Otrdiena, 2012. gada 12. jūnijs

65. pievērš uzmanību vajadzībai veicināt brīvprātīgo darbu, jo īpaši 2013. gadā, kas ir Eiropas Pilsoņu gads, un aicina Komisiju starptautiskās attīstības palīdzības politikā iekļaut atbalstu brīvprātīgajam darbam, jo īpaši nolūkā īstenot visus Tūkstošgades attīstības mērķos paredzētos uzdevumus;

66. atbalsta iespēju oficiāli apsvērt solidaritātes priekšlikumu par starpiestāžu cilvēkresursu programmu ES iestādēs, lai veicinātu iestāžu personāla un stažieru iesaistīšanos brīvprātīgajā darbā un humānās palīdzības un sociālās darbībās gan personāla apmācības ietvaros, gan kā brīvprātīgu darbu;

67. uzsver, ka ierosinātā programma sniedz izmaksu ietaupījumu un augstu pievienoto vērtību un palīdzētu īstenot ES politiku un programmas;

68. iesaka Komisijai saglabāt vērtīgos kontaktpunktus, kas šajā nozarē izveidoti ar Eiropas brīvprātīgā darba gada (2011) apvienību un vēlāko Brīvprātīgo platformu, kurā iesaistītas daudzas pilsoniskās sabiedrības brīvprātīgā darba un tīklu veidošanas organizācijas, kā arī ar valstu koordinācijas iestādēm, stratēģiskiem partneriem un valstu valdību vadītājiem, ņemot vērā lielo dienestu skaitu, kas atbildīgi par brīvprātīgo darbu ES, un mudina šos kontaktpunktus izmantot ierosināto centralizēto ES portālu kā visas Eiropas platformu, lai atvieglotu turpmāku koordināciju un pastiprinātu pārrobežu aktivitāti;

69. uzsver šo kontaktu tīklu un paraugprakses apmaiņas nozīmi informācijas izplatīšanā par esošajām ES procedūrām, kas var palīdzēt un atbalstīt pārrobežu brīvprātīgo darbu;

70. aicina Komisiju attiecīgā gadījumā rīkoties saskaņā ar Eiropas Brīvprātīgā darba politikas programmu (*PAVE*), kuru izstrādāja brīvprātīgā darba organizācijas, kas bija iesaistītas Eiropas brīvprātīgā darba gada (2011) apvienībā;

71. uzdod priekšsēdētājam nosūtīt šo rezolūciju Padomei, Komisijai un dalībvalstu valdībām un parlamentiem.

Informācijas kritiskās infrastruktūras aizsardzība — virzība uz globālu kiberdrošību

P7_TA(2012)0237

Eiropas Parlamenta 2012. gada 12. jūnija rezolūcija par informācijas kritiskās infrastruktūras aizsardzību — sasniegumi un turpmākie pasākumi virzībā uz globālu kiberdrošību (2011/2284(INI))

(2013/C 332 E/03)

Eiropas Parlaments,

— ņemot vērā 2010. gada 5. maija rezolūciju „Jauna Eiropas digitālā programma — 2015.eu” [1],

— ņemot vērā 2010. gada 15. jūnija rezolūciju „Interneta pārvaldība — turpmāk veicamie pasākumi” [2],

— ņemot vērā 2011. gada 6. jūlija rezolūciju „Platjosla Eiropā — ieguldījums digitāli virzītā izsaugsmē” [3],

— ņemot vērā Reglamenta 48. pantu,

— ņemot vērā Rūpniecības, pētniecības un enerģētikas komitejas ziņojumu un Pilsoņu brīvību, tieslietu un iekšlietu komitejas atzinumu (A7-0167/2012),

[1] OV C 81E, 15.3.2011., 45. lpp.
[2] OV C 236E, 12.8.2011., 33. lpp.
[3] Pieņemtie teksti, P7_TA(2011)0322.

