Ceturtdiena, 2013. gada 12. septembris

4. prasa Komisijai palīdzēt dalībvalstīm samazināt no dzimuma atkarīgas darba samaksas atšķirību par vismaz 5 % gadā, lai līdz 2020. gadam no dzimuma atkarīgu darba samaksas atšķirību varētu likvidēt;

5. atzīst – lai īstenotu daudzpusīgu vairāklīmeņu pieeju, Komisijai ir jāpalīdz dalībvalstīm sekmēt labu praksi un īstenot politikas virzienus no dzimuma atkarīgas darba samaksas atšķirības mazināšanai;

6. mudina Komisiju nekavējoties pārskatīt Direktīvu 2006/54/EK un ierosināt tajā grozījumus saskaņā ar minētās direktīvas 32. pantu un pamatojoties uz LESD 157. pantu, ievērojot sīki izstrādātus ieteikumus, kas izklāstīti Eiropas Parlamenta 2012. gada 24. maija rezolūcijas pielikumā;

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

P7_TA(2013)0376

ES kiberdrošības stratēģija – atvērta un droša kibertelpa

Eiropas Parlamenta 2013. gada 12. septembra rezolūcija par ES kiberdrošības stratēģiju – atvērta un droša kibertelpa (2013/2606(RSP))

(2016/C 093/16)

Eiropas Parlaments,

— ņemot vērā 2013. gada 7. februāra Eiropas Komisijas un Eiropas Savienības Augstās pārstāves ārlietās un drošības politikas jautājumos kopīgo paziņojumu "Eiropas Savienības kiberdrošības stratēģija – atvērta un droša kibertelpa" (JOIN(2013)0001),

— ņemot vērā Komisijas 2013. gada 7. februāra priekšlikumu direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā (COM(2013)0048),

— ņemot vērā Komisijas gada 2010. gada 19. maija paziņojumu "Digitālā programma Eiropai" (COM(2010)0245) un 2012. gada 18. decembra paziņojumu "Eiropas digitalizācijas programma – digitalizācijas virzīta Eiropas izaugsme" (COM(2012)0784),

— ņemot vērā Komisijas 2012. gada 27. septembra paziņojumu "Mākoņdatošanas potenciāla atraisīšana Eiropā" (COM (2012)0529),

— ņemot vērā Komisijas 2012. gada 28. marta paziņojumu "Vēršanās pret noziedzību mūsu digitālajā laikmetā: Eiropas Kibernoziedzības centra izveide" (COM(2012)0140) un ņemot vērā Padomes 2012. gada 7. jūnija secinājumus par šo paziņojumu,

— ņemot vērā Eiropas Parlamenta un Padomes 2013. gada 12. augusta Direktīvu 2013/40/ES par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI ([1]),

— ņemot vērā Padomes 2008. gada 8. decembra Direktīvu 2008/114/EK par to, lai apzinātu un noteiktu Eiropas kritiskās infrastruktūras un novērtētu vajadzību uzlabot to aizsardzību ([2]),

([1]) OV L 218, 14.8.2013., 8. lpp.
([2]) OV L 345, 23.12.2008., 75. lpp.

— ņemot vērā Eiropas Parlamenta un Padomes 2011. gada 13. decembra Direktīvu 2011/92/ES par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu, un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI ([1]),

— ņemot vērā Stokholmas programmu ([2]) par brīvības, drošības un tiesiskuma telpu, Komisijas paziņojumus "Brīvības, drošības un tiesiskuma telpas nodrošināšana Eiropas pilsoņiem – Stokholmas programmas īstenošanas rīcības plāns" (COM(2010)0171) un "ES iekšējās drošības stratēģija darbībā – pieci soļi pretim drošākai Eiropai" (COM(2010)0673), kā arī Parlamenta 2012. gada 22. maija rezolūciju par Eiropas Savienības iekšējās drošības stratēģiju ([3]),

— ņemot vērā Komisijas un augstās pārstāves kopīgu priekšlikumu Padomes lēmumam par kārtību, kādā Savienība īsteno solidaritātes klauzulu (JOIN(2012)0039),

— ņemot vērā Padomes 2001. gada 28. maija Pamatlēmumu 2001/413/TI par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem ([4]),

— ņemot vērā 2012. gada 12. jūnija rezolūciju par informācijas kritiskās infrastruktūras aizsardzību – sasniegumi un turpmākie pasākumi virzībā uz globālu kiberdrošību ([5]) un Padomes 2011. gada 27. maija secinājumus par Komisijas paziņojumu par informācijas kritiskās infrastruktūras aizsardzību "Sasniegumi un turpmākie pasākumi – virzība uz globālu kiberdrošību" (COM(2011)0163),

— ņemot vērā 2012. gada 11. decembra rezolūciju par vienotā digitālā tirgus izveides pabeigšanu ([6]),

— ņemot vērā 2012. gada 22. novembra rezolūciju par kiberdrošību un kiberaizsardzību ([7]),

