EIROPAS PARLAMENTS 2009 - 2014

Sesijas dokuments

A7-0335/2012

17.10.2012

ZIŅOJUMS

par kiberdrošību un kiberaizsardzību
(2012/2096(INI))

Ārlietu komiteja

Referents: *Tunne Kelam*

SATURA RĀDĪTĀJS

Lpp.

EIROPAS PARLAMENTA REZOLŪCIJAS PRIEKŠLIKUMS

par kiberdrošību un kiberaizsardzību

(2012/2096(INI))

Eiropas Parlaments,

– ņemot vērā ziņojumu par Eiropas drošības stratēģijas īstenošanu, ko Eiropadome apstiprināja 2008. gada 11. un 12. decembrī,

– ņemot vērā 2004. gada 23. novembrī Budapeštā pieņemto Eiropas Padomes Konvenciju par kibernoziegumiem,

– ņemot vērā Padomes 2011. gada 27. maija secinājumus par informācijas kritiskās infrastruktūras aizsardzību un iepriekšējos Padomes secinājumus par kiberdrošību,

– ņemot vērā Komisijas 2010. gada 19. maija paziņojumu „Digitālā programma Eiropai" (COM(2010)0245),

– 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[1],

– ņemot vērā neseno Komisijas paziņojumu par Eiropas Kibernoziedzības centra izveidi kā iekšējās drošības stratēģijas prioritāti (COM(2012)0140),

– ņemot vērā tā 2010. gada 10. marta rezolūciju par Eiropas drošības stratēģijas un Eiropas kopējās drošības un aizsardzības politikas īstenošanu[2],

– ņemot vērā tā 2011. gada 11. maija rezolūciju par kopējās drošības un aizsardzības politikas attīstību pēc Lisabonas līguma stāšanās spēkā[3],

– ņemot vērā tā 2012. gada 22. maija rezolūciju par Eiropas Savienības iekšējās drošības stratēģiju[4],

– ņemot vērā tā 2011. gada 27. septembra rezolūciju par priekšlikumu Eiropas Parlamenta un Padomes Regulai, ar kuru groza Regulu (EK) Nr. 1334/2000, ar ko nosaka Kopienas režīmu divējāda lietojuma preču un tehnoloģiju eksporta kontrolei[4],

– ņemot vērā tā 2012. gada 12. jūnija rezolūciju par informācijas kritiskās infrastruktūras aizsardzību — sasniegumi un turpmākie pasākumi virzībā uz globālu kiberdrošību[5],

---

[1] OV L 345, 23.12.2008., 75. lpp.
[2] Pieņemtie teksti, P7_TA(2010)0061.
[3] Pieņemtie teksti, P7_TA(2011)0228.
[4] Pieņemtie teksti, P7_TA(2012)0207.
[4] Pieņemtie teksti, P7_TA(2012)0406.
[5] Pieņemtie teksti, P7_TA(2012)0237.

– ņemot vērā ANO Cilvēktiesību padomes 2012. gada 5. jūlija rezolūciju „Cilvēktiesību veicināšana, aizsardzība un īstenošana internetā”[6], kurā atzīta cilvēktiesību aizsardzības un brīvas informācijas plūsmas tiešsaistē nozīme,

– ņemot vērā 2012. gada 20. maija Čikāgas augstākā līmeņa sanāksmes secinājumus,

– ņemot vērā ES līguma V sadaļu,

– ņemot vērā Reglamenta 48. pantu,

– ņemot vērā Ārlietu komitejas ziņojumu (A7-0335/2012),

A. tā kā šodienas globalizētajā pasaulē ES un tās dalībvalstis ir kļuvušas būtiski atkarīgas no drošas kibertelpas, informācijas un digitālo tehnoloģiju drošas izmantošanas un elastīgiem un drošiem informācijas pakalpojumiem un ar tiem saistītajām infrastruktūrām;

B. tā kā informācijas un komunikāciju tehnoloģijas izmanto arī kā represijas rīkus; tā kā šo tehnoloģiju izmantošanas konteksts lielā mērā nosaka, kāda ietekme tām var būt kā pozitīvas attīstības vai represiju līdzeklim;

