2012 m. birželio 12 d., antradienis

65. atkreipia dėmesį į būtinybę skatinti savanorišką veiklą, ypač per 2013-uosius Europos piliečių metus, ir ragina Komisiją įtraukti paramą savanoriškai veiklai į tarptautinę paramos vystymuisi politiką, ypač siekiant įvykdyti visus uždavinius, nustatytus pagal Tūkstantmečio vystymosi tikslus;

66. palankiai vertina „Solidaritė“ pasiūlymo dėl tarpinstitucinės žmogiškų išteklių programos ES institucijose oficialų nagrinėjimą siekiant palengvinti institucijų darbuotojų ir stažuotojų dalyvavimą savanoriškoje, humanitarinėje ir socialinėje veikloje ne tik kaip darbuotojų mokymų dalį, bet ir kaip savanorišką veiklą laisvalaikiu;

67. pabrėžia, kad pasiūlyta programa sutaupomos lėšos ir stipriai padidinama pridėtinė vertė ir ji padėtų įgyvendinti ES politiką ir programas;

68. rekomenduoja Komisijai palaikyti naudingus informacinius ryšius, kurie užmegzti ir su grupe „EYV 2011 Alliance“ ir su vėlesne Savanoriškos veiklos programa, apimančiomis daugelį savanoriškos veiklos organizacijų ir pilietinės visuomenės tinklų, ir su nacionalinėmis koordinavimo institucijomis, strateginiais partneriais ir nacionalinių vyriausybių atstovais šioje srityje, atsižvelgiant į didelę tarnybų, atsakingų už savanorišką veiklą, įvairovę ES, ir skatina šiuos informacinius ryšius įsitraukti į siūlomą centralizuotą ES portalą, kuris būtų visos Europos programa, siekiant sudaryti palankesnes sąlygas toliau koordinuoti ir stiprinti tarpvalstybinę veiklą;

69. pabrėžė ryšių tinklų ir keitimosi gerąja praktika svarbą siekiant platinti informaciją apie esamas ES procedūras, kurios gali padėti ir paremti tarptautinę savanorišką veiklą;

70. ragina Komisiją, kur reikia, imtis veiksmų, susijusių su savanoriškos veiklos politikos darbotvarke Europoje, kurią parengė grupei „EYV 2011 Alliance“ priklausančios savanoriškos veiklos organizacijos;

71. paveda Pirmininkui perduoti šią rezoliuciją Tarybai, Komisijai bei valstybių narių vyriausybėms ir parlamentams.

Ypatingos svarbos informacinės infrastruktūros apsauga. Visuotinio kibernetinio saugumo užtikrinimas

P7_TA(2012)0237

2012 m. birželio 12 d. Europos Parlamento rezoliucija dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“ (2011/2284(INI))

(2013/C 332 E/03)

Europos Parlamentas,

— atsižvelgdamas į savo 2010 m. gegužės 5 d. rezoliuciją „Nauja Europos skaitmeninė darbotvarkė „2015.eu““ ([1]),

— atsižvelgdamas į savo 2010 m. birželio 15 d. rezoliuciją „Tolesni interneto valdymo etapai“ ([2]),

— atsižvelgdamas į savo 2011 m. liepos 6 d. rezoliuciją „Plačiajuostis ryšis Europoje. Investavimas į skaitmeninių technologijų skatinamą augimą“ ([3]),

— atsižvelgdamas į Darbo tvarkos taisyklių 48 straipsnį,

— atsižvelgdamas į Pramonės, mokslinių tyrimų ir energetikos komiteto pranešimą ir į Piliečių laisvių, teisingumo ir vidaus reikalų komiteto nuomonę (A7-0167/2012),

([1]) OL C 81 E, 2011 3 15, p. 45.
([2]) OL C 236 E, 2011 8 12, p. 33.
([3]) Priimti tekstai, P7_TA(2011)0322.

