darbuotojų mokymą mokymo įstaigose; ragina ENISA ir kitas susijusias įstaigas padėti valstybėms narėms užtikrinti išteklių kaupimą ir dalijimąsi jais, taip pat išvengti dubliavimo;

31. primygtinai ragina valstybes nares numatyti, kad moksliniai tyrimai ir technologinė plėtra būtų vienas pagrindinių kibernetinio saugumo ir gynybos ramsčių, ir skatinti informacinių sistemų apsaugos specialistų inžinierių mokymą; ragina valstybes nares įvykdyti įsipareigojimą padidinti moksliniams tyrimams ir technologinei plėtrai skirtas gynybos išlaidas bent iki 2 proc., ypatingą dėmesį skiriant kibernetiniam saugumui ir gynybai;

32. ragina Komisiją ir valstybes nares parengti programas, kuriomis privatūs ir verslo vartotojai būtų skatinami apskritai saugiai naudoti internetą, informacines sistemas ir ryšių technologijas ir būtų didinamas jų informuotumas šiais klausimais; siūlo Komisijai pradėti su tuo susijusią viešąją visos Europos masto švietimo iniciatyvą ir ragina valstybes nares įtraukti mokymą apie kibernetinį saugumą į kuo jaunesniems mokiniams skirtas mokymo programas;

Viešojo ir privačiojo sektorių bendradarbiavimas

33. pabrėžia, kad valdžios institucijoms ir privačiajam sektoriui labai svarbu prasmingai ir vieniems kitus papildant bendradarbiauti kibernetinio saugumo klausimais ES ir nacionaliniu lygmenimis, siekiant sukurti tarpusavio pasitikėjimą; žino, kad toliau didinant susijusių viešųjų institucijų patikimumą ir veiksmingumą bus padedama didinti pasitikėjimą ir dalytis ypatingos svarbos informacija;

34. ragina privačiojo sektoriaus partnerius kuriant naujus produktus, prietaisus, paslaugas ir taikomąsias programas apsvarstyti saugumo nuo ankstyvo etapo sprendimus ir numatyti paskatas tiems, kurie kuria naujus produktus, prietaisus, paslaugas ir taikomąsias programas kaip esminę savybę numatydami saugumo sprendimus; ragina bendradarbiaujant su privačiuoju sektoriumi, kai siekiama užkirsti kelią kibernetiniams išpuoliams ir persekioti su jais susijusius asmenis, taikyti būtiniausius skaidrumo standartus ir ataskaitų teikimo mechanizmus;

35. pabrėžia, kad ypatingos svarbos informacinės infrastruktūros apsauga yra įtraukta į ES vidaus saugumo strategiją siekiant užtikrinti aukštesnį piliečių ir įmonių saugumo lygį kibernetinėje erdvėje;

36. ragina su šiais partneriais palaikyti nuolatinį dialogą geriausio informacinių sistemų naudojimo ir atsparumo klausimais, taip pat atsakomybės dalijimosi klausimu, kad būtų galima užtikrinti saugų ir tinkamą šių sistemų veikimą;

37. mano, kad valstybės narės, ES institucijos ir privatusis sektorius, bendradarbiaudami su ENISA, turėtų imtis priemonių didinti informacinių sistemų saugumą ir neliečiamumą, užkirsti kelią išpuoliams ir kuo labiau sumažinti jų poveikį; remia Komisijos pastangas pasiūlyti įmonėms skirtus būtiniausius kibernetinio saugumo standartus ir sertifikavimo sistemas, taip pat teikti tinkamas paskatas, kuriomis siekiama skatinti privačiojo sektoriaus pastangas stiprinti saugumą;

38. ragina Komisiją ir valstybių narių vyriausybes skatinti privačiojo sektoriaus ir pilietinės visuomenės veikėjus įtraukti kibernetinių krizių valdymą į savo krizių valdymo planus ir rizikos analizę; be to, ragina pradėti rengti visiems savo darbuotojams informuotumo didinimo mokymo kursus esminiais kibernetinio saugumo ir elektroninių nusikaltimų prevencijos klausimais;

39. ragina Komisiją, bendradarbiaujant su valstybėmis narėmis ir atitinkamomis agentūromis bei įstaigomis, parengti skubaus keitimosi informacija sistemos programas ir priemones, kuriomis būtų užtikrinamas apie kibernetinius incidentus pranešančių privačiojo sektoriaus subjektų anonimiškumas, sudaromos sąlygos nuolat teikti viešiesiems subjektams naujausią informaciją ir prireikus teikti pagalbą;