C. tā kā kiberproblēmas, kiberdraudi un kiberuzbrukumi pieaug dramatiskā tempā un lielā mērā apdraud nacionālo valstu un privātā sektora drošību, aizsardzību, stabilitāti un konkurētspēju; tā kā šādus draudus nedrīkst uzskatīt tikai par nākotnes problēmu; tā kā lielākā daļa labi uzskatāmu un kaitniecisku kiberincidentu mūsdienās ir politiski motivēti; tā kā vairākums kiberincidentu ir primitīvi, taču nozīmīgiem objektiem radītais apdraudējums kļūst arvien sarežģītāks un tāpēc ir pamatoti nepieciešama padziļināta aizsardzība;

D. tā kā kibertelpa ar gandrīz diviem miljardiem globāli savienotu lietotāju ir kļuvusi par vienu no visspēcīgākajiem un efektīvākajiem līdzekļiem demokrātisku ideju veicināšanai un cilvēku organizēšanai, kad tie cenšas realizēt savus sapņus par brīvību un cīnīties pret diktatūru; tā kā nedemokrātiski un autoritāri režīmi, izmantojot kibertelpu, aizvien vairāk apdraud cilvēku tiesības uz vārda un biedrošanās brīvību; tā kā tādēļ ir svarīgi nodrošināt, lai kibertelpa arī turpmāk būtu atvērta brīvai ideju, informācijas un izpausmes plūsmai;

E. tā kā ES un dalībvalstīs ir daudz politisku, likumdošanas un organizatorisku šķēršļu, kas kavē vispārējas un vienotas kiberaizsardzības un kiberdrošības pieejas izveidi; tā kā konfidenciālajā un neaizsargātajā kiberdrošības jomā trūkst kopējas definīcijas, standartu un pasākumu;

F. tā kā ES iestādēs dalīšanās un koordinācija ar dalībvalstīm un dalībvalstu starpā, kā arī ar ārējiem partneriem ir vēl aizvien nepietiekama;

G. tā kā ES un starptautiskajā līmenī trūkst skaidru un saskaņotu „kiberdrošības” un „kiberaizsardzības” definīciju; tā kā dažādās valstīs kiberdrošības un citu galveno terminu izpratne ir ļoti atšķirīga;

[6] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

H. tā kā ES vēl nav izstrādājusi saskaņotu politiku attiecībā uz informācijas kritiskās infrastruktūras aizsardzību, kam ir vajadzīga daudznozaru pieeja, lai stiprinātu drošību, bet vienlaikus ievērotu arī pamattiesības;

I. tā kā ES ir ierosinājusi dažādas iniciatīvas civilā līmeņa kibernoziegumu novēršanai, tostarp jauna Eiropas Kibernoziedzības centra izveidi, taču tai joprojām nav konkrēta plāna drošības un aizsardzības līmenī;

J. tā kā uzticēšanās un sapratnes iedibināšana starp privātā sektora, tiesībaizsardzības, aizsardzības un citām kompetentajām iestādēm ir ārkārtīgi svarīga cīņā pret kibernoziedzību;

K. tā kā uzticēšanās un savstarpēja paļāvība attiecībās starp valsts un nevalstiskajiem dalībniekiem ir priekšnoteikums uzticamai kiberdrošībai;

L. tā kā par lielāko daļu kiberincidentu publiskajā un privātajā sektorā netiek ziņots konfidenciālas informācijas un iespējama kaitējuma dēļ iesaistītā uzņēmuma prestižam;