A. kadangi informacinių ir ryšių technologijų (IRT) pajėgumus siekiant ekonomikos ir visuomenės pažangos galima visapusiškai išnaudoti tik tada, jeigu vartotojai tiki ir pasitiki jų saugumu ir atsparumu ir jei veiksmingai užtikrinamas galiojančių teisės aktų, reglamentuojančių duomenų privatumą ir intelektinės nuosavybės teises, vykdymas interneto erdvėje;

B. kadangi interneto ir IRT poveikis įvairiems piliečių gyvenimo aspektams sparčiai didėja, ir tai yra esminis veiksnys, skatinantis mūsų socialinę sąveiką, plečiantis kultūrines ribas ir skatinantis ekonomikos augimą;

C. kadangi IRT ir interneto saugumas yra visa apimanti sąvoka, daranti bendrą poveikį ekonominiam, socialiniam, technologiniam ir kariniam aspektams, jos atžvilgiu būtina aiškiai apibrėžti ir paskirstyti atsakomybės sritis ir nustatyti patikimą tarptautinio bendradarbiavimo sistemą;

D. kadangi ES skaitmeninės darbotvarkės pavyzdine iniciatyva siekiama didinti Europos konkurencingumą ir tokį didinimą pagrįsti IRT stiprinimu, taip pat kurti sąlygas dideliam ir sparčiam augimui bei su technologijomis susijusių darbo vietų kūrimui;

E. kadangi praėjusį dešimtmetį investavęs milijardus eurų privatusis sektorius išlieka svarbiausias investuotojas į informacijos saugumo produktus, paslaugas, taikomąsias programas ir infrastruktūrą ir jų pagrindinis savininkas bei valdytojas; kadangi tokį jo dalyvavimą reikėtų didinti taikant tinkamas politikos priemones, kuriomis skatinamas viešojo, privačiojo arba viešojo ir privačiojo sektorių valdomų infrastruktūrų arba infrastruktūrų, kurios jiems priklauso, atsparumas;

F. kadangi didinant IRT tinklų, paslaugų ir technologijų saugumą ir atsparumą, padidės Europos Sąjungos ekonomikos konkurencingumas, nes bus geriau įvertinama ir valdoma kibernetinė rizika ir visai ES ekonomikai bus užtikrinama patikimesnė informacijos infrastruktūra, kuria bus remiamos inovacijos ir augimas, įmonėms sukuriamos naujos galimybės tapti našesnėmis;

G. kadangi iš turimų teisėsaugos duomenų apie elektroninius nusikaltimus (kurie apima kibernetines atakas ir kitus internetinius nusikaltimus) matyti, kad nusikaltimų įvairiose Europos šalyse daugėja; tačiau kadangi teisėsaugos institucijų ir CERT (kompiuterinių incidentų tyrimo tarnybos) pateikiami statistiniu požiūriu reprezentatyvūs duomenys apie kibernetines atakas vis dar nepakankami ir ateityje juos reikės kaupti geriau, dėl to visos ES teisėsaugos institucijos galės geriau reaguoti ir bus galima imtis labiau informacija pagrįstų teisėkūros priemonių vis didėjančiai kibernetinei grėsmei mažinti;

H. kadangi tinkamo lygio informacijos saugumas būtinas norint užtikrintai plėtoti internetines paslaugas;

I. kadangi pastarojo meto kibernetiniai incidentai, veiklos sutrukdymas ir atakos prieš ES institucijų, pramonės bei valstybių narių informacijos infrastruktūrą rodo, kad būtina sukurti patikimą, naujovišką ir veiksmingą ypatingos svarbos informacinės infrastruktūros apsaugos sistemą, kuri būtų pagrįsta visapusišku tarptautiniu bendradarbiavimu ir būtinaisiais valstybių narių atsparumo standartais;

J. kadangi norint greitai kurti naujus IRT taikymo būdus, kaip antai nuotolinių kompiuterinių išteklių paslaugas, daug dėmesio reikia skirti interneto saugumui, kad būtų galima visiškai naudotis technologijų srities laimėjimų teikiama nauda;

K. kadangi Europos Parlamentas nuolat reikalauja taikyti aukštus duomenų privatumo ir apsaugos, tinklo neutralumo ir intelektinės nuosavybės teisių apsaugos standartus;

Priemonės, skirtos ypatingos svarbos informacinės infrastruktūros apsaugai valstybių narių ir ES lygmenimis stiprinti

1. palankiai vertina tai, kad valstybės narės įgyvendino Europos programą dėl ypatingos svarbos informacinės infrastruktūros apsaugos, taip pat tai, kad buvo sukurtas Ypatingos svarbos infrastruktūros objektų įspėjamasis informacinis tinklas (CIWIN);

