2013 m. rugsėjo 12 d., ketvirtadienis

4. prašo Komisijos remti valstybių narių pastangas vyrų ir moterų darbo užmokesčio skirtumą kasmet sumažinti bent 5 procentiniais punktais, siekiant tikslo iki 2020 m. šį skirtumą visiškai panaikinti;

5. pripažįsta, jog norint vadovautis kelis lygmenis apimančiu ir daugialypiu požiūriu būtina, kad Komisija remtų valstybių narių pastangas skatinti gerąją patirtį ir įgyvendinti politiką, skirta vyrų ir moterų darbo užmokesčio skirtumui panaikinti;

6. ragina Komisiją nedelsiant atlikti Direktyvos 2006/54/EB peržiūrą ir, remiantis šios direktyvos 32 straipsniu bei SESV 157 straipsniu, pasiūlyti jos pakeitimus atsižvelgiant į išsamias Europos Parlamento 2012 m. gegužės 24 d. rezoliucijos priede pateiktas rekomendacijas;

7. paveda Pirmininkui perduoti šią rezoliuciją Tarybai, Komisijai ir valstybių narių vyriausybėms.

P7_TA(2013)0376

ES kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė

2013 m. rugsėjo 12 d. Europos Parlamento rezoliucija „Europos Sąjungos kibernetinio saugumo strategija: atvira, saugi ir patikima kibernetinė erdvė“ (2013/2606(RSP))

(2016/C 093/16)

Europos Parlamentas,

— atsižvelgdamas į 2013 m. vasario 7 d. Europos Komisijos ir Europos Sąjungos vyriausiosios įgaliotinės užsienio reikalams ir saugumo politikai bendrą komunikatą „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“ (JOIN(2013)0001),

— atsižvelgdamas į 2013 m. vasario 7 d. Komisijos pasiūlymą dėl direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (COM(2013)0048),

— atsižvelgdamas į 2010 m. gegužės 19 d. Komisijos komunikatą „Europos skaitmeninė darbotvarkė“ (COM(2010)0245) ir į 2012 m. gruodžio 18 d. Komisijos komunikatą „Europos skaitmeninė darbotvarkė. Skaitmeninėmis technologijomis grindžiamas Europos augimas“ (COM(2012)0784),

— atsižvelgdamas į 2012 m. rugsėjo 27 d. Komisijos komunikatą „Nuotolinės kompiuterijos galimybių naudojimas Europoje“ (COM(2012)0529),

— atsižvelgdamas į 2012 m. kovo 28 d. Komisijos komunikatą „Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas“ (COM(2012)0140) ir į su tuo susijusias 2012 m. birželio 7 d. Tarybos išvadas,

— atsižvelgdamas į 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyvą 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR ([1]),

— 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 ([2]),

---

([1]) OL L 218, 2013 8 14, p. 8.
([2]) OL L 345, 2008 12 23, p. 75.

— atsižvelgdamas į 2011 m. gruodžio 13 d. Europos Parlamento ir Tarybos direktyvą 2011/92/ES dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija, kuria pakeičiamas Tarybos pamatinis sprendimas 2004/68/TVR ([1]),

— atsižvelgdamas į programą dėl laisvės, saugumo ir teisingumo erdvės (Stokholmo programa) ([2]), į Komisijos komunikatą „Sukurti laisvės, saugumo ir teisingumo erdvę Europos piliečiams. Stokholmo programos įgyvendinimo veiksmų planas“ (COM(2010)0171) ir į Komisijos komunikatą „ES vidaus saugumo strategijos įgyvendinimas. Penki žingsniai kuriant saugesnę Europą“ (COM(2010)0673), taip pat į savo 2012 m. gegužės 22 d. rezoliuciją dėl Europos Sąjungos vidaus saugumo strategijos ([3]),

— atsižvelgdamas į Komisijos ir Vyriausiosios įgaliotinės bendrą pasiūlymą dėl Tarybos sprendimo dėl tvarkos, kuria Sąjunga įgyvendina solidarumo sąlygą (JOIN(2012)0039),

— atsižvelgdamas į 2001 m. gegužės 28 d. Tarybos pamatinį sprendimą 2001/413/TVR, skirtą kovai su sukčiavimu negrynosiomis mokėjimo priemonėmis ir jų klastojimu ([4]),

— atsižvelgdamas į savo 2012 m. birželio 12 d. rezoliuciją dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“ ([5]) ir į Tarybos 2011 m. gegužės 27 d. išvadas dėl Komisijos komunikato dėl ypatingos svarbos informacinės infrastruktūros apsaugos „Visuotinio kibernetinio saugumo užtikrinimas. Laimėjimai ir tolesni veiksmai“ (COM(2011)0163),

— atsižvelgdamas į savo 2012 m. gruodžio 11 d. rezoliuciją dėl bendrosios skaitmeninės rinkos kūrimo užbaigimo ([6]),

— atsižvelgdamas į savo 2012 m. lapkričio 22 d. rezoliuciją dėl kibernetinio saugumo ir gynybos ([7]),