M. tā kā liels skaits kiberincidentu notiek tādēļ, ka privātā un publiskā tīkla infrastruktūra nav pietiekami elastīga un noturīga un datubāzes un citas plūsmas informācijas kritiskajā infrastruktūrā ir vāji aizsargātas vai nodrošinātas; tā kā tikai dažas dalībvalstis tīklu un informācijas sistēmu un saistīto datu aizsardzību uzskata par savu attiecīgo rūpības pienākumu daļu, ar ko var izskaidrot ieguldījumu trūkumu modernās drošības tehnoloģijās, apmācībā un atbilstīgu pamatnostādņu izstrādē, tā kā daudzas dalībvalstis ir atkarīgas no trešo valstu drošības tehnoloģijām un tām būtu jāpalielina centieni mazināt šo atkarību;

N. tā kā lielākā daļa tādu augsta līmeņa kiberuzbrukumu izdarītāju, kas apdraud valstu vai starptautisko drošību un aizsardzību, nekad netiek identificēti un saukti pie atbildības; tā kā nav panākta starptautiska vienošanās par reaģēšanas veidu uz valsts atbalstītiem kiberuzbrukumiem citai valstij, kā arī nav izpratnes par to, vai šādu uzbrukumu var uzskatīt par *casus belli*;

O. tā kā Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*) ir iesaistīta kā dalībvalstu koordinatore, lai atbalstītu labas prakses apmaiņu kiberdrošības jomā, sniedzot ieteikumus par to, kā izstrādāt, īstenot un uzturēt kiberdrošības stratēģiju; aģentūra atbalsta valstu kiberdrošības stratēģijas, valstu ārkārtas rīcības plānus, organizē Eiropas un starptautiskas mācības par informācijas kritiskās infrastruktūras aizsardzību (*CIIP*), kā arī izstrādā valstu mācību scenārijus;

P. tā kā tikai 10 ES dalībvalstis 2012. gada jūnijā bija oficiāli pieņēmušas valsts kiberdrošības stratēģiju;

Q. tā kā kiberaizsardzība ir viena no galvenajām Eiropas Aizsardzības aģentūras (EAA) prioritātēm, kas saskaņā ar Spēju attīstības plānu ir izveidojusi kiberdrošības projektu izstrādes grupu, kurā piedalās vairākums dalībvalstu, lai uzkrātu pieredzi un sniegtu ieteikumus;

R. tā kā ieguldījumi kiberdrošības un kiberaizsardzības jomas pētniecībā un izstrādē ir

svarīgi, lai panāktu progresu un uzturētu augstu kiberdrošības un kiberaizsardzības līmeni; tā kā aizsardzības izdevumi pētniecībā un izstrādē ir samazinājušies un nav sasnieguši līmeni, par ko panākta vienošanās, — 2 % no kopējiem aizsardzības izdevumiem;

S. tā kā izpratnes veidošanai un iedzīvotāju izglītošanai par kiberdrošību ir jābūt visaptverošas kiberdrošības stratēģijas pamatā;

T. tā kā ir jānodrošina līdzsvars starp drošības pasākumiem un LESD noteiktajām pilsoņu tiesībām, piemēram, tiesībām uz privātumu, datu aizsardzību un vārda brīvību, nevienu no tām neupurējot citas vārdā;

U. tā kā aizvien labāk ir jāievēro un jāaizsargā personas tiesības uz privātumu, kā noteikts ES hartā un LESD 16. pantā; tā kā nepieciešamība valstu līmenī nodrošināt un aizsargāt kibertelpu iestādēm un aizsardzības struktūrām ir svarīga, taču to nekādā gadījumā nevajadzētu izmantot par attaisnojumu jebkādai tiesību un brīvību ierobežošanai kibertelpā un informācijas telpā;

V. tā kā interneta globālā un bezrobežu būtība nosaka nepieciešamību pēc jaunām starptautiskās sadarbības un pārvaldības formām ar daudzām ieinteresētajām personām;

W. tā kā valdības aizvien vairāk paļaujas uz privātā sektora dalībniekiem, lai nodrošinātu kritiskās infrastruktūras drošību;

X. tā kā Eiropas Ārējās darbības dienests (EĀDD) vēl nav aktīvi iekļāvis kiberdrošības aspektu savās attiecībās ar trešām valstīm;