2. mano, kad dėl veiksmų ypatingos svarbos informacinės infrastruktūros apsaugos srityje ne tik bus užtikrintas didesnis visapusiškas piliečių saugumas, bet taip pat piliečiai ims geriau suvokti, kas yra saugumas, ir ims labiau pasitikėti vyriausybės priimtomis jų apsaugos priemonėmis;

2012 m. birželio 12 d., antradienis

3. pripažįsta, kad Europos Komisija svarsto galimybę persvarstyti Tarybos direktyvą 2008/114/EB ([1]), ir ragina prieš imantis tolesnių priemonių pateikti įrodymų dėl šios direktyvos veiksmingumo ir jos daromo poveikio; ragina apsvarstyti galimybę išplėsti šios direktyvos taikymo sritį, visų pirma, į ją įtraukiant IRT sektorių ir finansines paslaugas, be to, apsvarstyti tokias sritis kaip sveikata, maisto ir vandens tiekimo sistemos, branduoliniai tyrimai ir pramonė (jei šioms sritims netaikomos konkrečios nuostatos); mano, kad šiems sektoriams taip pat reikėtų naudotis tarpsektorinio metodo, priimto CIWIN (kurį sudaro bendradarbiavimas, įspėjimo sistema ir keitimasis geriausia patirtimi), teikiama nauda;

4. pabrėžia, jog svarbu sukurti ir užtikrinti ilgalaikę Europos mokslinių tyrimų integraciją, siekiant išlaikyti ir sustiprinti Europos kompetenciją ypatingos svarbos informacinės infrastruktūros apsaugos srityje;

5. atsižvelgdamas į tarpusavyje susijusį ir tarpusavyje labai priklausomą, neskelbtiną, strateginį ir pažeidžiamą nacionalinių ir Europos ypatingos svarbos informacinės infrastruktūros pobūdį, ragina nuolat atnaujinti būtinuosius pasirengimo reaguoti ir reagavimo į veiklos sutrikdymą, incidentus, mėginimus sunaikinti ar atakas, pvz., dėl nepakankamai patikimos infrastruktūros arba nepakankamai apsaugotų galinių įrenginių, standartus;

6. pabrėžia informacijos saugumo standartų ir protokolų svarbą ir palankiai vertina tai, kad 2011 m. Europos standartizacijos komitetui (CEN), Europos elektrotechnikos standartizacijos komitetui (Cenelec) ir Europos telekomunikacijų standartų institutui (ETSI) suteikti įgaliojimai sukurti saugumo standartus;

7. tikisi, kad ypatingos svarbos informacinės infrastruktūros savininkai ir valdytojai naudotojams suteiks galimybę ir, prireikus, padės naudoti tinkamas priemones, padėsiančias infrastruktūrą apsaugoti nuo piktavališkų atakų ir (arba) veiklos trikdymo, jei riekės, infrastruktūrą prižiūrint žmonėms ir vykdant automatizuotą priežiūrą;

8. remia viešųjų ir privačiųjų suinteresuotųjų subjektų bendradarbiavimą Sąjungos lygmeniu ir skatina jų pastangas kurti ir įgyvendinti civilinės (viešojo sektoriaus, privačiojo sektoriaus arba viešojo ir privačiojo sektorių), nacionalinės ir Europos Sąjungos ypatingos svarbos informacinės infrastruktūros apsaugos sistemos saugumo ir atsparumo standartus;

9. pabrėžia, kad svarbu imtis visos Europos masto veiksmų pasirengiant didelių tinklo saugumo incidentams ir apibrėžti bendrus pavojaus vertinimo standartus;

10. ragina Europos Komisiją bendradarbiaujant su valstybėmis narėmis įvertinti ypatingos svarbos informacinės infrastruktūros apsaugos sistemos veiksmų plano įgyvendinimą; ragina valstybes nares įsteigti veiksmingų nacionalinių (valstybinių) CERT tinklą, rengti nacionalines kibernetinio saugumo strategijas, organizuoti nuolatines nacionalines ir europines kibernetinių incidentų pratybas, parengti nacionalinius su kibernetiniu saugumu susijusius nenumatytų atvejų planus ir iki 2012 m. pabaigos padėti parengti Europos Sąjungos su kibernetiniu saugumu susijusį nenumatytų atvejų planą;

11. rekomenduoja taikyti operatorių saugumo planus ar lygiavertes priemones visai Europos ypatingos svarbos informacinei infrastruktūrai ir paskirti saugumo ryšių palaikymo pareigūnus;