— atsižvelgdamas į savo pozicija priimtą 2013 m. balandžio 16 d. per pirmąjį svarstymą dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento dėl Europos tinklų ir informacijos apsaugos agentūros (ENISA) (COM(2010)0521) ([8]),

— atsižvelgdamas į savo 2012 m. gruodžio 11 d. rezoliuciją dėl skaitmeninės laisvės strategijos ES užsienio politikoje ([9]),

— atsižvelgdamas į 2001 m. lapkričio 23 d. Europos Tarybos konvenciją dėl elektroninių nusikaltimų,

— atsižvelgdamas į Sąjungos tarptautinius įsipareigojimus, ypač pagal Bendrąjį susitarimą dėl prekybos paslaugomis (GATS),

— atsižvelgdamas į Sutarties dėl Europos Sąjungos veikimo (SESV) 16 straipsnį ir į Europos Sąjungos pagrindinių teisių chartiją, ypač į jos 6, 8 ir 11 straipsnius,

— atsižvelgdamas į vykstančias Europos Sąjungos ir Jungtinių Amerikos Valstijų derybas dėl Tarpatlantinės prekybos ir investicijų partnerystės (TPIP),

— atsižvelgdamas į Darbo tvarkos taisyklių 110 straipsnio 2 dalį,

A. kadangi didėjantys kibernetiniai iššūkiai, įgaunantys sudėtingų grėsmių ir išpuolių formą, yra didelė grėsmė valstybių narių, taip pat privataus sektoriaus ir platesnės bendruomenės saugumui, stabilumui ir ekonominei gerovei; kadangi dėl šios priežasties mūsų visuomenės apsauga ir ekonomika bus nuolat kintanti užduotis;

([1]) OL L 335, 2011 12 17, p. 1.
([2]) OL C 115, 2010 5 4, p. 1.
([3]) Priimti tekstai, P7_TA(2012)0207.
([4]) OL L 149, 2001 6 2, p. 1.
([5]) Priimti tekstai, P7_TA(2012)0237.
([6]) Priimti tekstai, P7_TA(2012)0468.
([7]) Priimti tekstai, P7_TA(2012)0457.
([8]) Priimti tekstai, P7_TA(2013)0103.
([9]) Priimti tekstai, P7_TA(2012)0470.

2013 m. rugsėjo 12 d., ketvirtadienis

B. kadangi kibernetinė erdvė ir kibernetinė sauga turėtų būti vienas iš ES ir kiekvienos valstybės narės saugumo ir gynybos politikos strateginių ramsčių; kadangi labai svarbu užtikrinti, kad kibernetinė erdvė išliktų atvira laisvam idėjų, informacijos ir saviraiškos srautui;

C. kadangi elektroninė prekyba ir internetinės paslaugos labai svarbios interneto gyvavimui ir yra būtinos įgyvendinant strategijos „Europa 2020“ tikslus siekiant naudos piliečiams ir privačiajam sektoriui; kadangi Sąjunga turi visapusiškai išnaudoti interneto siūlomą potencialą ir galimybes tolesnio bendrosios rinkos vystymo srityje, įskaitant skaitmeninę rinką;

D. kadangi Bendrame komunikate dėl Europos Sąjungos kibernetinio saugumo strategijos nustatyti prioritetai apima kibernetinį atsparumą, elektroninių nusikaltimų skaičiaus mažinimą, kibernetinės gynybos politikos ir pajėgumų, susijusių su bendra saugumo ir gynybos politika (BSGP), sukūrimą, taip pat nuoseklios tarptautinės Europos Sąjungos kibernetinės erdvės politikos sukūrimą;

E. kadangi visoje Sąjungoje tinklų ir informacinės sistemos yra labai susijusios; kadangi, atsižvelgiant į pasaulinį interneto pobūdį, daugelis tinklų ir informacijos saugumo incidentų peržengia valstybių sienas ir gali trukdyti veikti vidaus rinkai ir kenkti vartotojų pasitikėjimui skaitmenine bendrąja rinka;

F. kadangi visoje Sąjungoje, kaip ir pasaulyje, kibernetinis saugumas yra tik tiek stiprus, kiek stiprus jo silpniausias saitas, ir sutrikimai viename sektoriuje ar valstybėje narėje turi pasekmių kitam sektoriui ar valstybei narei, darydami pašalinį poveikį visai Sąjungos ekonomikai;

G. kadangi nuo 2013 m. balandžio mėn. tik 13 valstybių narių oficialiai priėmė nacionalines kibernetinio saugumo strategijas; kadangi tarp valstybių narių yra esminių skirtumų jų pasirengimo, saugumo, strateginės kultūros ir gebėjimų kurti ir įgyvendinti nacionalines kibernetinio saugumo strategijas srityje, taip pat kadangi reikėtų atlikti šių skirtumų vertinimą;

H. kadangi dėl saugumo kultūrų skirtumų ir teisinės sistemos trūkumo atsiranda susiskaldymas ir skaitmeninėje bendrojoje rinkoje jomis reikia rūpintis pirmiausia; kadangi trūksta suderinto požiūrio į kibernetinį saugumą ir dėl to kyla dideli pavojai ekonomikos gerovei ir sandorių saugumui, taip pat kadangi dėl to reikalingos vyriausybių, privačiojo sektoriaus, teisėsaugos ir žvalgybos tarnybų suderintos pastangos ir glaudesnis bendradarbiavimas;