— ņemot vērā 2013. gada 16. aprīļa nostāju pirmajā lasījumā par priekšlikumu Eiropas Parlamenta un Padomes regulai, kas attiecas uz Eiropas Tīklu un informācijas drošības aģentūru *(ENISA)* (COM(2010)0521) ([8]),

— ņemot vērā 2012. gada 11. decembra rezolūciju par Digitālās brīvības stratēģiju ES ārpolitikā ([9]),

— ņemot vērā Eiropas Padomes 2001. gada 23. novembra Konvenciju par kibernoziegumiem,

— ņemot vērā Savienības starptautiskās saistības, jo īpaši saskaņā ar Vispārējo vienošanos par pakalpojumu tirdzniecību *(GATS)*,

— ņemot vērā Līguma par Eiropas Savienības darbību (LESD) 16. pantu un Eiropas Savienības Pamattiesību hartu, jo īpaši tās 6., 8. un 11. pantu,

— ņemot vērā notiekošās sarunas par transatlantisko tirdzniecības un ieguldījumu partnerību *(TTIP)* starp Eiropas Savienību un Amerikas Savienotajām Valstīm,

— ņemot vērā Reglamenta 110. panta 2. punktu,

A. tā kā pieaugošās ar kiberdrošību saistītās problēmas, kas izpaužas kā arvien izsmalcinātāki draudi un uzbrukumi, ir nozīmīgs apdraudējums gan dalībvalstu drošībai, stabilitātei un ekonomiskajai labklājībai, gan arī privātajam sektoram un sabiedrībai kopumā; tā kā Eiropas sabiedrības un tautsaimniecības aizsardzība tādēļ ir pastāvīgi risināms uzdevums;

([1]) OV L 335, 17.12.2011., 1. lpp.
([2]) OV C 115, 4.5.2010., 1. lpp.
([3]) Pieņemtie teksti, P7_TA(2012)0207.
([4]) OV L 149, 2.6.2001., 1. lpp.
([5]) Pieņemtie teksti, P7_TA(2012)0237.
([6]) Pieņemtie teksti, P7_TA(2012)0468.
([7]) Pieņemtie teksti, P7_TA(2012)0457.
([8]) Pieņemtie teksti, P7_TA(2013)0103.
([9]) Pieņemtie teksti, P7_TA(2012)0470.

Ceturtdiena, 2013. gada 12. septembris

B. tā kā kibertelpas jautājumiem un kiberdrošībai vajadzētu būt vienam no stratēģiskajiem balstiem ES un ikvienas dalībvalsts drošības un aizsardzības politikā; tā kā ir ļoti svarīgi nodrošināt, lai kibertelpa arī turpmāk paliktu atvērta brīvai ideju un informācijas plūsmai un tajā tiktu nodrošināta vārda brīvība;

C. tā kā elektroniskā komercija un tiešsaistes pakalpojumi ir nozīmīga interneta joma un tie ir ļoti svarīgi stratēģijas "Eiropa 2020" mērķu sasniegšanai, sniedzot labumu gan iedzīvotājiem, gan privātajam sektoram; tā kā Savienībai ir pilnībā jāīsteno potenciāls un iespējas, ka internets piedāvā vienotā tirgus turpmākai attīstībai, tostarp digitālā vienotā tirgus attīstībai;

D. tā kā kopīgajā paziņojumā par Eiropas Savienības kiberdrošības stratēģiju izklāstītās stratēģiskās prioritātes paredz panākt kibernoturību, samazināt kibernoziedzību, attīstīt kiberaizsardzības politiku un veidot kiberspējas saistībā ar kopējo drošības un aizsardzības politiku (KDAP) un panākt saskaņotu ES starptautisko kibertelpas politiku;

E. tā kā tīklu un informācijas sistēmas visā Savienībā ir savstarpēji ļoti saistītas; tā kā interneta globālais raksturs nosaka to, ka daudzi tīklu un informācijas drošības negadījumi sniedzas pāri valstu robežām un var apdraudēt iekšējā tirgus darbību un patērētāju uzticēšanos digitālajā vienotajā tirgū;

F. tā kā kiberdrošība visā Savienībā, tāpat kā citur pasaulē, ir tikai tik stipra, cik stiprs ir tās vājākais posms, un traucējumi vienā jomā vai dalībvalstī var ietekmēt citas jomas vai dalībvalstis, radot domino efektu, kas ietekmē Savienības ekonomiku kopumā;

G. tā kā 2013. gada aprīlī tikai 13 dalībvalstis bija apstiprinājušas oficiālās valsts kiberdrošības stratēģijas; tā kā starp dalībvalstīm vēl arvien ir būtiskas atšķirības attiecībā uz to sagatavotību, drošību, stratēģisko kultūru un spēju izstrādāt un īstenot valsts kiberdrošības stratēģijas, un tā kā šīs atšķirības būtu jānovērtē;