40. pabrėžia, kad ES turi sudaryti palankesnes sąlygas Europos Sąjungoje plėtoti konkurencingą ir novatorišką kibernetinio saugumo rinką, kad šioje srityje galėtų geriau veikti MVĮ ir kartu būtų galima prisidėti prie ekonomikos augimo stiprinimo ir darbo vietų kūrimo;

Tarptautinis bendradarbiavimas

41. ragina EIVT imtis iniciatyvos kibernetinio saugumo klausimais ir įtraukti kibernetinio saugumo aspektą į visus savo veiksmus, visų pirma santykius su trečiosiomis šalimis; ragina paspartinti bendradarbiavimą su trečiosiomis šalimis ir keitimąsi informacija apie tai, kaip spręsti kibernetinio saugumo klausimus;

42. pabrėžia, kad tik baigus rengti išsamią ES kibernetinio saugumo strategiją bus galima nustatyti tokį veiksmingą tarptautinį bendradarbiavimą kibernetinio saugumo klausimais, kokio reikia atsižvelgiant į tarpvalstybinį kibernetinių pavojų pobūdį;

43. ragina valstybes nares, kurios dar nepasirašė arba neratifikavo Europos Tarybos konvencijos dėl elektroninių nusikaltimų (Budapešto konvencija), nedelsiant tai padaryti; remia Komisijos ir EIVT pastangas propaguoti šią konvenciją ir jos vertybes trečiosiose šalyse;

44. žino, kad atsakas į elektroninės erdvės pavojus turi būti sutartas ir koordinuojamas

tarptautiniu lygmeniu; todėl ragina Komisiją, EIVT ir valstybes nares imtis vadovaujamojo vaidmens visuose forumuose, ypač Jungtinėse Tautose, siekiant platesnio tarptautinio bendradarbiavimo ir galutinio susitarimo dėl bendro elgsenos kibernetinėje erdvėje normų supratimo, taip pat skatinti bendradarbiauti siekiant kurti kibernetinių ginklų kontrolės susitarimus;

45. ragina keistis žiniomis su BRICS šalimis ir kitomis besiformuojančios rinkos ekonomikos šalimis kibernetinio saugumo srityje, siekiant išnagrinėti bendro atsako į didėjantį elektroninį nusikalstamumą ir elektroninės erdvės pavojus ir kibernetinius išpuolius galimybes civiliniu ir kariniu lygmenimis;

46. primygtinai ragina EIVT ir Komisiją atitinkamuose tarptautiniuose forumuose ir organizacijose, visų pirma JT, ESBO, EBPO ir Pasaulio banke, imtis iniciatyvos, kad būtų taikomi galiojantys tarptautinės teisės aktai ir susitarta dėl atsakingo valstybių elgesio kibernetinio saugumo ir gynybos srityje normų, ir koordinuoti valstybių narių pozicijas siekiant propaguoti pagrindines ES vertybes ir politiką kibernetinio saugumo ir gynybos srityje;

47. ragina Tarybą ir Komisiją palaikant dialogą bei santykius ir sudarant bendradarbiavimo susitarimus su trečiosiomis šalimis, ypač tomis šalimis, kurios yra numačiusios bendradarbiauti technologijų srityje arba keistis šiomis technologijomis, primygtinai reikalauti laikytis būtiniausių kibernetinio nusikalstamumo ir kibernetinių išpuolių prevencijos ir kovos su jais reikalavimų, taip pat būtiniausių informacinių sistemų saugumo standartų;

48. ragina Komisiją prireikus sudaryti trečiosioms šalims palankesnes sąlygas ir padėti joms stengiantis padidinti savo kibernetinio saugumo ir kibernetinės gynybos pajėgumus;

Bendradarbiavimas su NATO

49. pakartoja, kad ES ir NATO, remdamosi bendromis vertybėmis ir strateginiais interesais, yra atsakingos ir gali spręsti didėjančias kibernetinio saugumo problemas veiksmingiau ir glaudžiai bendradarbiaudamos, ieškodamos galimybių viena kitą papildyti, nedubliuodamos veiksmų ir laikydamosi atitinkamų įsipareigojimų;