I. kadangi elektroniniai nusikaltimai yra vis brangesnė tarptautinė problema, šiuo metu pasaulio ekonomikai, anot Jungtinių Tautų narkotikų kontrolės ir nusikalstamumo prevencijos biuro, kainuojanti 295 mlrd. EUR per metus;

J. kadangi tarptautinis organizuotas nusikalstamumas, naudodamasis technologine pažanga, toliau savo veiklą perkelia į kibernetinę erdvę, kurioje elektroniniai nusikaltimai radikaliai keičia tradicinę organizuotų nusikalstamų grupių struktūrą; kadangi dėl to organizuotas nusikalstamumas yra mažiau lokalizuotas ir nusikaltėliai gali pasaulio lygiu išnaudoti skirtingas teisės sistemas ir skirtingas nacionalinės teisės jurisdikcijas;

K. kadangi kompetentingoms valdžios institucijoms tirti elektroninius nusikaltimus vis dar trukdo kelios kliūtys, pvz., vadinamosios virtualiosios valiutos naudojimas sudarant sandorius kibernetinėje erdvėje – tai gali būti naudojama pinigų plovimui, problemos, susijusios su teritoriškumu ir jurisdikcijų ribomis, nepakankami dalijimosi žvalgybos informacija pajėgumai, išmokytų darbuotojų stoka ir nenuoseklus bendradarbiavimas su kitais suinteresuotaisiais asmenimis;

L. kadangi technologija yra kibernetinės erdvės pagrindas ir nuolatinis prisitaikymas prie technologinių pokyčių turi esminę svarbą, jei norima pagerinti ES kibernetinės erdvės atsparumą ir saugą; kadangi reikia imtis priemonių siekiant užtikrinti, kad teisės aktai būtų pritaikyti prie naujų technologinių pokyčių, kad būtų galima nustatyti ir persekioti elektroninius nusikaltėlius ir apsaugoti elektroninių nusikaltimų aukas; kadangi ES kibernetinio saugumo strategija turi

apimti priemones, skirtas informuotumui, švietimui, kompiuterinių incidentų tyrimo tarnyboms (CERT) plėtoti, kibernetinio saugumo produktams ir paslaugų vidaus rinkai kurti ir investicijoms į mokslinius tyrimus, plėtrą ir inovacijas skatinti;

1. palankiai vertina Bendrą komunikatą dėl Europos Sąjungos kibernetinio saugumo strategijos ir pasiūlymą dėl direktyvos dėl priemonių, skirtų aukšto lygio tinklo ir informacijos saugumui visoje Sąjungoje užtikrinti;

2. pabrėžia pirmaeilę ir vis didėjančią interneto ir kibernetinės erdvės svarbą politiniams, ekonominiams ir visuomeniniams sandoriams, ne tik Sąjungoje, bet ir kitų veikėjų visame pasaulyje atžvilgiu;

3. pabrėžia, kad būtina išplėtoti strateginę komunikacijos politiką ES kibernetinio saugumo, kibernetinių krizių situacijų, strategijų peržiūrų, viešojo ir privačiojo sektoriaus bendradarbiavimo ir įspėjimų, taip pat rekomendacijų visuomenei klausimais;

4. primena, kad aukšto lygio tinklų ir informacijos apsauga reikalinga ne tik tam, kad būtų išlaikytos sklandžiai visuomenės ir ekonomikos veiklai būtinos paslaugos, bet ir tam, kad būtų išsaugota fizinė piliečių neliečiamybė stiprinant itin svarbių infrastruktūrų efektyvumą, veiksmingumą ir saugią veiklą; pabrėžia, kad nors turi būti sprendžiama tinklų ir informacijos saugumo problema, fizinio saugumo gerinimas taip pat yra svarbus klausimas; pabrėžia, kad infrastruktūra turėtų būti atspari ir tyčiniams, ir netyčiniams sutrikimams; pabrėžia, kad siekiant šio tikslo kibernetinio saugumo strategijoje daugiau dėmesio turėtų būti skiriama bendroms sistemų netyčinių gedimų priežastims;

5. pakartoja savo raginimą valstybėms narėms priimti nacionalines kibernetinio saugumo strategijas, kurios apimtų techninius, koordinavimo, žmogiškųjų išteklių ir finansavimo skyrimo aspektus ir kurios taip pat apimtų atskiras taisykles dėl privačiojo sektoriaus naudos ir atsakomybės, siekiant užtikrinti jo nedelsiamą dalyvavimą ir numatyti išsamias rizikos valdymo procedūras bei išsaugoti reguliavimo aplinką;

6. pažymi, kad tik Sąjungos institucijų ir valstybių narių vadovavimas ir politinė atsakomybė sudarys sąlygas užtikrinti tinklų ir informacijos aukšto lygio saugumą visoje Sąjungoje ir taip padės užtikrinti saugų ir sklandų bendrosios rinkos veikimą;