A. tā kā informācijas un komunikācijas tehnoloģijas (IKT) var nodrošināt pilnvērtīgu ieguldījumu ekonomikas un sabiedrības attīstībā tikai tad, ja lietotāji tām uzticas un ir pārliecināti par to drošību un elastīgumu un ja interneta vidē efektīvi īsteno spēkā esošos tiesību aktus datu konfidencialitātes un intelektuālā īpašuma jomā;

B. tā kā interneta un IKT ietekme uz dažādiem iedzīvotāju dzīves aspektiem pieaug arvien straujāk un tā kā tie ir nozīmīgs sabiedrības mijiedarbības, kultūras bagātināšanas un ekonomikas izaugsmes dzinējspēks;

C. tā kā IKT un interneta drošība ir plašs jēdziens, kas globālā mērogā ietekmē ekonomiskos, sociālos, tehnoloģiskos un militāros aspektus, tāpēc ir nepieciešams skaidri definēt un diferencēt pienākumus, kā arī izveidot spēcīgu starptautiskās sadarbības mehānismu;

D. tā kā pamatiniciatīvas „Eiropas digitalizācijas programma" mērķis ir uzlabot Eiropas konkurētspēju, stiprinot IKT, un radīt apstākļus straujai un stabilai izaugsmei un uz tehnoloģijām balstītu darba vietu izveidei;

E. tā kā privātajam sektoram joprojām ir galvenā investora, īpašnieka un pārvaldītāja statuss attiecībā uz informācijas drošības produktiem, pakalpojumiem, lietojumiem un infrastruktūru, pēdējos desmit gados tajos ieguldot miljardiem euro; tā kā šī līdzdalība būtu jāuzlabo ar atbilstošām politikas stratēģijām, lai veicinātu publiskajam, privātajam vai publiskajam un privātajam sektoram piederošo vai to apsaimniekoto infrastruktūru elastīgumu;

F. tā kā ļoti drošu un elastīgu IKT tīklu, pakalpojumu un tehnoloģiju izstrādei būtu jāpaaugstina ES ekonomikas konkurētspēja, gan uzlabojot kiberdrošības riska novērtēšanu un pārvaldību, gan arī nodrošinot ES ekonomikai kopumā stabilākas informācijas infrastruktūras, lai atbalstītu inovācijas un izaugsmi un tādējādi radītu uzņēmējiem jaunas iespējas uzlabot produktivitāti;

G. tā kā pieejamie tiesībaizsardzības dati attiecībā uz kibernoziegumiem (ieskaitot kiberuzbrukumus, kā arī cita veida noziegumus tiešsaistē) norāda uz ievērojamu noziedzības pieaugumu vairākās Eiropas valstīs; tā kā gan tiesībaizsardzības iestāžu, gan arī *CERT* (datorapdraudējumu reaģēšanas vienības) sniegtie statistiski reprezentatīvie dati attiecībā uz kiberuzbrukumiem tomēr joprojām nav pietiekami un to apkopošanas procedūra turpmāk būs jāuzlabo, lai pastiprinātu tiesībaizsardzības iestāžu reakciju visā ES un nodrošinātu, ka likumdevēji, reaģējot uz aizvien pieaugošajiem kibernoziedzības draudiem, ir labāk informēti;

H. tā kā stabilai interneta pakalpojumu attīstībai ir nepieciešams atbilstošs informācijas drošības līmenis;

I. tā kā nesen notikušie kiberincidenti, infrastruktūru darbības pārrāvumi un uzbrukumi ES iestāžu, nozares un dalībvalstu informācijas infrastruktūrai liecina par vajadzību izveidot stabilu, novatorisku un efektīvu informācijas kritiskās infrastruktūras aizsardzības (*CIIP*) sistēmu, kas balstītos uz visaptverošu starptautisko sadarbību un obligātajiem elastīguma standartiem starp dalībvalstīm;

J. tā kā jaunu IKT līdzekļu, piemēram, mākoņdatošanas, straujā attīstība liek pastiprināti pievērsties drošībai, lai varētu pilnībā izmantot visas tehnoloģiju sasniegumu sniegtās priekšrocības;

K. tā kā Eiropas Parlaments ir vairākkārt pieprasījis piemērot augstus standartus datu konfidencialitātes un datu aizsardzības, tīkla neitralitātes un intelektuālā īpašuma tiesību aizsardzības jomā,

Pasākumi CIIP stiprināšanai valstu un Savienības mērogā

1. atzinīgi vērtē to, ka dalībvalstis īsteno Eiropas programmu *CIIP* jomā, tostarp izveidojot Kritiskās infrastruktūras brīdinājuma informācijas tīklu (*CIWIN*);