H. tā kā dažāda drošības kultūra un tiesiskā regulējuma trūkums rada sadrumstalotību un ir galvenā problēma digitālajā vienotajā tirgū; tā kā nav saskaņotas pieejas kiberdrošībai un tas rada nopietnu risku ekonomiskajai labklājībai un darījumu drošībai, un tā kā tāpēc ir vajadzīga saskaņota rīcība un ciešāka sadarbība starp valdībām, privāto sektoru, kā arī tiesībaizsardzības un izlūkošanas iestādēm;

I. tā kā kibernoziedzība ir starptautiska problēma, kas rada arvien lielākas izmaksas, un saskaņā ar ANO Narkotiku un noziedzības novēršanas biroja datiem ik gadu pasaules ekonomikai nodara teju 295 miljardu eiro lielus zaudējumus;

J. tā kā starptautiskā organizētā noziedzība izmanto tehnoloģiju attīstību un turpina novirzīt savu darbību uz kibertelpu, turklāt kibernoziedzība radikāli maina tradicionālo organizētās noziedzības grupu struktūru; tā kā tādēļ organizētā noziedzība kļūst arvien mazāk lokalizējama un labāk spējīga izmantot teritoriālās un valstu jurisdikcijas atšķirības pasaules mērogā;

K. tā kā kompetento iestāžu izmeklēšanu kibernoziedzības jomā joprojām kavē dažādi šķēršļi, tostarp virtuālo valūtu lietošana kibertelpas darījumos, kuras var izmantot nelikumīgi iegūtu līdzekļu legalizēšanai, kā arī jautājumi par teritoriālajām un jurisdikcijas robežām, nepietiekamas iespējas apmainīties ar izlūkošanas informāciju, apmācīta personāla trūkums un nekonsekventa sadarbība ar citām ieinteresētajām personām;

L. tā kā tehnoloģija ir kibertelpas attīstības pamats un nepārtraukta pielāgošanās tehnoloģiju izmaiņām ir ļoti svarīga, lai uzlabotu ES kibertelpas noturību un drošību; tā kā ir jāveic pasākumi un jānodrošina, lai tiesību akti neatpaliek no jauno tehnoloģiju attīstības, ļaujot efektīvi identificēt un saukt pie atbildības kibernoziedzniekus un aizsargāt kibernoziegumu

upurus, tā kā ES kiberdrošības stratēģijā jāiekļauj pasākumi, kas vērsti uz izpratni, izglītību, datorapdraudējumu reaģēšanas vienību (CERT) izveidi un kiberdrošības produktu un pakalpojumu iekšējā tirgus attīstīšanu, kā arī uz to, lai tiktu veicināti ieguldījumi pētniecībā, izstrādē un jauninājumos,

1. atzinīgi vērtē kopīgo paziņojumu par kiberdrošības stratēģiju un priekšlikumu direktīvai par pasākumiem, lai nodrošinātu augsta līmeņa tīklu un informācijas drošību visā Savienībā;

2. uzsver milzīgo un arvien pieaugošo nozīmi, kāda internetam un kibertelpai ir politiskās, ekonomiskās un sabiedriskās norisēs, turklāt ne tikai Savienībā, bet arī attiecībās ar citiem dalībniekiem visā pasaulē;

3. uzsver, ka ir nepieciešams izstrādāt stratēģiskās komunikācijas politiku ES kiberdrošības, kiberkrīzes situāciju, stratēģisku pārskatu, publiskā un privātā sektora sadarbības un brīdinājumu jomā, kā arī ieteikumus sabiedrībai;

4. atgādina, ka augsta līmeņa tīklu un informācijas drošība ir nepieciešama ne tikai tādēļ, lai turpinātu sniegt pakalpojumus, kas ir būtiski sabiedrības un ekonomikas raitai darbībai, bet arī lai aizsargātu iedzīvotāju fizisko integritāti, uzlabojot kritisko infrastruktūru efektivitāti un lietderīgumu un panākot to drošu darbību; uzsver – lai gan tīklu un informācijas drošības jautājumi ir jārisina, svarīgs jautājums ir arī fiziskās drošības uzlabošana; uzsver, ka infrastruktūrai vajadzētu būt noturīgai pret apzinātiem un neapzinātiem traucējumiem; šajā sakarībā uzsver, ka kiberdrošības stratēģijā vairāk vajadzētu uzsvērt netīšu sistēmas traucējumu biežākos iemeslus;

5. atkārto aicinājumu dalībvalstīm bez liekas kavēšanās pieņemt valstu kiberdrošības stratēģijas, kuras aptvertu tehniskos, koordinācijas, cilvēkresursu un finanšu sadales aspektus, un kurās būtu paredzēti skaidri noteikumi par privātā sektora ieguvumiem un pienākumiem, lai panāktu tā iesaisti, kā arī nodrošināt visaptverošas riska pārvaldības procedūras un atbilstošu normatīvo vidi;

6. atzīmē, ka tikai Savienības iestāžu un dalībvalstu kopēja vadība un politiskā atbildība ļaus panākt augsta līmeņa tīklu un informācijas drošību visā Savienībā un tādējādi veicinās drošu un netraucētu vienotā tirgus darbību;