12. palankiai vertina tai, kad dabar persvarstomas Tarybos pamatinis sprendimas 2005/222/TVR dėl atakų prieš informacines sistemas ([2]); atkreipia dėmesį į būtinybę koordinuoti ES veiksmus kovojant su stambaus masto kibernetinėmis atakomis, atsižvelgiant į Europos tinklų ir informacijos apsaugos agentūrų (ENISA), valstybių narių nacionalinių kompiuterinių incidentų tyrimo tarnybų (CERT) ir būsimų Europos Sąjungos kompiuterinių incidentų tyrimo tarnybų (CERT) įgaliojimus;

13. mano, kad ENISA gali atlikti pagrindinį vaidmenį Europos lygmeniu ypatingos svarbos informacinės infrastruktūros apsaugos srityje perduodama techninę praktinę patirtį valstybėms narėms ir Europos Sąjungos institucijoms bei įstaigoms, taip pat teikdama ataskaitas ir tyrimus, susijusius su informacinių sistemų apsauga Europos ir pasauliniu lygmeniu;

Papildoma ES veikla, kuria siekiama užtikrinti patikimą interneto saugumą

14. ragina ENISA kasmet koordinuoti ir įgyvendinti informuotumui apie ES interneto saugumą didinti skirtų mėnesių programą, kad valstybės narės ir ES piliečiai ypač daug dėmesio skirtų su kibernetiniu saugumu susijusiems klausimams;

([1]) OL L 345, 2008 12 23, p. 75.
([2]) OL L 69, 2005 3 16, p. 67.

15. remia ENISA, kuri vadovaudamasi skaitmeninės darbotvarkės tikslais atlieka savo pareigas, susijusias su tinklo informacijos saugumo užtikrinimu, pirmiausia pateikdama gaires ir patardama valstybėms narėms, kaip užtikrinti jų CERT pagrindinius pajėgumus, ir remdama jų keitimąsi geriausia patirtimi kuriant pasitikėjimo aplinką; ragina agentūrą konsultuoti atitinkamus suinteresuotuosius subjektus dėl panašių privačių tinklų ir infrastruktūrų savininkų ir valdytojų kibernetiniam saugumui užtikrinti reikalingų priemonių ir padėti Komisijai bei valstybėms narėms kurti ir taikyti informacijos saugumo sertifikavimo sistemas, elgesio normas ir siekti nacionalinių ir europinių CERT ir infrastruktūros savininkų bei valdytojų bendradarbiavimo, jei reikia, apibrėžiant technologiniu požiūriu neutralius bendrus būtinuosius reikalavimus;

16. palankiai vertina dabartinį pasiūlymą dėl ENISA įgaliojimų, pirmiausia, jų pratęsimo, ir agentūros uždavinių išplėtimo persvarstymo; mano, kad ENISA turėtų būti suteikta teisė ne tik padėti valstybėms narėms teikiant praktinę patirtį ir analizę, bet ir atlikti daugybę administracinių užduočių ES lygmeniu, ir bendradarbiaujant su kolegomis iš JAV atlikti užduotis, susijusias su tinklo ir informacijos saugumo incidentų prevencija bei nustatymu ir valstybių narių bendradarbiavimo didinimu; atkreipia dėmesį į tai, kad pagal ENISA reglamentą agentūrai galėtų būti suteikti tokie papildomi įgaliojimai, susiję su reagavimu į interneto atakas, kad ji teiktų aiškią pridėtinę vertę esamoms nacionalinėms reagavimo priemonėms;

17. palankiai vertina 2010 m. ir 2011 m. europinių kibernetinio saugumo pratybų, kurios rengiamos visoje Sąjungoje ir kurias prižiūri ENISA, kurios tikslas buvo padėti valstybėms narėms kurti, išlaikyti ir išbandyti europinį nenumatytų atvejų planą, rezultatus; ragina ENISA į savo darbotvarkę ir toliau įtraukti tokias pratybas ir vis labiau tinkamai įtraukti susijusius privačius operatorius siekiant galimai padidinti bendras Europos Sąjungos interneto saugumo galimybes ir laukia tolesnės tarptautinės plėtros su panašiai mąstančiais partneriais;