2. uzskata, ka ar *CIIP* saistītie centieni ne vien palielinās iedzīvotāju vispārējo drošību, bet arī uzlabos viņu izpratni par drošību un viņu uzticēšanos valdības veiktajiem pasākumiem iedzīvotāju aizsardzības jomā;

Otrdiena, 2012. gada 12. jūnijs

3. atzīst, ka Komisija apsver Padomes Direktīvas 2008/114/EK ([1]) pārskatīšanu, un aicina pirms turpmāku darbību veikšanas sniegt pierādījumus par direktīvas efektivitāti un ietekmi; aicina apsvērt tās darbības jomas paplašināšanu, jo īpaši iekļaujot IKT nozari un finanšu pakalpojumus; aicina arī apsvērt tādas jomas kā veselības aprūpe, pārtikas un ūdens piegādes sistēmas, kodolpētniecība un rūpniecība (ja uz tām neattiecas īpaši noteikumi); uzskata, ka arī šīm nozarēm būtu jāizmanto priekšrocības, ko sniedz *CIWIN* īstenotā starpnozaru pieeja (ko veido sadarbība, brīdināšanas sistēma un paraugprakses apmaiņa);

4. uzsver, ka ir svarīgi ieviest un nodrošināt ilgstošu Eiropas pētniecības integrāciju, lai saglabātu un uzlabotu Eiropas izcilību *CIIP* jomā;

5. ņemot vērā savstarpēji savienotās un ļoti saistītās, jutīgās, stratēģiskās un neaizsargātās dalībvalstu un Eiropas informācijas kritiskās infrastruktūras, aicina regulāri atjaunināt obligātos elastīguma standartus, lai nodrošinātu gatavību un reaģēšanu uz infrastruktūru darbības pārrāvumiem, incidentiem, iznīcināšanas mēģinājumiem vai uzbrukumiem, piemēram, tādiem, kas pieļauti nepietiekami stabilas infrastruktūras vai nepietiekami drošu termināļu dēļ;

6. uzsver informācijas drošības standartu un protokolu nozīmi un atzinīgi vērtē 2011. gadā piešķirto mandātu *CEN*, *Cenelec* un *ETSI* drošības standartu izstrādei;

7. vēlas, lai informācijas kritisko infrastruktūru īpašnieki un apsaimniekotāji ļautu un, ja nepieciešams, palīdzētu lietotājiem izmantot atbilstošus līdzekļus, lai tos pasargātu no ļaunprātīgiem uzbrukumiem un/vai infrastruktūru darbības pārrāvumiem, vajadzības gadījumā nodrošinot gan personisku, gan arī automatizētu uzraudzību;

8. atbalsta publisko un privāto ieinteresēto personu sadarbību Savienības līmenī, kā arī to centienus izstrādāt un ieviest drošības un elastīguma standartus civilajām (publiskajām, privātajām vai publiskajām un privātajām) valstu un Eiropas informācijas kritiskajām infrastruktūrām;

9. uzsver visā Eiropā nodrošināmu mācību nozīmīgumu, lai sagatavotos liela mēroga starpgadījumiem saistībā ar tīkla drošību, kā arī vienota standartu kopuma izveidošanas nozīmīgumu, lai novērtētu apdraudējumu;

10. aicina Komisiju sadarbībā ar dalībvalstīm novērtēt *CIIP* rīcības plāna īstenošanu; mudina dalībvalstis izveidot labi funkcionējošas valstu/valdību datorapdraudējumu reaģēšanas vienības, izstrādāt valsts kiberdrošības stratēģijas, organizēt regulāras valsts un Eiropas mēroga mācības kiberincidentu jomā, izstrādāt valsts plānus ārkārtas rīcībai kiberincidentu gadījumos un sniegt ieguldījumu Eiropas kiberincidentu ārkārtas rīcības plāna izstrādē līdz 2012. gada beigām;

11. iesaka ieviest apsaimniekotāju drošības plānus vai veikt līdzvērtīgus pasākumus attiecībā uz visām Eiropas informācijas kritiskajām infrastruktūrām un iecelt sadarbības koordinatorus drošības jomā;