7. uzsver, ka Savienības kiberdrošības politikai vajadzētu nodrošināt drošu un uzticamu digitālo vidi, kas pamatota ar dažādu brīvību un cieņas pret pamattiesībām aizsardzību un saglabāšanu internetā un paredzēta šo vērtību nodrošināšanai, kā noteikts ES Pamattiesību hartā un LESD 16. pantā, jo īpaši saistībā ar tiesībām uz privāto dzīvi un datu aizsardzību; uzskata, ka īpaša uzmanība jāpievērš bērnu aizsardzībai tiešsaistē;

8. aicina dalībvalstis un Komisiju veikt visus vajadzīgos pasākumus, lai kā daļu no digitālo prasmju apgūšanas jau no agrīna vecuma piedāvātu tādas apmācību programmas, kuru mērķis ir veicināt un uzlabot Eiropas iedzīvotāju izpratni, iemaņas un izglītību; atzinīgi vērtē ierosmi ar *ENISA* atbalstu un sadarbībā ar valsts iestādēm un privāto sektoru rīkot Eiropas kiberdrošības mēnesi, lai palielinātu informētību par problēmām, kas saistītas ar tīklu un informācijas sistēmu aizsardzību;

9. uzskata, ka izglītība kiberdrošības jautājumos palielina Eiropas sabiedrības informētību par kiberdraudiem, tādējādi veicinot atbildīgu kibertelpas izmantošanu, un palīdz palielināt kiberiemaņu apjomu; atzīst Eiropola un tā jaunizveidotā Eiropas Kibernoziedzības centra *(EC3)*, kā arī *ENISA* un *Eurojust* svarīgo lomu, ES līmenī nodrošinot apmācību par to, kā izmantot starptautiskās tiesiskās sadarbības instrumentus un attiecībā uz tiesībaizsardzību, kas saistīta ar dažādiem kibernoziedzības aspektiem;

10. atkārtoti uzsver nepieciešamību sniegt tehniskas konsultācijas un juridisko informāciju, kā arī izveidot programmas kibernoziedzības novēršanai un apkarošanai; mudina veikt gan kiberinženieru apmācību, kuri specializētos kritiskās infrastruktūras un informācijas sistēmu aizsardzībā, gan arī apmācīt transporta kontroles sistēmu un satiksmes vadības centru operatorus; uzsver lielo nepieciešamību ieviest regulāras kiberdrošības mācību sistēmas publiskā sektora darbiniekiem visos līmeņos;

Ceturtdiena, 2013. gada 12. septembris

11. atkārto aicinājumu rīkoties piesardzīgi, kad tiek piemēroti ierobežojumi iedzīvotāju iespējām izmantot sakaru un informācijas tehnoloģiju rīkus, un uzsver, ka dalībvalstīm būtu jācenšas nekad neapdraudēt pilsoņu tiesības un brīvības, kad tās izstrādā risinājumus saistībā ar kiberdraudiem un uzbrukumiem, un tām vajadzētu būt atbilstošiem likumdošanas līdzekļiem, lai nošķirtu civila un militāra līmeņa kibernegadījumus;

12. uzskata, ka regulatīvajai iesaistei kiberdrošības jomā vajadzētu būt orientētai uz risku, vērstai uz kritiskās infrastruktūras pienācīgas darbības nodrošināšanu, kas ir sabiedrības interesēs, un būt pamatotai ar nozarē jau pastāvošiem un tirgū balstītiem pasākumiem, lai nodrošinātu tīklu noturīgumu; uzsver, cik liela nozīme ir sadarbībai operatīvā līmenī, veicinot efektīvāku apmaiņu ar informāciju par kiberdraudiem starp valsts iestādēm un privāto sektoru, turklāt gan Savienības, gan valstu līmenī, kā arī ar Savienības stratēģiskajiem partneriem, lai tādējādi panāktu tīklu un informācijas drošību, radot savstarpēju uzticību, veidojot kopējas vērtības un iesaistīšanos un apmainītos ar pieredzi; uzskata, ka publiskā un privātā sektora partnerības pamatā vajadzētu būt tīklu un tehnoloģiskajai neitralitātei un galvenā uzmanība būtu jāpievērš centieniem risināt problēmas, kam ir liela sabiedriska ietekme; aicina Komisiju mudināt visus iesaistītos tirgus dalībniekus būt modrākiem un gatavākiem sadarbībai, lai aizsargātu citus uzņēmējus no kaitējuma viņu pakalpojumiem;

13. atzīst, ka kiberdrošības negadījumu atklāšana un paziņošana par tiem ir ļoti svarīga, lai Savienībā veicinātu kibernoturību; uzskata, ka būtu jāievieš samērīgas un nepieciešamas informācijas atklāšanas prasības, lai kompetentajām valsts iestādēm tiktu paziņots par negadījumiem, kas saistīti ar būtiskiem drošības pārkāpumiem, un tādējādi varētu uzlabot kibernoziedzības uzraudzību un veicināt centienus palielināt informētību visos līmeņos;