18. ragina valstybes nares parengti nacionalinius su kibernetiniais incidentais susijusių nenumatytų atvejų planus, į juos įtraukti svarbiausius aspektus, pvz., svarbius informacijos centrus, nuostatas dėl pagalbos, izoliavimo ir sutvarkymo tarpvalstybinės svarbos kibernetinės veiklos sutrikdymo ar atakų atveju; pabrėžia, kad valstybės narės nacionaliniu lygmeniu taip pat turėtų taikyti tinkamus koordinavimo mechanizmus ir struktūras, kurie padėtų užtikrinti geresnį kompetentingų nacionalinių institucijų koordinavimą ir didesnį jų veiksmų nuoseklumą;

19. siūlo Komisijai pasiūlyti privalomas priemones, padėsiančias vykdant ES kibernetinių incidentų nenumatytų atvejų planą ES lygmeniu geriau koordinuoti nacionalinių ir vyriausybių CERT technines ir valdymo funkcijas;

20. ragina Komisiją ir valstybes nares imtis būtinų priemonių siekiant apsaugoti ypatingos svarbos infrastruktūrą nuo kibernetinių atakų ir numatyti priemones visiškai užkirsti kelią prieigai prie ypatingos svarbos infrastruktūros, jeigu tiesioginės kibernetinės atakos kelia didžiulę grėsmę jos tinkamam veikimui;

21. tikisi, kad bus baigtos steigti CERT ES, kurios bus pagrindinis veiksnys siekiant vykdyti tyčinių ir piktavališkų kibernetinių atakų, nukreiptų prieš ES institucijas, prevenciją, jas susekti, į jas reaguoti ir atkurti veiklą po tokių atakų;

22. rekomenduoja Komisijai pasiūlyti privalomas priemones būtiniesiems saugumo ir atsparumo standartams nustatyti ir nacionalinių CERT koordinavimui gerinti;

23. ragina valstybes nares ir ES institucijas užtikrinti, kad būtų įsteigtos gerai veikiančios nacionalinės CERT, galinčios užtikrinti būtiną saugumą ir atsparumą, kurių veikla būtų pagrįsta susitarta geriausia patirtimi; atkreipia dėmesį į tai, kad nacionalinės CERT turėtų priklausyti veiksmingam tinklui, kuriame būtų keičiamasi svarbia informacija, remiantis būtinaisiais konfidencialumo standartais; ragina kiekvienoje valstybėje narėje įsteigti visą parą septynias dienas per savaitę veikiančią ypatingos svarbos informacinės infrastruktūros apsaugos tarnybą ir sukurti bendrą Europos ekstremaliųjų situacijų protokolą, kurį taikytų nacionaliniai informacijos centrai;

24. pabrėžia, kad labai svarbu skatinti valstybių narių pasitikėjimą ir bendradarbiavimą siekiant apsaugoti duomenis ir nacionalinius tinklus bei infrastruktūras; ragina Europos Komisiją pasiūlyti bendrą procedūrą, skirtą bendram kovos su tarpvalstybinėmis IRT grėsmėmis metodui nustatyti ir sukurti, tikintis, kad valstybės narės Europos Komisijai teiks bendrą informaciją apie riziką, grėsmę ir pažeidžiamumą, susijusius su jų ypatingos svarbos informacinės infrastruktūros apsaugos veiksmų planu;

2012 m. birželio 12 d., antradienis

25. palankiai vertina Komisijos iniciatyvą iki 2013 m. sukurti Europos informacijos mainų ir įspėjimo sistemą;

26. palankiai vertina kai kurias Komisijos inicijuotas konsultacijas su suinteresuotaisiais subjektais interneto saugumo ir ypatingos svarbos informacinės infrastruktūros apsaugos klausimais, pavyzdžiui, Europos viešojo ir privačiojo sektorių partnerystę atsparumo klausimais; pripažįsta, kad daug IRT paslaugų pardavėjų jau dabar aktyviai dalyvauja ir yra įsipareigoję siekti šio tikslo, ragina Komisiją dar labiau stengtis skatinti aktyvesnį akademinės bendruomenės ir IRT naudotojų asociacijų dalyvavimą ir remti konstruktyvų įvairių suinteresuotųjų subjektų dialogą kibernetinio saugumo klausimais; remia tolesnį Skaitmeninės darbotvarkės, kaip ypatingos svarbos informacinės infrastruktūros apsaugos valdymo struktūros, vystymą;