7. pabrėžia, kad Sąjungos kibernetinio saugumo politika turėtų suteikti saugią ir patikimą skaitmeninę aplinką, pagrįstą laisvių apsauga ir išsaugojimu, taip pat pagarba pagrindinėms teisėms, kaip numatyta ES chartijoje ir SESV 16 straipsnyje, ypač teisėms į privatų gyvenimą ir duomenų apsaugą, taip pat būti skirta šioms teisėms užtikrinti; mano, kad ypatingą dėmesį reikėtų skirti vaikų apsaugai internete;

8. ragina valstybes nares ir Komisiją imtis visų reikalingų veiksmų, kad būtų pasiūlytos mokymo programos, skirtos Europos piliečių informuotumui, įgūdžiams ir švietimui skatinti ir gerinti, ypač nuo pat ankstyvo amžiaus atsižvelgiant į asmeninį saugumą, kaip į skaitmeninio raštingumo programos dalį; palankiai vertina iniciatyvą surengti Europos kibernetinio saugumo mėnesį, remiant agentūrai ENISA ir bendradarbiaujant su viešojo sektoriaus institucijomis ir privačiuoju sektoriumi, siekiant didinti informuotumą apie iššūkius, susijusius su tinklų ir informacinių sistemų apsauga;

9. mano, kad švietimas kibernetinio saugumo klausimais didina Europos visuomenės informuotumą apie kibernetines grėsmes ir taip skatina atsakingai naudotis kibernetine erdve, taip pat padeda didinti kibernetinius įgūdžius; pripažįsta, kad Europolas ir jo naujasis Europos kovos su elektroniniu nusikalstamumu centras (EC3), taip pat ENISA ir Eurojust atlieka labai svarbų vaidmenį ES lygmeniu teikdami mokymus, kaip naudotis tarptautinio teisminio bendradarbiavimo priemonėmis ir užtikrinti teisėsaugą įvairiais elektroninių nusikaltimų aspektais;

10. primena, kad reikia teikti techninius patarimus ir teisinę informaciją, taip pat kurti programas, skirtas elektroninių nusikaltimų prevencijai ir kovai su jais; ragina mokyti kibernetikos inžinierius, kurių specializacija – ypatingos svarbos infrastruktūros ir informacinių sistemų apsauga, taip pat transporto kontrolės sistemų ir eismo valdymo centrų operatorius; pabrėžia žūtbūtinį poreikį įdiegti visų lygių viešojo sektoriaus darbuotojams skirto reguliaraus mokymo kibernetinio saugumo klausimais sistemas;

2013 m. rugsėjo 12 d., ketvirtadienis

11. pakartoja savo raginimą atsargiai taikyti apribojimus, taikomus piliečių galėjimui naudotis komunikacijos ir informacijos technologijų priemonėmis, ir pabrėžia, kad valstybės narės, reaguodamos į kibernetinės grėsmes ir išpuolius, turėtų siekti niekada nekelti grėsmės piliečių teisėms ir laisvėms, ir turėtų turėti tinkamas teisėkūros priemones, kad galėtų atskirti civilio ir karinio lygių kibernetinius incidentus;

12. mano, kad reguliuojamasis kišimasis į kibernetinio saugumo erdvę turėtų būti orientuotas į riziką, sutelktas į ypatingos svarbos infrastruktūrą, kurios tinkamas veikimas turi didelę svarbą visuomenei, ir turėtų būti grindžiamas esamomis, rinka grindžiamomis pramonės pastangomis siekiant užtikrinti tinklų atsparumą; pabrėžia ypatingą bendradarbiavimo operacijų lygiu svarbą stiprinant veiksmingesnį viešųjų valdžios institucijų ir privačiojo sektoriaus keitimąsi informacija, susijusia su kibernetinėmis grėsmėmis, tiek Sąjungos, tiek nacionaliniu lygmeniu, taip pat šia informacija keičiantis su strateginiais Sąjungos partneriais siekiant užtikrinti tinklų ir informacijos saugumą, kuriant tarpusavio pasitikėjimą, vertę ir įsipareigojimus, taip pat keičiantis patirtimi; mano, kad viešojo ir privačiojo sektorių partnerystė turėtų būti grindžiama tinklų ir technologijų neutralumu ir turėtų būti sutelkta į pastangas problemoms, kurios daro didelį poveikį visuomenei, spręsti; ragina Komisiją skatinti visus su tuo susijusius rinkos dalyvius būti atidesnius ir labiau bendradarbiauti, kad būtų galima kitus dalyvius apsaugoti nuo žalos jų paslaugoms;

13. pripažįsta, kad kibernetinio saugumo incidentų aptikimas ir pranešimas apie juos turi esminę svarbą Sąjungoje skatinant kibernetinį atsparumą; yra įsitikinęs, kad turėtų būti nustatyti proporcingi ir reikalingi informacijos atskleidimo kompetentingoms nacionalinėms institucijoms reikalavimai siekiant pranešti apie incidentus, apimančius didelius saugumo pažeidimus, taip sudarant sąlygas geriau stebėti su elektroniniais nusikaltimais susijusius incidentus ir skatinti pastangas didinti informuotumą visais lygmenimis;