14. mudina Komisiju un citus dalībniekus ieviest kiberdrošības un kibernoturības politiku, kas paredzētu ekonomiskus stimulus, lai veicinātu augsta līmeņa kiberdrošību un kibernoturību;

Kibernoturība

15. atzīmē, ka dažādām nozarēm un dalībvalstīm ir atšķirīga līmeņa spējas un prasmes, un tas kavē uzticamu sadarbību un traucē vienotā tirgus darbību;

16. uzskata, ka prasībās attiecībā uz mazajiem un vidējiem uzņēmumiem būtu jāievēro samērīga un uz risku balstīta pieeja;

17. prasa nostiprināt kritiskās infrastruktūras kibernoturību un atgādina, ka turpmākajās vienošanās attiecībā uz solidaritātes klauzulas (LESD 222. pants) īstenošanu būtu jāņem vērā kiberuzbrukuma risks kādai dalībvalstij; aicina Komisiju un augsto pārstāvi ņemt vērā šo risku to kopīgajos integrēto draudu un riska novērtējuma ziņojumos, kas tiks sagatavoti, sākot no 2015. gada;

18. uzsver, ka jo īpaši kritisko pakalpojumu datu integritātes, pieejamības un konfidencialitātes nodrošināšanai būtu jāpanāk, ka tiek atjaunināta kritiskās infrastruktūras identifikācija un klasifikācija, un jānosaka arī nepieciešamās obligātās drošības prasības to tīklu un informācijas sistēmām;

19. atzīst, ka priekšlikumā direktīvai par pasākumiem, kas nodrošinātu vienādi augsta līmeņa tīklu un informācijas drošību visā Savienībā, ir paredzētas šādas obligātās drošības prasības informācijas sabiedrības pakalpojumu sniedzējiem un kritiskās infrastruktūras operatoriem;

20. aicina dalībvalstis un Savienību radīt atbilstošu pamatu ātru divvirzienu informācijas apmaiņas sistēmu izveidei, kas garantētu anonimitāti privātajam sektoram, bet pastāvīgi nodrošinātu jaunāko informāciju publiskajam sektoram un, vajadzības gadījumā, sniegtu privātajam sektoram palīdzību;

21. atzinīgi vērtē Komisijas vēlmi veidot riska pārvaldības kultūru attiecībā uz kiberdrošību un mudina dalībvalstis un Savienības iestādes nekavējoties iekļaut kiberkrīžu pārvaldību savos krīžu pārvaldības un riska novērtējuma plānos; turklāt aicina dalībvalstu valdības un Komisiju mudināt privātā sektora dalībniekus iekļaut kiberkrīžu pārvaldību savos pārvaldības un riska novērtējuma plānos un apmācīt savus darbiniekus kiberdrošības jautājumos;

22. aicina visas dalībvalstis un Savienības iestādes izveidot labi strādājošu datorapdraudējumu reaģēšanas vienību *(CERT)* tīklu, kas darbotos nepārtraukti; norāda, ka valstu *CERT* vajadzētu būt daļai no efektīva tīkla, kurā notiek svarīgas informācijas apmaiņa, ievērojot nepieciešamos uzticēšanās un konfidencialitātes standartus; norāda, ka iniciatīvas, kuru mērķis ir apvienot *CERT* un citas attiecīgās drošības iestādes, var kļūt par noderīgu instrumentu, lai attīstītu uzticēšanos pārrobežu un starpnozaru kontekstā; norāda uz to, cik svarīga cīņā pret kibernoziedzību ir efektīva un rezultatīva sadarbība starp *CERT* un tiesībaizsardzības iestādēm;

23. atbalsta *ENISA*, tai īstenojot savus pienākumus saistībā ar tīklu un informācijas drošību, jo īpaši sniedzot konsultācijas un padomus dalībvalstīm, kā arī atbalstot labākās prakses apmaiņu un veidojot uzticēšanās gaisotni;

24. uzsver, ka nozarei ir jāīsteno atbilstošas kiberdrošības nodrošināšanas prasības visā to IKT produktu vērtību ķēdē, ko izmanto transporta tīklos un informācijas sistēmās, lai veiktu atbilstošu riska pārvaldību, pieņemtu drošības standartus un risinājumus, kā arī lai izstrādātu paraugpraksi un veiktu informācijas apmaiņu ar mērķi panākt, ka transporta sistēmas ir drošas pret kibernoziegumiem;

Rūpniecības un tehnoloģiskie resursi

25. uzskata, ka augsta līmeņa tīklu un informācijas drošības nodrošināšanai ir svarīga nozīme, lai palielinātu gan drošības risinājumu piegādātāju, gan lietotāju konkurētspēju Savienībā; uzskata – kaut arī IT drošības nozarei Savienībā ir nozīmīgs neizmantots potenciāls, tomēr gan privātā, gan valsts un uzņēmējdarbības sektora lietotāji nereti nav pienācīgi informēti par izmaksām un ieguvumiem no ieguldījumiem kiberdrošībā un tādējādi joprojām ir neaizsargāti pret kaitīgiem kiberdraudiem; uzsver, ka *CERT* ieviešana ir nozīmīgs faktors šajā sakarībā;