12. atzinīgi vērtē Padomes Pamatlēmuma 2005/222/TI ([2]) par uzbrukumiem informācijas sistēmām pašreizējo pārskatīšanu; atzīmē, ka jākoordinē ES pasākumi cīņā pret liela mēroga kiberuzbrukumiem, izmantojot *ENISA*, dalībvalstu *CERT* un nākotnē arī Eiropas *CERT* kompetenci;

13. uzskata, ka *ENISA* Eiropas līmenī var būt nozīmīga loma informācijas kritiskās infrastruktūras aizsardzībā, nodrošinot dalībvalstīm, Eiropas Savienības iestādēm un struktūrām tehniskas zināšanas, kā arī sniedzot ziņojumus un analīzi saistībā ar informācijas sistēmu drošību Eiropas un pasaules mērogā;

ES turpmākie pasākumi stabilai drošībai internetā

14. mudina Eiropas Tīklu un informācijas drošības aģentūru (*ENISA*) koordinēt un īstenot ES informācijas mēnešus par drošību internetā, lai jautājumi saistībā ar kiberdrošību nokļūtu īpašā dalībvalstu un ES iedzīvotāju uzmanības lokā;

([1]) OV L 345, 23.12.2008., 75. lpp.
([2]) OV L 69, 16.3.2005., 67. lpp.

15. saskaņā ar Digitalizācijas programmā izvirzītajiem mērķiem palīdz *ENISA* pildīt tās pienākumus attiecībā uz tīklu informācijas drošību un jo īpaši sniegt norādījumus un ieteikumus dalībvalstīm par to, kā to *CERT* nodrošināt bāzes spējas, kā arī veicināt paraugprakses apmaiņu, radot uzticēšanās atmosfēru; aicina aģentūru apspriesties ar attiecīgajām ieinteresētajām personām, lai noteiktu līdzīgus kiberdrošības pasākumus privāto tīklu un infrastruktūru īpašniekiem un apsaimniekotājiem, kā arī palīdzēt Komisijai un dalībvalstīm izstrādāt un ieviest informācijas drošības sertifikācijas shēmas, uzvedības normas un sadarbības praksi starp valstu un Eiropas *CERT* un infrastruktūru īpašniekiem un apsaimniekotājiem, ja tas ir nepieciešams, nosakot tehnoloģiski neitrālas kopīgās obligātās prasības;

16. atzinīgi vērtē pašreizējo priekšlikumu pārskatīt *ENISA* mandātu, jo īpaši attiecībā uz tā pagarināšanu un aģentūras pienākumu jomas paplašināšanu; uzskata, ka līdztekus palīdzībai dalībvalstīm, sniedzot ekspertu zināšanas un analīzi, *ENISA* vajadzētu būt tiesīgai vadīt vairākus administratīvus uzdevumus ES līmenī un sadarbībā ar attiecīgajiem kolēģiem ASV saistībā ar tīkla un informācijas drošības incidentu novēršanu un atklāšanu un dalībvalstu sadarbības uzlabošanu; norāda, ka saskaņā ar *ENISA* regulu šai aģentūrai varētu tikt uzticēti arī citi pienākumi, kas saistīti ar reaģēšanu uz uzbrukumiem internetā, ciktāl tas nodrošina skaidru pievienoto vērtību esošajiem valstu reaģēšanas mehānismiem;

17. atzinīgi vērtē 2010. un 2011. gadā Eiropas mērogā notikušo kiberdrošības mācību rezultātus, kuras tika īstenotas visā Savienībā *ENISA* uzraudzībā un kuru mērķis bija sniegt palīdzību dalībvalstīm Eiropas ārkārtas rīcības plāna izstrādē, uzturēšanā un izmēģināšanā; aicina *ENISA* šādas mācības saglabāt savā programmā un attiecīgā gadījumā pakāpeniski iesaistīt attiecīgos privātos apsaimniekotājus, lai uzlabotu Eiropas vispārējās spējas interneta drošības jomā; sagaida turpmāku paplašināšanos starptautiskā mērogā, pievienojoties līdzīgi domājošiem partneriem;