14. ragina Komisiją ir kitus veikėjus nustatyti kibernetinio saugumo ir kibernetinio atsparumo politiką, kuri apimtų ekonomines paskatas skatinti aukšto lygio kibernetinį saugumą ir kibernetinį atsparumą;

Kibernetinis atsparumas

15. primena, kad įvairūs sektoriai ir valstybės narės turi įvairių lygių pajėgumus ir įgūdžius ir kad tai trukto plėtoti pasitikėjimu pagrįstą bendradarbiavimą ir trukdo veikti bendrajai rinkai;

16. mano, kad reikalavimai, skirti mažosioms ir vidutinėms įmonėms, turėtų būti nustatyti laikantis proporcingo ir rizika grindžiamo požiūrio;

17. primygtinai reikalauja vystyti ypatingos svarbos infrastruktūrų atsparumą ir primena, kad nustatant būsimą tvarką, kuria Sąjunga įgyvendina solidarumo sąlygą (SESV 222 straipsnis), turėtų būti atsižvelgiama į kibernetinio išpuolio prieš valstybę narę pavojų; ragina Komisiją ir Vyriausiąją įgaliotinę atsižvelgti į šį pavojų rengiant savo integruotas grėsmių ir rizikos vertinimo ataskaitas, kurios turėtų būti rengiamos nuo 2015 m.;

18. pabrėžia, kad ypač siekiant užtikrinti ypatingos svarbos paslaugų patikimumą, prieinamumą ir konfidencialumą, ypatingos svarbos infrastruktūros nustatymas ir kategorizavimas turi būti atnaujinamas ir turi būti nustatyti reikalingi minimalūs jų tinklų ir informacinių sistemų saugumo reikalavimai;

19. pripažįsta, kad pasiūlyme dėl direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti tokie minimalūs saugumo reikalavimai numatomi informacinės visuomenės paslaugų teikėjams ir ypatingos svarbos infrastruktūros operatoriams;

20. ragina valstybes nares ir Sąjungą nustatyti tinkamus pagrindus greitoms abipusio keitimosi informacija sistemoms, tai užtikrins anonimiškumą privačiajam sektoriui ir sudarys sąlygas nuolat informuoti privatų sektorių, taip pat prireikus teikti paramą viešajam sektoriui;

21. palankiai vertina Komisijos ketinimą sukurti su kibernetiniu saugumu susijusios rizikos valdymo kultūrą ir ragina valstybes nares ir Sąjungos institucijas į savo krizių valdymo planus ir rizikos analizes greitai įtraukti kibernetinių krizių valdymą; taip pat ragina valstybių narių vyriausybes ir Komisiją skatinti privačiojo sektoriaus veikėjus į savo valdymo planus ir rizikos analizes įtraukti kibernetinių krizių valdymą ir mokyti savo darbuotojus kibernetinio saugumo klausimais;

22. ragina valstybes nares ir Sąjungos institucijas sukurti gerai veikiančių kompiuterinių incidentų tyrimo tarnybų (CERT) tinklą, kuris veiktų visą parą kiekvieną savaitės dieną; atkreipia dėmesį į tai, kad nacionalinės CERT turėtų priklausyti veiksmingam tinklui, kuriame būtų keičiamasi svarbia informacija, remiantis būtinaisiais pasitikėjimo ir konfidencialumo standartais; pažymi, kad bendros iniciatyvos, apimančios CERT ir kitas svarbias apsaugos įstaigas, gali būti naudingos priemonės kuriant pasitikėjimą tarpvalstybiniame ir tarpsektoriniame kontekste; pripažįsta efektyvaus ir veiksmingo CERT ir teisėsaugos tarnybų bendradarbiavimo svarbą kovojant su elektroniniais nusikaltimais;

23. palaiko savo su tinklų ir informacijos saugumu susijusias užduotis vykdančią, ypač gaires teikiančią ir valstybes nares konsultuojančią, taip pat keitimąsi geriausios praktikos pavyzdžiais ir pasitikėjimo aplinkos kūrimą remiančią agentūrą ENISA;

24. pabrėžia poreikį, kad pramonė visoje transporto tinkluose ir informacijos sistemose naudojamų IRT produktų vertės grandinėje taikytų kibernetinio saugumo užtikrinimo reikalavimus, vykdytų tinkamą rizikos valdymą, priimtų saugumo standartus ir sprendimus ir išvystytų geriausią praktiką ir keitimąsi informacija siekiant užtikrinti kibernetiniu požiūriu saugias transportavimo sistemas;

Pramonės ir technologijų ištekliai

25. laikosi nuomonės, kad tinklų ir informacijos aukšto lygio saugumo užtikrinimas atlieka pagrindinį vaidmenį Sąjungoje didinant ir saugumo sprendimų tiekėjų, ir naudotojų konkurencingumą; mano, kad nors IT saugumo pramonė Sąjungoje turi didelį neišnaudotą potencialą, privatūs, viešieji ir verslo srities naudotojai dažnai nėra informuoti apie investavimo į kibernetinį saugumą sąnaudas ir naudą ir todėl lieka pažeidžiami dėl jiems gresiančių kenksmingų kibernetinių grėsmių; pabrėžia, kad CERT įgyvendinimas yra šiuo požiūriu svarbus veiksnys;