26. uzskata, ka kiberdrošības risinājumu stabilam piedāvājumam un pieprasījumam nepieciešami IKT jomā iesaistīto valsts iestāžu veikti atbilstoši ieguldījumi akadēmiskos resursos, pētniecībā un izstrādē, kā arī zināšanu un spēju attīstīšanā, lai veicinātu jauninājumus un radītu pietiekamu izpratni par tīklu un informācijas drošības riskiem, kā rezultātā veidotos vienota Eiropas drošības nozare;

27. aicina Savienības iestādes un dalībvalstis veikt nepieciešamos pasākumus, lai izveidotu kiberdrošības vienoto tirgu, kurā lietotāji un piegādātāji vislabāk varētu izmantot jauninājumus un sinerģiju un apvienot pieredzi par piedāvājumiem, un kuram varētu pievienoties arī MVU;

28. mudina dalībvalstis apsvērt iespēju veikt kopīgus ieguldījumus Eiropas kiberdrošības nozarē, līdzīgi kā tas tiek darīts citās jomās, piemēram, aviācijas nozarē;

Kibernoziedzība

29. uzskata, ka noziedzīgās darbības kibertelpā var būt tikpat kaitīgas sabiedrībās labklājībai kā nodarījumi fiziskajā pasaulē, un ka šīs noziedzības formas bieži pastiprina viena otru, kā to var novērot, piemēram, saistībā ar bērnu seksuālu izmantošanu, organizēto noziedzību un nelikumīgi iegūtu līdzekļu legalizēšanu;

30. atzīmē, ka dažos gadījumos pastāv saikne starp likumīgu un nelikumīgu saimniecisko darbību; uzsver interneta veicināto saikni starp terorisma finansēšanu un smagu organizēto noziedzību; uzsver, ka sabiedrība ir jāinformē par to, cik nopietnas sekas var būt iesaistei kibernoziegumos, un par iespēju, ka tas, kas pirmajā mirklī var šķist sociāli pieņemams nodarījums, piemēram, nelegāla filmu lejupielāde, nereti nodrošina lielus ienākumus starptautiskiem noziedzīgiem sindikātiem;

Ceturtdiena, 2013. gada 12. septembris

31. piekrīt Komisijai, ka tās pašas normas un principus, kas darbojas bezsaistes jomā, jāpiemēro arī tiešsaistē, un tāpēc cīņa pret kibernoziegumiem jāpastiprina ar atjauninātiem tiesību aktiem un operatīvajām iespējām;

32. uzskata – ņemot vērā kibernoziegumu pārrobežu raksturu īpaši svarīgs ir Savienības līmenī kopīgi paveiktais un piedāvātā ekspertīze, kas pārsniedz atsevišķu dalībvalstu līmeni, un ka *Eurojust*, Eiropola *EC3*, *CERT* un augstskolu un pētniecības centri ir jānodrošina ar atbilstīgiem resursiem un iespējām, lai tie pienācīgi darbotos kā zināšanu, sadarbības un informācijas apmaiņas mezglu punkti;

33. ļoti atzinīgi vērtē *EC3* izveidi un mudina turpināt attīstīt šo aģentūru un tās nozīmīgo lomu, koordinējot savlaicīgu un efektīvu informācijas un zināšanu pārrobežu apmaiņu, lai atbalstītu centienus novērst, atklāt un izmeklēt kibernoziegumus;

34. aicina dalībvalstis nodrošināt, ka iedzīvotāji var viegli piekļūt informācijai par kiberdraudiem un par to, kā pret tiem cīnīties; uzskata, ka šādās norādēs būtu jāiekļauj informācija par to, kā lietotāji var aizsargāt savu privāto dzīvi internetā, kā atklāt iedraudzināšanu tiešsaistē un ziņot par to, kā instalēt programmatūru un ugunsmūrus, kā pārvaldīt paroles un kā atklāt viltus prasības sevi identificēt *(phishing)*, ievilināšanu *(pharming)* un citus uzbrukumu veidus;

35. uzstāj, ka tām dalībvalstīm, kas vēl nav ratificējušas Eiropas Padomes Budapeštas konvenciju par kibernoziegumiem, tas jādara bez turpmākas kavēšanās; atzinīgi vērtē Eiropas Padomes viedokli par nepieciešamību atjaunināt konvenciju, ņemot vērā tehnoloģiju attīstību, lai nodrošinātu tās pastāvīgu efektivitāti kibernoziegumu novēršanā, un aicina Komisiju un dalībvalstis piedalīties šajās diskusijās; atbalsta centienus panākt, lai konvenciju ratificē arī citas valstis, un aicina Komisiju to veicināt arī ārpus Savienības;

Kiberaizsardzība

36. uzsver, ka kiberproblēmas, kiberdraudi un kiberuzbrukumi apdraud dalībvalstu aizsardzības un valsts drošības intereses, un ka gan ar civilo, gan militāro pieeju kritiskās infrastruktūras aizsardzības uzdevumam un centieniem panākt sinerģiju vajadzētu palielināt ieguvumus abām pusēm;