27. palankiai vertina iki šiol valstybių narių Europos forumo nuveiktą darbą nustatant sektoriui pritaikytus kriterijus, pagal kuriuos nustatoma ypatingos svarbos Europos infrastruktūra, ypatingą dėmesį skiriant fiksuotajam ir judriajam ryšiui, taip pat svarstant ES interneto atsparumo ir stabilumo principus ir gaires; tikisi, kad valstybės narės toliau sieks bendro sutarimo, ir šiuo atžvilgiu ragina minėtąjį forumą dabartinį metodą, kurį taikant daugiausia dėmesio skiriama materialiajam turtui, papildyti veiksmais, kurie taip pat apimtų loginės infrastruktūros turtą, kuris vis labiau virtualėjant technologijoms ir vis labiau plėtojant nuotolinių kompiuterinių išteklių paslaugas bus vis svarbesnis ypatingos svarbos informacinės infrastruktūros apsaugos veiksmingumui užtikrinti;

28. siūlo Komisijai pradėti viešąją europinę švietiamąją iniciatyvą, skiriant dėmesį privačiojo ir verslo sektorių galutinių vartotojų mokymui ir geresniam jų informavimui apie galimą grėsmę interneto ir fiksuotojo bei mobiliojo ryšio IRT įrenginiams visuose bendrosios paskirties grandinės etapuose, skatinant saugesnį asmenų elgesį internete; atsižvelgdamas į tai primena, kokią riziką kelia pasenusi IT įranga ir programinė įranga;

29. ragina valstybes nares, remiant Komisijai, gerinti mokymus ir švietimo informacijos saugumo klausimais programas, skirtas nacionalinėms teisėsaugos ir teisminėms institucijoms ir susijusioms ES agentūroms;

30. remia ES mokslininkų ekspertų informacijos saugumo mokymo programų rengimą, nes šios programos darytų teigiamą poveikį ES praktinei patirčiai ir pasirengimui nuolat vykstančiai kibernetinės erdvės plėtrai ir jai kylančioms grėsmėms;

31. pasisako už švietimo kibernetinio saugumo srityje (doktorantūros studentų stažuotės, kursai universitetuose, seminarai, mokymai studentams ir kt.) skatinimą ir specializuotą mokomąją veiklą ypatingos svarbos informacinės infrastruktūros apsaugos srityje;

32. ragina Komisiją iki 2012 m. pabaigos pasiūlyti išsamią ES interneto saugumo strategiją, pagrįstą aiškiais terminais; mano, kad įgyvendinant interneto saugumo strategiją turėtų būti siekiama sukurti kibernetinę erdvę, kuri būtų pagrįsta saugia ir atsparia infrastruktūra ir viešais standartais, palanki inovacijoms ir klestėjimui laisvai judant informacijai, taip pat užtikrinant patikimą privatumo ir kitų piliečių laisvių apsaugą; laikosi nuomonės, kad strategijoje reikėtų išsamiai nurodyti principus, tikslus, metodus, priemones ir politikos kryptis (vidaus ir išorės), būtinus nacionalinėms ir ES pastangoms didinti ir būtiniesiems valstybių narių atsparumo standartams nustatyti, siekiant užtikrinti saugias, sklandžias, tvirtas ir atsparias paslaugas, susijusias su ypatingos svarbos infrastruktūra ar bendru interneto naudojimu;

33. pabrėžia, kad rengiama Komisijos interneto saugumo strategija visų pirma turėtų būti pagrįsta veikla ypatingos svarbos informacinės infrastruktūros apsaugos srityje ir ją įgyvendinant turėtų būti siekiama laikytis visa apimančio ir sisteminio požiūrio į kibernetinį saugumą, įtraukiant tiek veiklos priemones, pvz., būtinųjų standartų dėl saugos priemonių nustatymą arba atskirų naudotojų, įmonių ir valstybės institucijų mokymą, tiek atsakomąsias priemones, pvz., baudžiamąsias, civilines ir administracines sankcijas;

34. primygtinai ragina Komisiją pasiūlyti patikimą priemonę, kuri būtų skirta koordinuoti interneto saugumo strategijos įgyvendinimą ir reguliarų jos atnaujinimą; laikosi nuomonės, kad ši priemonė turėtų būti remiama pakankamais administraciniais, ekspertų ir finansiniais ištekliais ir padėti palengvinti ES pozicijos parengimą plėtojant santykius su vidaus ir tarptautiniais suinteresuotaisiais subjektais sprendžiant su interneto saugumu susijusius klausimus;