26. yra įsitikinęs, kad norėdamos turėti tvirtą kibernetinio saugumo sprendimų pasiūlą ir paklausą nacionalinės valdžios institucijos, įtrauktos į IRT klausimus, turi atitinkamai investuoti į akademinius išteklius, mokslinius tyrimus ir plėtrą, taip pat stiprinti žinias ir gebėjimus, kad būtų skatinamos naujovės ir užtikrinamas pakankamas informuotumas apie tinklų ir informacijos saugumo pavojus, sudarant pagrindą suderintai Europos saugumo pramonei;

27. ragina Sąjungos institucijas ir valstybes nares imtis reikalingų priemonių siekiant sukurti bendrąją kibernetinio saugumo rinką, kurioje naudotojai ir tiekėjai galėtų kuo geriau pasinaudoti naujovėmis, sąveikomis, suderinta su pasiūla susijusia patirtimi ir kuri sudarytų sąlygas MVĮ įsijungimui;

28. ragina valstybes nares svarstyti bendrų investicijų į Europos kibernetinio saugumo pramonę galimybę, panašiai kaip tai padaryta kitose pramonės srityse, pvz., aviacijos sektoriuje;

Elektroniniai nusikaltimai

29. mano, kad nusikalstama veikla kibernetinėje erdvėja gali būti tiek pat žalinga visuomenės gerovei, kiek nusikaltimai fiziniame pasaulyje, taip pat kad šios nusikaltimų formos dažnai palaiko viena kitą, kaip tai galima teigti, pavyzdžiui, vaikų seksualinio išnaudojimo ir organizuoto nusikalstamumo bei pinigų plovimo atveju;

30. pažymi, kad kai kuriais atvejais yra ryšys tarp teisėtos ir neteisėtos verslo veiklos; pažymi, kad labai svarbus terorizmo finansavimo ir rimto organizuoto nusikalstamumo ryšys, kuriam palankesnes sąlygas sudaro internetas; pabrėžia, kad visuomenė turi būti informuota apie rimtus įsitraukimo į elektroninius nusikaltimus padarinius ir apie tai, kad iš pirmo žvilgsnio visuomenei priimtinu nusikaltimu atrodanti veikla, pvz., neteisėtas filmų parsisiuntimas, dažnai tarptautinėms nusikalstamoms grupėms padeda gauti dideles pinigų sumas;

2013 m. rugsėjo 12 d., ketvirtadienis

31. sutinka su Komisija, kad tos pačios normos ir principai, kurie galioja ne internete, taip pat galioja ir internete, ir todėl kova su elektroniniais nusikaltimais turi būti sustiprinta atnaujinant teisės aktus ir operacinius pajėgumus;

32. laikosi požiūrio, kad atsižvelgiant į beribį elektroninių nusikaltimų pobūdį, Sąjungos lygmeniu, viršesniu už atskirų valstybių narių lygmenį, dedamos bendros pastangos ir teikiamos žinios yra itin svarbios ir kad todėl Eurojustui, Europolo EC3, CERT, universitetams ir mokslinių tyrimų centrams turi būti teikiami atitinkami ištekliai ir pajėgumai, kad jie galėtų tinkamai veikti kaip žinių, bendradarbiavimo ir keitimosi informacija centrai;

33. labai palankiai vertina EC3 įsteigimą ir ragina ateityje plėtoti šią agentūrą ir jos gyvybiškai svarbų vaidmenį koordinuojant laiku atliekamą ir veiksmingą tarpvalstybinį keitimąsi informacija ir patirtimi palaikant pastangas užkirsti kelią elektroniniams nusikaltimams, juos aptikti ir tirti;

34. ragina valstybes nares užtikrinti, kad piliečiai galėtų lengvai gauti informaciją apie kibernetines grėsmes ir apie tai, kaip su jomis kovoti; yra įsitikinęs, kad tokios gairės turėtų apimti informaciją apie tai, kaip naudotojai gali internete apsaugoti savo privatumą, kaip aptikti vaiko viliojimo atvejus ir apie juos pranešti, kaip įdiegti programinę įrangą ir užkardas, kaip tvarkyti slaptažodžius ir nustatyti klaidingą identifikavimą (duomenų vagystes), viliojimą (neteisėtą nukreipimą į tam tikras svetaines) ir kitokius išpuolius;

35. primygtinai reikalauja, kad valstybės narės, kurios dar neratifikavo Europos Tarybos Budapešto konvencijos dėl elektroninių nusikaltimų, tai padarytų be reikalo nedelsdamos; palankiai vertina Europos Tarybos pastabas dėl poreikio konvenciją atnaujinti atsižvelgiant į technologinius pokyčius, kad būtų galima užtikrinti jos nuolatinį veiksmingumą kovojant su elektroniniais nusikaltimais, ir ragina Komisiją ir valstybes nares dalyvauti šiose diskusijose; palaiko pastangas skatinti konvencijos ratifikavimą kitose šalyse ir ragina Komisiją ją aktyviai propaguoti už Sąjungos ribų;