18. aicina dalībvalstis izstrādāt valsts ārkārtas rīcības plānus kiberincidentu jomā un iekļaut tādus svarīgus elementus kā atbilstīgi kontaktpunkti un noteikumi par palīdzību, ierobežošanu un novēršanu infrastruktūru darbības pārrāvumu vai reģionāla, valsts vai starptautiska mēroga uzbrukumu gadījumā; norāda, ka dalībvalstīm būtu jāievieš arī atbilstīgi koordinēšanas mehānismi un struktūras valsts līmenī, kas palīdzētu uzlabot kompetento valsts iestāžu koordināciju un uzlabotu to darbības saskaņotību;

19. iesaka Komisijai ierosināt saistošus pasākumus ar ES ārkārtas rīcības plānu kiberincidentu jomā, lai ES līmenī uzlabotu tehnisko un vadošo funkciju koordināciju starp valstu un valdību *CERT*;

20. aicina Komisiju un dalībvalstis veikt vajadzīgos pasākumus, lai aizsargātu kritisko infrastruktūru no kiberuzbrukumiem un nodrošinātu iespējas hermētiski slēgt piekļuvi kritiskajai infrastruktūrai tieša kiberuzbrukuma gadījumā, kas nopietni apdraud šīs infrastruktūras pienācīgu darbību;

21. sagaida, kad pilnībā tiks ieviesta ES *CERT*, kurai būs galvenā loma pret ES iestādēm vērstu tīšu un ļaunprātīgu kiberuzbrukumu novēršanā, atklāšanā, reaģēšanā uz tiem un normālas darbības atjaunošanā;

22. iesaka Komisijai ierosināt saistošus pasākumus, kas izstrādāti nolūkā piemērot obligātos drošības un elastīguma standartus un uzlabot valstu *CERT* koordināciju;

23. aicina dalībvalstis un ES iestādes nodrošināt labi funkcionējošas *CERT* ar obligātām drošības un elastīguma spējām, kuru pamatā ir saskaņota paraugprakse; uzsver, ka valstu *CERT* vajadzētu būt iekļautām efektīvā tīklā, kur saskaņā ar nepieciešamajiem konfidencialitātes standartiem tiek veikta attiecīgās informācijas apmaiņa; prasa katrā dalībvalstī nodrošināt *CIIP* pakalpojumu nepārtrauktību divdesmit četras stundas diennaktī un septiņas dienas nedēļā, kā arī izveidot Eiropas kopējo protokolu ārkārtas situācijām, kas piemērojams valstu kontaktpunktiem;

24. uzsver, ka uzticēšanās vairošanai un sadarbības veicināšanai starp dalībvalstīm ir ļoti iela nozīme datu un valstu tīklu un infrastruktūru aizsardzībā; aicina Komisiju ierosināt vienotu procedūru, lai apzinātu un noteiktu vienotu pieeju, kā reaģēt uz IKT pārrobežu draudiem, sagaidot, ka dalībvalstis sniegs Komisijai vispārēju informāciju par to informācijas kritisko infrastruktūru riskiem, draudiem un neaizsargātību;

Otrdiena, 2012. gada 12. jūnijs

25. atzinīgi vērtē Komisijas iniciatīvu laikā līdz 2013. gadam izveidot Eiropas Informācijas apmaiņas un brīdināšanas sistēmu;

26. atzinīgi vērtē Komisijas ierosinātās apspriedes ar dažādām ieinteresētajām personām par drošību internetā un *CIIP*, kā, piemēram, Eiropas publiskā un privātā sektora partnerību infrastruktūru elastīguma jautājumos; atzīst IKT pārdošanas uzņēmumu līdzšinējo nozīmīgo iesaistīšanos un ieguldījumu šajā darbā; mudina Komisiju turpināt darbu, lai veicinātu akadēmisko aprindu un IKT lietotāju apvienību aktīvāku iesaistīšanos, un stimulēt konstruktīvu dažādu ieinteresēto personu dialogu par kiberdrošības jautājumiem; atbalsta Digitālās asamblejas kā *CIIP* pārvaldes struktūras turpmāku pilnveidošanu;