35. ragina Komisiją pateikti pasiūlymą dėl ES pranešimų apie ypatingos svarbos sektorių, pavyzdžiui, energetikos, transporto, vandens ir maisto tiekimo, taip pat IRT ir finansinių paslaugų sektorių, saugumo pažeidimus sistemos, skirtos užtikrinti, kad atitinkamų valstybių narių valdžios institucijos ir vartotojai būtų informuojami apie kibernetinius incidentus, atakas ar sutrikdymus;

36. ragina Komisiją tobulinti statistiniu požiūriu reprezentatyvių duomenų apie ES, valstybių narių ir pramonės sektoriaus (pirmiausia finansinių paslaugų ir IRT sektoriaus) išlaidas, susijusias su kibernetinėmis atakomis, prieinamumą, didinant numatyto Europos kibernetinių nusikaltimų centro, kuris turėtų būti įsteigtas iki 2013 m., CERT ir kitų Komisijos iniciatyvų, pvz., Europos informacijos mainų ir įspėjimo sistemos, duomenų rinkimo pajėgumus, siekiant užtikrinti, kad nuolat būtų perduodami su kibernetinėmis atakomis ir kitų formų kibernetiniais nusikaltimais, darančiais poveikį Europos pramonei ir valstybėms narėms, susiję duomenys ir jais būtų dalijamasi ir kad būtų stiprinama teisėsauga;

37. ragina nacionalinį privatųjį sektorių ir Europos tinklus ir informacijos apsaugos agentūrą (ENISA) glaudžiai bendradarbiauti ir bendrauti, siekiant susieti nacionalinių ir (arba) vyriausybės kompiuterinių incidentų tyrimo tarnybų (CERT) veiklą su Europos informacijos mainų ir įspėjimo sistemos (EISAS) plėtojimu;

38. pažymi, kad IRT pramonė yra svarbiausia technologijų, skirtų interneto saugumui didinti, plėtros ir naudojimo varomoji jėga; primena, kad įgyvendinant ES politikos kryptis reikia stengtis netrukdyti Europos internetinės ekonomikos augimui ir į jas įtraukti reikiamas paskatas siekiant visapusiškai išnaudoti verslo ir viešojo bei privačiojo sektorių partneryščių galimybes; rekomenduoja ištirti kitas paskatas pramonei kurti daugiau patikimų veiklos saugumo planų, kaip nustatyta Tarybos direktyvoje 2008/114/EB;

39. ragina Komisiją pateikti pasiūlymą dėl teisėkūros procedūra priimamo akto dėl tolesnio kibernetinių atakų ((t. y. tikslingo internetinio sukčiavimo (angl. *spear-phishing*), sukčiavimo internete ir kt. veiklos) priskyrimo nusikaltimams;

Tarptautinis bendradarbiavimas

40. primena, kad tarptautinis bendradarbiavimas yra pagrindinė priemonė siekiant nustatyti veiksmingas kibernetinio saugumo priemones; pripažįsta, kad šiuo metu ES reguliariai aktyviai nedalyvauja su kibernetiniu saugumu susijusiuose tarptautinio bendradarbiavimo procesuose ir dialoguose; ragina Komisiją ir Europos išorės veiksmų tarnybą (EIVT) su visomis to paties tikslo siekiančiomis šalimis pradėti konstruktyvų dialogą siekiant bendro sutarimo ir parengti bendros politikos kryptis interneto ir ypatingos svarbos infrastruktūros atsparumui didinti; laikosi nuomonės, kad ES turėtų interneto saugumo klausimus nuolat įtraukti į išorės santykių sritį, *inter alia*, kurdama įvairias finansines priemones arba įsipareigodama tarptautiniais susitarimais, kuriuose minimas keitimasis neskelbtinais duomenimis ir jų saugojimas;

41. atkreipia dėmesį į 2001 m. Europos Tarybos Budapešto konvencijos dėl kibernetinių nusikaltimų laimėjimus; vis dėlto atkreipia dėmesį į tai, kad skatindama daugiau šalių pasirašyti ir ratifikuoti minėtą konvenciją, EIVT turėtų su panašiai mąstančiais tarptautiniais partneriais sudaryti dvišalius ir daugiašalius susitarimus dėl interneto saugumo ir atsparumo;