Y. tā kā stabilitātes instruments ir pašlaik vienīgā ES programma, kas paredzēta steidzamai reaģēšanai uz krīzēm vai globālās/starpreģionālās drošības problēmām, tostarp arī kiberdrošības apdraudējumiem;

Z. tā kā kopīga reaģēšana — iesaistot ES un ASV kiberdrošības un kibernoziegumu apkarošanas darba grupu — uz kiberdrošības apdraudējumu ir viens no ES un ASV attiecību prioritārajiem jautājumiem,

Pasākumi un koordinācija ES

1. norāda, ka kiberdraudi un kiberuzbrukumi, kas vērsti uz valdības, pārvaldes, militārajām un starptautiskajām struktūrām, strauji pieaug gan ES, gan visā pasaulē un ir ievērojami iemesli bažām, ka valsts un nevalstiski dalībnieki, jo īpaši teroristu un kriminālās organizācijas spēj uzbrukt ES iestāžu un dalībvalstu kritiskajām informācijas un komunikāciju struktūrām un infrastruktūrām, iespējams, radot būtisku kaitējumu, tostarp dinamisku ietekmi;

2. tāpēc uzsver vajadzību pēc vispārējas un saskaņotas pieejas šīm problēmām ES līmenī, izstrādājot visaptverošu ES kiberdrošības stratēģiju, kurā jānodrošina vienota kiberdrošības, kiberaizsardzības un ar aizsardzību saistīta kiberuzbrukuma definīcija, kopīgas darbības redzējums un jāņem vērā arī pašreizējo aģentūru un organizāciju pievienotā vērtība, kā arī to dalībvalstu labā prakse, kurās jau ir valsts kiberdrošības stratēģija; uzsver būtisko nozīmi, kāda ir koordinācijai un sinerģijas radīšanai ES līmenī,

lai palīdzētu apvienot dažādas militāras un civilas iniciatīvas, programmas un pasākumus; uzsver, ka šādai stratēģijai jānodrošina elastība un tā ir regulāri jāatjaunina, lai pielāgotos strauji mainīgajai kibertelpai;

3. aicina Komisiju un Savienības augsto pārstāvi ārlietās un drošības politikas jautājumos gaidāmajā priekšlikumā par solidaritātes klauzulas (LESD 222. pants) īstenošanas noteikumiem ņemt vērā nopietna kiberuzbrukuma iespējamību kādai dalībvalstij; turklāt uzskata — lai arī kiberuzbrukumi, kas apdraud valsts drošību, vēl ir jādefinē, izmantojot vienotu terminoloģiju, tos varētu ietvert savstarpējās aizsardzības klauzulas darbības jomā (LES 42. panta 7. punkts), neskarot proporcionalitātes principu;

4. uzsver, ka kopējā drošības un aizsardzības politikā (KDAP) ir jānodrošina ES militāro operāciju un civilo misiju aizsardzība pret kiberuzbrukumiem; uzsver arī, ka kiberaizsardzībai vajadzētu būt aktīvai KDAP spējai;

5. uzsver, ka ES kiberdrošības politika jāveido tā, lai maksimāli aizsargātu un saglabātu digitālās brīvības un cilvēktiesību ievērošanu tiešsaistē; uzskata, ka internets un IKT ir jāintegrē ES ārpolitikā un drošības politikā, lai sekmētu šos centienus;

6. aicina Komisiju un Padomi nepārprotami atzīt digitālās brīvības par pamattiesībām un nepieciešamiem priekšnosacījumiem vispārēju cilvēktiesību nodrošināšanai; uzsver, ka dalībvalstīm jācenšas ievērot, lai, izstrādājot pasākumus reaģēšanai uz kiberdraudiem un uzbrukumiem, nekādā gadījumā netiktu apdraudētas to iedzīvotāju tiesības un brīvības, un to tiesību aktos pienācīgi jānošķir civila un militāra līmeņa kiberincidenti; aicina ievērot piesardzību, ierobežojot iedzīvotāju spēju izmantot informācijas un komunikāciju tehnoloģiju rīkus;