Kibernetinė gynyba

36. pabrėžia, kad kibernetiniai iššūkiai, grėsmės ir išpuoliai kelia pavojų valstybių narių gynybos ir nacionalinio saugumo interesams ir kad civiliai ir kariniai metodai, taikomi vykdant užduotį apsaugoti ypatingos svarbos infrastruktūrą, siekiant sąveikų, turėtų padidinti naudą šiose abiejose srityse;

37. taigi ragina valstybes nares intensyviau bendradarbiauti su Europos gynybos agentūra (EGA) siekiant parengti iniciatyvas ir pasiūlymus, skirtus gynybos pajėgumams stiprinti ir paremtus naujausiomis iniciatyvomis ir projektais; pabrėžia poreikį didinti mokslinius tyrimus ir plėtrą, taip pat kaupiant išteklius ir jais dalijantis;

38. pakartoja, kad rengiant išsamią ES kibernetinio saugumo strategiją turėtų būti atsižvelgiama į esamų agentūrų ir įstaigų papildomą vertę ir į tų valstybių narių, kurios jau taiko savo nacionalines kibernetinio saugumo strategijas, sukauptą gerąją praktiką;

39. ragina Komisijos pirmininko pavaduotoją-vyriausiąją įgaliotinę kibernetinių krizių valdymą įtraukti į krizių valdymo planavimą ir pabrėžia poreikį, kad valstybės narės, bendradarbiaudamos su EGA, parengtų planus, kaip nuo kibernetinių išpuolių apsaugoti BSGP misijas ir operacijas; ragina jas kartu sudaryti Europos kibernetinės gynybos pajėgas;

40. pabrėžia, kad kibernetinio saugumo srityje vyksta geras praktinis bendradarbiavimas su NATO ir kad šį bendradarbiavimą reikia remti, ypač glaudžiau jį koordinuojant planavimo, technologijų, mokymo ir įrangos srityse;

41. ragina Sąjungą dėti pastangas pradėti mainus su tarptautiniais partneriais, įskaitant NATO, nustatyti bendradarbiavimo sritis, kur įmanoma, išvengti veiklos dubliavimo ir ją papildyti;

Tarptautinė politika

42. yra įsitikinęs, kad tarptautinis bendradarbiavimas ir dialogas atlieka esminį vaidmenį kuriant pasitikėjimą ir skaidrumą ir skatinant aukšto lygio tinklų kūrimą ir keitimąsi informacija pasauliniu lygmeniu; taigi ragina Komisiją ir Europos išorės veiksmų tarnybą sudaryti kibernetinės diplomatijos grupę, kurios užduotys apimtų dialogo su panašiai mąstančiomis šalimis ir organizacijomis skatinimą; ragina ES aktyviau dalyvauti gausiose tarptautinio lygio konferencijose kibernetinio saugumo klausimais;

43. mano, kad reikia rasti pusiausvyrą tarp duomenų perdavimo, duomenų apsaugos ir kibernetinio saugumo konkuruojančių tikslų, laikantis Sąjungos tarptautinių įsipareigojimų, ypač pagal GATS;

44. ragina Komisijos pirmininko pavaduotoją-vyriausiąją įgaliotinę kibernetinio saugumo aspektą įtraukti į ES išorės veiksmus, ypač susijusius su trečiosiomis šalimis, siekiant intensyviau bendradarbiauti ir keistis patirtimi bei informacija apie tai, kaip spręsti kibernetinio saugumo klausimus;

45. ragina Sąjungą dėti pastangas pradėti mainus su tarptautiniais partneriais siekiant nustatyti bendradarbiavimo sritis, kur įmanoma, išvengti veiklos dubliavimo ir ją papildyti; ragina Komisijos pirmininko pavaduotoją-vyriausiąją įgaliotinę ir Komisiją proaktyviai veikti tarptautinėse organizacijose ir derinti valstybių narių pozicijas dėl to, kaip veiksmingai skatinti sprendimus ir politiką kibernetikos srityje;

46. laikosi nuomonės, jog turi būti stengiamasi užtikrinti, kad turimos tarptautinės teisinės priemonės, ypač Europos Tarybos konvencija dėl elektroninių nusikaltimų, būtų taikomos kibernetinėje erdvėje; taigi mano, kad dabar nėra poreikio tarptautiniu lygiu rengti naujas teisines priemones; vis dėlto palankiai vertina tarptautinį bendradarbiavimą siekiant rengti elgesio kibernetinėje erdvėje normas, kurios kibernetinėje erdvėje palaikytų teisinės valstybės principą; mano, kad reikėtų svarstyti galimybę atnaujinti esamas teisines priemones, kad jos atitiktų technologijos pažangą; laikosi nuomonės, kad sprendžiant jurisdikcijos klausimus reikia nuoseklių diskusijų teisminio bendradarbiavimo ir persekiojimo tarpvalstybinio nusikalstamumo atveju temomis;