27. atzinīgi vērtē līdzšinējo Dalībvalstu Eiropas foruma darbu saistībā ar nozarei specifisku kritēriju noteikšanu Eiropas kritisko infrastruktūru identificēšanai, īpašu uzmanību pievēršot fiksētajiem un mobilajiem sakariem, kā arī saistībā ar ES principu un vadlīniju apspriešanu attiecībā uz elastīgumu un stabilitāti internetā; cer, ka turpināsies darbs, lai panāktu vienprātību dalībvalstu vidū, un šajā saistībā aicina forumu pilnveidot pašreizējo pieeju, kas vērsta uz fiziskajiem aktīviem, paredzot pasākumus, lai ietvertu arī loģiskās infrastruktūras aktīvus, kuru nozīme *CIIP* efektivitātes nodrošināšanā, attīstoties virtualizācijai un mākoņu tehnoloģijām, aizvien pieaugs;

28. iesaka Komisijai uzsākt publisku Eiropas mēroga izglītības iniciatīvu, kas vērsta uz privāto un komerciālo galalietotāju izglītošanu un izpratnes veidošanu par iespējamajiem draudiem internetā un fiksētajām un mobilajām IKT ierīcēm ikvienā pakalpojumu ķēdes līmenī, kā arī uz drošākas indivīdu uzvedības veicināšanu tiešsaistē; šajā sakarā atgādina par risku saistībā ar novecojušu IT aprīkojumu un programmatūru;

29. aicina dalībvalstis ar Komisijas atbalstu pilnveidot mācību un izglītības programmas informācijas drošības jomā, kas paredzētas valstu tiesībaizsardzības un tiesu iestādēm un attiecīgajām ES aģentūrām;

30. atbalsta ES mācību programmas izveidi zinātniskajiem ekspertiem informācijas drošības jomā, jo tas sekmētu ES kompetenci un sagatavotību attiecībā uz kibertelpu, kas nepārtraukti attīstās, un ar to saistītajiem draudiem;

31. pauž atbalstu izglītības veicināšanai kiberdrošības jomā (doktorantūras studentu praksēm, universitāšu programmām, semināriem, studentu apmācībai u.c.) un specializētai apmācībai *CIIP*;

32. aicina Komisiju līdz 2012. gada beigām ierosināt visaptverošu Savienības stratēģiju drošībai internetā, kas būtu balstīta uz skaidru terminoloģiju; uzskata, ka stratēģijas par drošību internetā mērķim vajadzētu būt tādas kibertelpas radīšanai (balstoties uz drošu un elastīgu infrastruktūru un atvērtiem standartiem), kas ar brīvu informācijas plūsmu radītu labvēlīgus apstākļus inovācijām un labklājībai, vienlaicīgi nodrošinot konfidencialitātes un citu pilsoņu brīvību stingru aizsardzību; uzskata, ka stratēģijā būtu detalizēti jāizklāsta principi, mērķi, metodes, instrumenti un politikas (gan iekšējās, gan ārējās) nostādnes, kas ir vajadzīgas, lai racionalizētu valstu un ES centienus un izveidotu obligātos elastīguma standartus starp dalībvalstīm, lai garantētu drošu, nepārtrauktu, stabilu un elastīgu pakalpojumu — gan saistībā ar kritisko infrastruktūru, gan ar vispārēju interneta izmantojumu;

33. uzsver, ka gaidāmajā Komisijas interneta drošības stratēģijā par galveno atskaites punktu būtu jānosaka darbs saistībā ar *CIIP* un jāparedz mērķis īstenot vienotu un sistemātisku pieeju kiberdrošībai, ietverot gan preventīvus pasākumus, piemēram, obligātu drošības pasākumu standartu ieviešanu vai individuālu lietotāju, uzņēmumu un publisku iestāžu pārstāvju apmācību, gan atbildes pasākumus, piemēram, krimināltiesiskas, civiltiesiskas un administratīvas sankcijas;

34. mudina Komisiju ierosināt stingru mehānismu, lai koordinētu stratēģijas par drošību internetā īstenošanu un regulāru atjaunināšanu; uzskata, ka šis mehānisms būtu jāatbalsta ar pietiekamiem administratīviem, ekspertu un finanšu resursiem, un tā kompetencē būtu jāietver palīdzības sniegšana ES nostājas veidošanā attiecībās gan ar vietējām, gan starptautiskām ieinteresētajām personām par jautājumiem saistībā ar drošību internetā;