7. aicina Padomi un Komisiju kopā ar dalībvalstīm izstrādāt Balto grāmatu par kiberaizsardzību, nosakot skaidras definīcijas un kritērijus, pēc kuriem kiberuzbrukumus klasificē civilos un militāros kiberuzbrukumos atbilstīgi to motivācijai un radītajai ietekmei, kā arī nosaka pasākumus, tostarp noziedzīga nodarījuma izdarītāju meklēšana, atklāšana un kriminālvajāšana;

8. konstatē, ka noteikti ir nepieciešams atjaunināt Eiropas drošības stratēģiju, lai noteiktu un rastu līdzekļus individuālu, ar tīklu saistītu un valsts atbalstītu kiberuzbrucēju vajāšanai un saukšanai pie atbildības;

ES līmenī

9. uzsver, ka liela nozīme ir ES iestāžu un aģentūru horizontālai sadarbībai un koordinācijai kiberdrošības jautājumos;

10. uzsver, ka jaunās tehnoloģijas liek mainīt veidu, kā valdības veic ierastos pamatuzdevumus; atkārtoti norāda, ka aizsardzības un drošības politika un tostarp arī pienācīga demokrātiskā uzraudzība ir tieši valdības ziņā; ņem vērā privātā sektora dalībnieku pieaugošo nozīmi drošības un aizsardzības uzdevumu izpildē, kurā bieži vien nav nodrošināta pārredzamība, pārskatatbildība vai demokrātiskās uzraudzības mehānismi;

11. uzsver, ka valdībām, izmantojot jaunās tehnoloģijas drošības un aizsardzības jomā, jāievēro starptautisko publisko un humanitāro tiesību pamatprincipi, piemēram, valstiskās suverenitātes un cilvēktiesību ievērošana; norāda uz ES dalībvalstu, piemēram, Igaunijas, vērtīgo pieredzi kiberdrošības politikas noteikšanā un izstrādē, kā arī kiberaizsardzības jomā;

12. atzīst vajadzību novērtēt kiberuzbrukumu ES informācijas sistēmām un infrastruktūrai vispārējo līmeni; šajā saistībā uzsver vajadzību regulāri novērtēt ES iestāžu gatavības pakāpi novērst potenciālus kiberuzbrukumus; jo īpaši uzsver nepieciešamību stiprināt informācijas kritisko infrastruktūru;

13. tāpat uzsver nepieciešamību nodrošināt informācijas sistēmām ziņas par vājajām vietām, trauksmi un brīdinājumiem attiecībā uz jauniem apdraudējumiem;

14. norāda, ka nesenie kiberuzbrukumi Eiropas informācijas tīkliem un valdību informācijas sistēmām ir nodarījuši būtisku kaitējumu valstu ekonomikai un drošībai, kura apjoms vēl nav pienācīgi novērtēts;

15. aicina visas ES iestādes vistuvākajā laikā izstrādāt kiberdrošības stratēģijas un ārkārtas rīcības plānus savu sistēmu aizsardzībai;

16. aicina visas ES iestādes iekļaut savos riska analīzes un krīžu pārvaldības plānos kiberkrīžu pārvaldības jautājumu; turklāt aicina visas ES iestādes organizēt saviem darbiniekiem informatīvas mācības par kiberdrošību; ierosina reizi gadā organizēt kibermācības līdzīgi tam, kā tiek organizētas mācības ārkārtas gadījumiem;

17. uzsver, ka liela nozīme ir ES Datorapdraudējumu reaģēšanas vienības (ES *CERT*) un valstu *CERT* efektīvai izveidei, kā arī valsts ārkārtas rīcības plānu izstrādei gadījumos, kad steidzami jārīkojas; atzinīgi vērtē to, ka līdz 2012. gada maijam visas ES dalībvalstis ir izveidojušas valsts *CERT*; mudina turpināt attīstīt valstu *CERT* un ES *CERT*, kas vajadzības gadījumā var reaģēt 24 stundu laikā; uzsver vajadzību izpētīt, vai šajā jomā ir iespējamas publiskā un privātā sektora partnerības;