47. mano, kad ypač ES ir JAV kibernetinio saugumo ir kovos su elektroniniais nusikaltimais darbo grupė turėtų būti priemonė ES ir JAV prireikus keistis geriausios praktikos pavyzdžiais kibernetinio saugumo politikos srityje; į tai atsižvelgdamas pažymi, kad su kibernetiniu saugumu susijusios sritys, pvz., paslaugos, priklausančios nuo saugaus tinklų ir informacinių sistemų veikimo, bus įtrauktos į būsimas Tarpatlantinės prekybos ir investicijų partnerystės derybas, siekiant šią partnerystę sudaryti taip, kad būtų išsaugotas ES suverenumas ir jos institucijų nepriklausomumas;

48. pažymi, kad kibernetinio saugumo įgūdžiai ir gebėjimas užkirsti kelią grėsmėms ir piktavališkiems išpuoliams, juos aptikti ir veiksmingai su jais kovoti pasaulyje nėra tolygiai išvystyti; pabrėžia, jog pastangos didinti kibernetinį atsparumą ir kovoti su kibernetinėmis grėsmėmis neturi būti vykdomos tik kartu su panašiai mąstančiais partneriais, bet ir turėtų būti dedamos mažiau išplėtotus pajėgumus, techninę infrastruktūrą ir teisines sistemas turinčiuose regionuose; mano, kad šiuo klausimus CERT koordinavimas yra labai svarbus; ragina Komisiją skatinti ir prireikus remti trečiųjų šalių pastangas pačioms stiprinti kibernetinio saugumo pajėgumus, naudojant tinkamas priemones;

Įgyvendinimas

49. ragina reguliariai aukščiausiuoju politiniu lygmeniu įvertinti nacionalinių kibernetinio saugumo strategijų veiksmingumą siekiant užtikrinti prisitaikymą prie naujų pasaulinių grėsmių ir tokį patį kibernetinio saugumo lygį skirtingose valstybėse narėse;

50. ragina Komisiją parengti aiškias gaires, kuriose būtų nustatyti terminai, iki kurių reikia pasiekti Sąjungos tikslus pagal kibernetinio saugumo strategiją ir atlikti jų vertinimą; ragina valstybes nares susitarti dėl panašaus nacionalinės veiklos įvykdymo pagal šią strategiją plano;

2013 m. rugsėjo 12 d., ketvirtadienis

51. prašo, kad Komisija, valstybės narės, Europolas ir naujai įsteigtas EC3, Eurojustas ir ENISA teiktų reguliarias ataskaitas, kuriose būtų įvertinama pažanga siekiant kibernetinio saugumo strategijoje nustatytų tikslų, įskaitant pagrindinius rezultatyvumo rodiklius, kuriais būtų vertinama įgyvendinimo pažanga;

o

o o

52. paveda Pirmininkui perduoti šią rezoliuciją Tarybai, Komisijai, valstybių narių vyriausybėms ir parlamentams, Europolui, Eurojustui bei Europos Tarybai.

P7_TA(2013)0377

Europos skaitmeninė darbotvarkė. Skaitmeninėmis technologijomis grindžiamas Europos augimas

2013 m. rugsėjo 12 d. Europos Parlamento rezoliucija „Skaitmeninė darbotvarkė. Augimas, judumas ir užimtumas: metas judėti sparčiau“ (2013/2593(RSP))

(2016/C 093/17)

Europos Parlamentas,

— atsižvelgdamas į 2012 m. gruodžio 18 d. Komisijos komunikatą „Europos skaitmeninė darbotvarkė. Skaitmeninėmis technologijomis grindžiamas Europos augimas“ (COM(2012)0784 *final*),

— atsižvelgdamas į Komisijai ir Tarybai pateiktus klausimus dėl rezoliucijos „Skaitmeninė darbotvarkė. Augimas, judumas ir užimtumas: metas judėti sparčiau“ (O-000085 – B7-0219/2013 ir O-000086 – B7-0220/2013),

— atsižvelgdamas į 2012 m. birželio 13 d. Europos Parlamento ir Tarybos reglamentą (ES) Nr. 531/2012 dėl tarptinklinio ryšio per viešuosius judriojo ryšio tinklus Europos Sąjungoje ([1]),

— atsižvelgdamas į 2012 m. kovo 14 d. Europos Parlamento ir Tarybos sprendimą Nr. 243/2012/ES, kuriuo nustatoma daugiametė radijo spektro politikos programa ([2]),

— atsižvelgdamas į vykstančias derybas dėl Europos infrastruktūros tinklų priemonės ir ypač į pakeistą pasiūlymą dėl Europos Parlamento ir Tarybos reglamento dėl transeuropinių telekomunikacijų tinklų gairių, kuriuo panaikinamas Sprendimas Nr. 1336/97/EB (COM(2013)0329),

— atsižvelgdamas į savo 2010 m. gegužės 5 d. rezoliuciją „Nauja Europos skaitmeninė darbotvarkė: „2015.eu“ ([3]),

— atsižvelgdamas į 2012 m. rugsėjo 27 d. Komisijos komunikatą „Nuotolinės kompiuterijos galimybių naudojimas Europoje“ (COM(2012)0529),

— atsižvelgdamas į 2012 m. sausio 25 d. pasiūlymą dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas) (COM(2012)0011),

---

([1]) OL L 172, 2012 6 30, p. 10.
([2]) OL L 81, 2012 3 21, p. 7.
([3]) OL C 81 E, 2011 3 15, p. 45.