37. tāpēc aicina dalībvalstis pastiprināt sadarbību ar Eiropas Aizsardzības aģentūru *(EDA)*, lai izstrādātu priekšlikumus un iniciatīvas kiberaizsardzības spēju nostiprināšanai, pamatojoties uz jaunākajām ierosmēm un projektiem; uzsver nepieciešamību uzlabot pētniecību un izstrādi, tostarp apvienojot un kopīgi izmantojot resursus;

38. atkārtoti uzsver, ka visaptverošā ES kiberdrošības stratēģijā būtu jāņem vērā esošo aģentūru un organizāciju sniegtā pievienoto vērtība, kā arī labā prakse no tām dalībvalstīm, kuras jau ir ieviesušas valsts kiberdrošības stratēģijas;

39. aicina Komisijas priekšsēdētāja vietnieci/Savienības augsto pārstāvi ārlietās un drošības politikas jautājumos iekļaut kiberkrīžu pārvaldību krīžu pārvaldības plānošanā un uzsver, ka dalībvalstīm kopā ar *EDA* jāizstrādā plāni par KDAP misiju un operāciju aizsardzību pret kiberuzbrukumiem; aicina tās kopīgi veidot Eiropas aizsardzības spēkus cīņai pret kibernoziegumiem;

40. uzsver veiksmīgo praktisko sadarbību ar NATO kiberdrošības jomā un nepieciešamību pastiprināt šo sadarbību, jo īpaši izmantojot ciešāku koordināciju plānošanas, tehnoloģiju, apmācības un aprīkojuma jomā;

41. prasa Savienībai aktīvāk iesaistīties apmaiņā ar starptautiskajiem partneriem, tostarp NATO, un noteikt sadarbības jomas, lai, ja vien iespējams, izvairītos no dublēšanās un savstarpēji papildinātu veicamās darbības;

Starptautiskā politika

42. uzskata, ka starptautiskā sadarbība un dialogs ir svarīgi, veidojot uzticību un pārredzamību, kā arī veicinot augsta līmeņa tīklu veidošanu un informācijas apmaiņu pasaules mērogā; tāpēc aicina Komisiju un Eiropas Ārējās darbības dienestu izveidot kiberdiplomātijas grupu, kura būtu atbildīga par dialoga veicināšanu ar līdzīgi domājošām valstīm un organizācijām; aicina Savienību aktīvāk iesaistīties dažādās starptautiskās augsta līmeņa konferencēs par kiberdrošību;

43. uzskata, ka jāpanāk līdzsvars starp pārrobežu datu pārsūtīšanas, datu aizsardzības un kiberdrošības savstarpēji konkurējošiem mērķiem, ievērojot Savienības starptautiskās saistības, jo īpaši saskaņā ar *GATS*;

44. aicina Komisijas priekšsēdētāja vietnieci/Savienības augsto pārstāvi ārlietās un drošības politikas jautājumos iekļaut kiberdrošības jautājumus ES ārējās darbībās, it īpaši attiecībās ar trešām valstīm, lai pastiprinātu sadarbību un pieredzes un informācijas apmaiņu par to, kā panākt kiberdrošību;

45. prasa Savienībai aktīvāk iesaistīties apmaiņā ar starptautiskajiem partneriem, lai noteiktu sadarbības jomas un, ja vien iespējams, izvairītos no dublēšanās un savstarpēji papildinātu veicamās darbības; aicina Komisijas priekšsēdētāja vietnieci/Savienības augsto pārstāvi ārlietās un drošības politikas jautājumos aktīvi rīkoties starptautiskajās organizācijās un koordinēt dalībvalstu pozīcijas par to, kā efektīvi veicināt risinājumus un politiku kiberjomā;

46. uzskata, ka būtu jācenšas panākt, lai kibertelpā tiktu piemēroti jau spēkā esošie starptautiskie juridiskie instrumenti, jo īpaši Eiropas Padomes Konvencija par kibernoziegumiem; tāpēc uzskata, ka pašlaik nav nepieciešams izveidot jaunu juridisko instrumentu starptautiskā līmenī; tomēr atzinīgi vērtē starptautisko sadarbību, lai izstrādātu uzvedības normas kibertelpā, atbalstot tiesiskuma nostiprināšanos tajā; uzskata, ka būtu jāapsver spēkā esošo juridisko instrumentu aktualizēšana, lai ņemtu vērā sasniegumus tehnoloģiju jomā; uzskata, ka saistībā ar jurisdikcijas jautājumiem nepieciešama rūpīga diskusija par tiesu iestāžu sadarbību un kriminālvajāšanu pārrobežu krimināllietās;