35. aicina Komisiju ierosināt ES regulējumu ziņošanai par drošības pārkāpumiem tādās kritiskajās nozarēs kā enerģētika, transports, ūdens un pārtikas piegāde, kā arī IKT un finanšu pakalpojumu nozarēs, lai nodrošinātu, ka attiecīgās dalībvalstu iestādes un lietotāji ir informēti par kiberincidentiem, kiberuzbrukumiem un infrastruktūru darbības pārrāvumiem;

36. mudina Komisiju uzlabot pieeju statistiski reprezentatīvajiem datiem par izmaksām, ko rada kiberuzbrukumi ES, dalībvalstīs un nozarē (jo īpaši finanšu pakalpojumu un IKT nozarē), uzlabojot datu vākšanas spējas plānotajam Eiropas kibernoziedzības centram (paredzēts izveidot līdz 2013. gadam), kā arī *CERT* un citām Komisijas iniciatīvām, piemēram, Eiropas Informācijas apmaiņas un brīdināšanas sistēmai, lai nodrošinātu sistemātisku ziņošanu un informācijas apmaiņu par kiberuzbrukumiem un citiem kibernoziedzības veidiem, kas vērsti pret Eiropas nozari un dalībvalstīm, un tādējādi pastiprinātu tiesību aizsardzību;

37. paužatbalstu ciešai dalībvalstu privātā sektora un *ENISA* saiknei un mijiedarbībai, lai dalībvalstu/valsts pārvaldes iestāžu *CERT* darbotos saskaņoti ar Eiropas Informācijas apmaiņas un brīdināšanas sistēmas (*EISAS*) pilnveidošanu;

38. norāda, ka galvenais virzītājspēks tādu tehnoloģiju izstrādei un izmantošanai, kas ir paredzētas drošības palielināšanai internetā, ir IKT nozare; atgādina, ka ES politika nedrīkst radīt šķēršļus Eiropas interneta ekonomikas izaugsmei un tajā jāiekļauj vajadzīgie stimuli, lai pilnībā izmantotu uzņēmumu un publiskā un privātā sektora partnerību sniegtās iespējas; iesaka izpētīt jaunus stimulus nozarei, lai izstrādātu stingrākus apsaimniekotāju drošības plānus saskaņā ar Direktīvu 2008/114/EK;

39. aicina Komisiju iesniegt tiesību akta priekšlikumu turpmākai krimināltbildības noteikšanai par kiberuzbrukumiem ((piem., pikšķerēšanu, krāpšanu tiešsaistē u. c.);

Starptautiskā sadarbība

40. atgādina, ka starptautiskā sadarbība ir svarīgākais instruments efektīvu kiberdrošības pasākumu īstenošanai; atzīst, ka pašlaik ES nav pastāvīgi iesaistīta ar kiberdrošību saistītos starptautiskās sadarbības procesos un dialogos; aicina Komisiju un Eiropas Ārējās darbības dienestu sākt konstruktīvu dialogu ar visām valstīm, kuras pārstāv līdzīgu viedokli, nolūkā radīt kopīgu izpratni un politiku ar mērķi nodrošināt lielāku interneta un kritiskās infrastruktūras elastīgumu; uzskata, ka tajā pašā laikā ES ārējo attiecību jomā būtu pastāvīgi jāiekļauj ar drošību internetā saistītie jautājumi, cita starpā izstrādājot dažādus finansēšanas instrumentus vai noslēdzot starptautiskas vienošanās, kas paredz sensitīvu datu apmaiņu un glabāšanu;

41. atzīmē 2001. gadā Budapeštā parakstītās Eiropas Padomes konvencijas par kibernoziegumiem pozitīvos sasniegumus; tomēr norāda — aicinot, lai šo konvenciju paraksta un ratificē arī citas valstis, Eiropas Ārējās darbības dienestam vienlaicīgi jāpanāk arī divpusējas un daudzpusējas vienošanās par interneta drošību un elastīgumu ar līdzīgi domājošiem starptautiskiem partneriem;

42. norāda — lai izvairītos no darbību dublēšanās, ir jākoordinē daudzie pasākumi, kurus pašlaik veic dažādas starptautiskās un ES iestādes, struktūras un aģentūras, kā arī dalībvalstis, un šajā nolūkā ir vērts apsvērt iespēju izraudzīties par koordinēšanu atbildīgu ierēdni, iespējams, ieceļot amatā ES kiberdrošības koordinatoru;