42. pažymi, kad įvairių tarptautinių ir ES institucijų, įstaigų ir agentūrų, taip pat ES valstybių narių vykdoma veikla turi būti koordinuojama, kad būtų išvengta dubliavimo; šiuo tikslu svarstytina galimybė paskirti pareigūną, atsakingą už veiksmų koordinavimą, galbūt paskiriant ES kibernetinio saugumo koordinatorių;

43. pabrėžia, kad ES ir JAV už ypatingos svarbos informacinės infrastruktūros apsaugą atsakingų pagrindinių subjektų ir teisės aktų leidėjų struktūrinis dialogas yra labai svarbus siekiant bendro supratimo, vienodo aiškinimo ir bendros pozicijos teisinių ir valdymo sistemų klausimais;

44. palankiai vertina tai, kad 2010 m. lapkričio mėn. ES ir JAV aukščiausiojo lygio susitikime buvo sudaryta ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupė, ir remia jos pastangas interneto saugumo klausimus įtraukti į transatlantinį politinį dialogą; palankiai vertina tai, kad Komisija ir JAV vyriausybė bendros ES ir JAV darbo grupės vardu drauge parengė bendrą programą ir veiksmų planą, pagal kurį 2012–2013 m. būtų vykdomos bendros suderintos tarpžemyninės kibernetinių atakų pratybos;

2012 m. birželio 12 d., antradienis

45. siūlo užmegzti struktūrinį ES ir JAV teisės aktų leidėjų dialogą, siekiant aptarti su internetu susijusius klausimus, kuris būtų bendro sutarimo, supratimo ir bendrų požiūrių paieškų dalis;

46. ragina EIVT ir Komisiją, remiantis valstybių narių Europos forumo nuveiktu darbu, išlaikyti aktyvią poziciją atitinkamuose tarptautiniuose forumuose, *inter alia*, derinant valstybių narių pozicijas, siekiant interneto saugumo ir atsparumo srityse skatinti pagrindines ES vertybes, tikslus ir politikos kryptis; pažymi, kad šiuose forumuose dalyvauja NATO, JT (visų pirma per Tarptautinę telekomunikacijų sąjungą ir Interneto valdymo forumą), Interneto vardų ir numerių paskyrimo korporacija, Interneto numerių skyrimo tarnyba, ESBO, Ekonominio bendradarbiavimo ir plėtros organizacija (OECD) ir Pasaulio bankas;

47. ragina Komisiją ir ENISA dalyvauti pagrindiniuose suinteresuotųjų subjektų diskusijose siekiant tarptautiniu lygmeniu apibrėžti technines ir teisines kibernetinės erdvės normas;

*

* *

48. paveda Pirmininkui perduoti šią rezoliuciją Tarybai ir Komisijai.

Bendradarbiavimas su užsienio partneriais energetikos politikos klausimais

P7_TA(2012)0238

2012 m. birželio 12 d. Europos Parlamento rezoliucija dėl bendradarbiavimo su užsienio partneriais energetikos politikos klausimais. Strateginis požiūris siekiant saugaus, tvaraus ir konkurencingo energijos tiekimo (2012/2029(INI))

(2013/C 332 E/04)

Europos Parlamentas,

— atsižvelgdamas į Komisijos komunikatą Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl energijos tiekimo saugumo ir tarptautinio bendradarbiavimo. „ES energetikos politika. Bendradarbiavimas su užsienio partneriais“ (COM(2011)0539),

— atsižvelgdamas į Komisijos pasiūlymą dėl Europos Parlamento ir Tarybos sprendimo, kuriuo tarpvyriausybiniams valstybių narių energetikos susitarimams su trečiosiomis šalimis nustatomas keitimosi informacija mechanizmas (COM(2011)0540),

— atsižvelgdamas į Tarybos 2011 m. lapkričio 24 d. išvadas dėl energijos tiekimo saugumo ir tarptautinio bendradarbiavimo „ES energetikos politika. Bendradarbiavimas su užsienio partneriais“,

— atsižvelgdamas į savo 2010 m. lapkričio 25 d. rezoliuciją dėl naujos energetikos strategijos Europai 2011–2020 m. ([1]),

— atsižvelgdamas į Darbo tvarkos taisyklių 48 straipsnį,

— atsižvelgdamas į Pramonės, mokslinių tyrimų ir energetikos komiteto pranešimą ir Užsienio reikalų komiteto, Vystymosi komiteto ir Tarptautinės prekybos komiteto nuomones (A7-0168/2012),

([1]) OL C 99 E, 2012 4 3, p. 64.