47. uzskata, ka jo īpaši ES un ASV darba grupa kiberdrošības un kibernoziedzības jautājumos būtu jāizmanto kā instruments, lai ES un ASV nepieciešamības gadījumā varētu apmainīties ar labāko praksi kiberdrošības politikas jomā; šajā sakarībā atzīmē, ka ar kiberdrošību saistītas jomas, piemēram, pakalpojumi, kas atkarīgi no tīklu un informācijas sistēmu drošas darbības, tiks iekļautas gaidāmajās sarunās par transatlantisko tirdzniecības un ieguldījumu partnerību, kurš jānoslēdz tā, lai aizsargātu ES suverenitāti un tās iestāžu neatkarību;

48. atzīmē, ka kiberdrošības prasmes un spējas novērst, atklāt un efektīvi cīnīties ar draudiem un ļaunprātīgiem uzbrukumiem nav vienmērīgi izplatītas visā pasaulē; uzsver, ka centienus palielināt kibernoturību un cīnīties ar kiberdraudiem nedrīkst izprast tikai kā sadarbību ar līdzīgi domājošiem partneriem, bet būtu arī jāiesaista reģioni ar mazāk attīstītām spējām, tehnisko infrastruktūru un tiesisko regulējumu; uzskata, ka šajā jautājumā izšķiroši svarīga ir *CERT* koordinēšana; aicina Komisiju veicināt trešo valstu centienus ar atbilstošiem līdzekļiem veidot pašām savas kiberdrošības spējas un, ja nepieciešams, palīdzēt šajā procesā;

Īstenošana

49. prasa augstākajā politiskajā līmenī regulāri novērtēt valstu kiberdrošības stratēģiju efektivitāti, lai pielāgotos jaunajiem globālajiem draudiem un garantētu līdzvērtīgu kiberdrošības līmeni dažādās dalībvalstīs;

50. prasa Komisijai izstrādāt precīzu plānu, kurā būtu noteikti termiņi attiecībā uz Savienības līmenī sasniedzamiem mērķiem saskaņā ar kiberdrošības stratēģiju, kā arī to novērtējumu; aicina dalībvalstis vienoties par līdzīgu valsts pasākumu īstenošanas plānu saskaņā ar šo stratēģiju;

Ceturtdiena, 2013. gada 12. septembris

51. prasa, lai Komisija, dalībvalstis, Eiropols un jaunizveidotā *EC3*, kā arī *Eurojust* un *ENISA* iesniegtu regulārus ziņojumus, kuros novērtētu kiberdrošības stratēģijā noteikto mērķu īstenošanā, norādot galvenos darbības rādītājus, ar kuriem noteikt panākumus īstenošanā;

o

o o

52. uzdod priekšsēdētājam nosūtīt šo rezolūciju Padomei, Komisijai, dalībvalstu valdībām un parlamentiem, Eiropolam, *Eurojust* un Eiropas Padomei.

P7_TA(2013)0377

Digitalizācijas programma izaugsmei, mobilitātei un nodarbinātībai

Eiropas Parlamenta 2013. gada 12. septembra rezolūcija par digitalizācijas programmu izaugsmei, mobilitātei un nodarbinātībai – laiks palielināt apgriezienus (2013/2593(RSP))

(2016/C 093/17)

Eiropas Parlaments,

— ņemot vērā Komisijas 2012. gada 18. decembra paziņojumu "Eiropas digitalizācijas programma – digitalizācijas virzīta Eiropas izaugsme" (COM(2012)0784),

— ņemot vērā jautājumus Komisijai un Padomei par digitalizācijas programmu izaugsmei, mobilitātei un nodarbinātībai – laiks palielināt apgriezienus (O-000085 – B7-0219/2013 un O-000086 – B7-0220/2013),

— ņemot vērā Eiropas Parlamenta un Padomes 2012. gada 13. jūnija Regulu (ES) Nr. 531/2012 par viesabonēšanu publiskajos mobilo sakaru tīklos Savienībā ([1]),

— ņemot vērā Eiropas Parlamenta un Padomes 2012. gada 14. marta Lēmumu Nr. 243/2012/ES, ar ko izveido radiofrekvenču spektra daudzgadu politikas programmu ([2]),

— ņemot vērā to, ka joprojām tiek apspriests Eiropas infrastruktūras savienošanas instruments, un jo īpaši ņemot vērā grozīto priekšlikumu Eiropas Parlamenta un Padomes regulai par vadlīnijām Eiropas telekomunikāciju tīkliem un ar ko atceļ Lēmumu Nr. 1336/97/EK (COM(2013)0329),

— ņemot vērā 2010. gada 5. maija rezolūciju par jaunu Eiropas digitālo programmu – 2015.eu ([3]),

— ņemot vērā Komisijas 2012. gada 27. septembra paziņojumu "Mākoņdatošanas potenciāla atraisīšana Eiropā" (COM (2012)0529),

— ņemot vērā 2012. gada 25. janvāra priekšlikumu Eiropas Parlamenta un Padomes regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula) (COM (2012)0011),

---

([1]) OV L 172, 30.6.2012., 10. lpp.
([2]) OV L 81, 21.3.2012., 7. lpp.
([3]) OV C 81 E, 15.3.2011., 45. lpp.