43. uzsver, ka īpaši liela nozīme ir strukturētam dialogam starp ES un ASV galvenajiem dalībniekiem un likumdevējiem, kuri ir iesaistīti *CIIP*, lai veidotu vienotu izpratni, interpretāciju un nostāju attiecībā uz tiesisko regulējumu un pārvaldības sistēmām;

44. atzinīgi vērtē 2010. gada novembra ES un ASV augstākā līmeņa sanāksmē izveidoto ES un ASV darba grupu kiberdrošības un kibernoziedzības jomā un atbalsta tās centienus interneta drošības jautājumus ietvert transatlantiskās politikas dialogā; atzinīgi vērtē to, ka Komisija un ASV valdība ES un ASV darba grupas vadībā kopīgi izstrādāja kopēju programmu un ceļvedi par kopīgām/sinhronizētām un transkontinentālām kibermācībām 2012./2013. gadā;

45. iesaka izveidot strukturētu dialogu starp ES un ASV likumdevējām iestādēm, lai apspriestu ar internetu saistītus jautājumus kā daļu no centieniem panākt kopīgu izpratni, interpretāciju un nostājas;

46. mudina Eiropas Ārējās darbības dienestu un Komisiju, balstoties uz Dalībvalstu Eiropas foruma paveikto darbu, nodrošināt aktīvu nostāju atbilstīgajos starptautiskajos forumos, cita starpā saskaņojot dalībvalstu nostājas, lai veicinātu ES pamatvērtību, mērķu un politikas īstenošanu jomā, kas saistīta ar drošību internetā un interneta elastīgumu; norāda, ka šādi forumi ir NATO, ANO (jo īpaši ar Starptautiskās Elektrosakaru savienības un Interneta pārvaldības foruma starpniecību), Piešķirto nosaukumu un numuru interneta korporācija, *Internet* numurpiešķires institūcija, EDSO (Eiropas Drošības un sadarbības organizācija), ESAO (Ekonomiskās sadarbības un attīstības organizācija) un Pasaules Banka;

47. mudina Komisiju un *ENISA* iesaistīties galveno ieinteresēto personu dialogos, lai starptautiskā līmenī definētu tehniskās un tiesiskās normas kibertelpā;

*

* *

48. uzdod priekšsēdētājam nosūtīt šo rezolūciju Padomei un Komisijai.

Sadarbība enerģētikas politikā ar partneriem ārpus ES robežām

P7_TA(2012)0238

Eiropas Parlamenta 2012. gada 12. jūnija rezolūcija par sadarbības veidošanu enerģētikas politikā ar partneriem ārpus ES robežām— stratēģiska pieeja drošas, ilgtspējīgas un konkurētspējīgas energoapgādes nodrošināšanai (2012/2029(INI))

(2013/C 332 E/04)

Eiropas Parlaments,

— ņemot vērā Komisijas paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par energoapgādes drošību un starptautisko sadarbību — „ES enerģētikas politika: attiecību veidošana ar partneriem ārpus mūsu robežām" (COM(2011)0539),

— ņemot vērā Komisijas priekšlikumu Eiropas Parlamenta un Padomes lēmumam, ar ko izveido informācijas apmaiņas mehānismu attiecībā uz starpvaldību nolīgumiem starp dalībvalstīm un trešām valstīm enerģētikas jomā (COM(2011)0540),

— ņemot vērā Padomes 2011. gada 24. novembra secinājumus par energoapgādes drošību un starptautisko sadarbību — „ES enerģētikas politika: attiecību veidošana ar partneriem ārpus mūsu robežām",

— ņemot vērā Parlamenta 2010. gada 25. novembra rezolūciju „Topošā jaunā Eiropas enerģētikas stratēģija 2011.–2020. gadam" ([1]),

— ņemot vērā Reglamenta 48. pantu,

— ņemot vērā Rūpniecības, pētniecības un enerģētikas komitejas ziņojumu un Ārlietu komitejas, Attīstības komitejas un Starptautiskās tirdzniecības komitejas atzinumus (A7-0168/2012),

([1]) OV C 99 E, 3.4.2012., 64. lpp.