50. pabrėžia, kad, atsižvelgiant į ES ir NATO papildomumą sprendžiant kibernetinio saugumo ir gynybos klausimus, reikia kaupti informaciją ir ja dalytis praktiniu lygmeniu; pabrėžia, kad reikia glaudesnio koordinavimo, visų pirma susijusio su kibernetinio saugumo ir gynybos planavimu, technologijomis, mokymu ir įranga;

51. atsižvelgdamas į esamą papildomą gynybos gebėjimų stiprinimo veiklą primygtinai ragina visas susijusias kibernetinio saugumo ir gynybos srityje veikiančias ES įstaigas stiprinti praktinį bendradarbiavimą su NATO, siekiant dalytis patirtimi ir išmokti didinti ES sistemų atsparumą;

Bendradarbiavimas su Jungtinėmis Amerikos Valstijomis

52. mano, kad siekdamos atremti kibernetinius išpuolius ir kovoti su elektroniniais nusikaltimais ES ir JAV turėtų stiprinti tarpusavio bendradarbiavimą, nes po 2010 m. ES

ir JAV aukščiausiojo lygio susitikimo Lisabonoje šis bendradarbiavimas nustatytas kaip transatlantinių santykių prioritetas;

53. palankiai vertina tai, kad per 2010 m. lapkričio mėn. ES ir JAV aukščiausiojo lygio susitikimą įsteigta ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupė, ir remia jos pastangas įtraukti kibernetinio saugumo klausimus į transatlantinį politinį dialogą;

54. palankiai vertina tai, kad Komisija ir JAV vyriausybė remdamosi ES ir JAV darbo grupės veikla drauge parengė bendrą programą ir veiksmų planą, pagal kurį 2012–2013 m. būtų vykdomos bendros suderintos tarpžemyninės kibernetinės pratybos; atkreipia dėmesį į pirmąsias 2011 m. surengtas pratybas „Cyber Atlantic“;

55. pabrėžia, kad JAV ir ES, kaip didžiausi kibernetinės erdvės ir naudotojų šaltiniai, turi bendradarbiauti siekdamos apsaugoti savo piliečių teises ir laisves naudotis šia erdve; pabrėžia, kad, nors nacionalinis saugumas yra svarbiausias uždavinys, kibernetinė erdvė turėtų būti saugi, bet taip pat apsaugota;

56. paveda Pirmininkui perduoti šią rezoliuciją Tarybai, Komisijai, Sąjungos vyriausiajai įgaliotinei ir Komisijos pirmininko pavaduotojai, EGA, ENISA ir NATO.

GALUTINIO BALSAVIMO KOMITETE REZULTATAI

Priėmimo data	10.10.2012
Galutinio balsavimo rezultatai	+: 47 –: 3 0: 6
Posėdyje per galutinį balsavimą dalyvavę nariai	Bastiaan Belder, Franziska Katharina Brantner, Elmar Brok, Jerzy Buzek, Tarja Cronberg, Arnaud Danjean, Mário David, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Liisa Jaakonsaari, Anneli Jäätteenmäki, Jelko Kacin, Ioannis Kasoulides, Tunne Kelam, Nicole Kiil-Nielsen, Evgeni Kirilov, Maria Eleni Koppa, Wolfgang Kreissl-Dörfler, Eduard Kukan, Vytautas Landsbergis, Krzysztof Lisek, Sabine Lösing, Mario Mauro, Francisco José Millán Mon, Alexander Mirsky, María Muñiz De Urquiza, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Justas Vincas Paleckis, Bernd Posselt, Cristian Dan Preda, Fiorello Provera, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Sophocles Sophocleous, Laurence J.A.J. Stassen, Kristian Vigenin, Sir Graham Watson, Karim Zéribi
Posėdyje per galutinį balsavimą dalyvavęs (-ę) pavaduojantis (-ys) narys (-iai)	Charalampos Angourakis, Elena Băsescu, Jean-Jacob Bicep, Véronique De Keyser, Diogo Feio, Elisabeth Jeggle, Indrek Tarand, Sampo Terho, László Tőkés, Traian Ungureanu, Luis Yáñez-Barnuevo García
Posėdyje per galutinį balsavimą dalyvavęs (-ę) pavaduojantis (-ys) narys (-iai) (187 straipsnio 2 dalis)	Joseph Cuschieri