18. atzīst, ka pirmās Eiropas mēroga mācības par informācijas kritiskās infrastruktūras aizsardzību „Cyber Europe 2010”, kurās piedalījās vairākas dalībvalstis un kuras vadīja *ENISA*, bija noderīgs pasākums un labas prakses piemērs; turklāt uzsver, ka pēc iespējas drīzāk Eiropas līmenī jāizveido Kritiskās infrastruktūras brīdinājuma informācijas tīkls;

19. 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;

20. aicina Komisiju izpētīt ES Kiberkoordinācijas punkta vajadzību un iespējamību;

21. uzskata, ka, ņemot vērā augsta līmeņa prasmes, kas nepieciešamas, lai aizsargātu kibersistēmas un infrastruktūru, kā arī uzbruktu tām, Komisijai, Padomei un dalībvalstīm jāizskata iespēja izstrādāt “likumīgo datorpirātu” stratēģiju; norāda, ka šādos gadījumos pastāv ļoti liela intelektuālā darbaspēka emigrācijas iespējamība un jo īpaši nepilngadīgām personām, kuras atzītas par vainīgām šādos uzbrukumos, ir lielas iespējas tikt reabilitētām

un integrētām aģentūrās un struktūrās;

Eiropas Aizsardzības aģentūra (EAA)

22. atzinīgi vērtē nesenās kiberaizsardzības iniciatīvas un projektus, jo īpaši attiecīgu kiberdrošības un kiberaizsardzības datu, kā arī ziņu par problēmām un vajadzībām vākšanu un kartēšanu, un mudina dalībvalstis kiberaizsardzības jomā ciešāk sadarboties ar EAA, tostarp arī militārā līmenī;

23. uzsver, ka dalībvalstu ciešai sadarbībai ar EAA ir liela nozīme kiberaizsardzības spēju attīstīšanā; uzskata, ka sinerģijas veidošana, resursu apvienošana un kopīga izmantošana Eiropas mērogā ir svarīgi aspekti, lai nodrošinātu efektīvu kiberaizsardzību Eiropas un valstu līmenī;

24. mudina EAA padziļināt sadarbību ar NATO, valstu un starptautiskajiem izcilības centriem, Eiropas Kibernoziedzības centru Eiropolā, ar kura palīdzību varēs ātrāk reaģēt uz kiberuzbrukumiem, un jo īpaši ar Kopējo kiberaizsardzības izcilības centru (*CCDCOE*), galveno uzmanību pievēršot spēju veidošanai un mācībām, kā arī informācijas un pieredzes apmaiņai;

25. ar bažām konstatē, ka līdz 2010. gadam tikai viena dalībvalsts bija sasniegusi 2 % izdevumu līmeni pētniecībai un izstrādei aizsardzības jomā un ka 2010. gadā piecas dalībvalstis nebija vispār ieguldījušas līdzekļus pētniecībā un izstrādē; mudina EAA apvienot resursus ar dalībvalstīm un efektīvi ieguldīt līdzekļus kopīgos pētniecības un izstrādes projektos, īpaši pievēršoties kiberdrošībai un aizsardzībai;

Dalībvalstis

26. aicina dalībvalstis nekavējoties izstrādāt un pilnveidot attiecīgās valsts kiberdrošības un aizsardzības stratēģijas un nodrošināt stabilu politikas veidošanas un normatīvo vidi, visaptverošas riska pārvaldības procedūras un atbilstīgus sagatavošanās pasākumus un mehānismus; aicina *ENISA* palīdzēt dalībvalstīm; pauž atbalstu *ENISA* nodomam izstrādāt labas prakses rokasgrāmatu, aprakstot tajā labas prakses piemērus un sniedzot ieteikumus, kā izstrādāt, īstenot un uzturēt kiberdrošības stratēģiju;

27. mudina visas dalībvalstis to militārajā struktūrā izveidot īpašas kiberdrošības un kiberaizsardzības vienības, lai sadarbotos ar līdzīgām struktūrām citās ES dalībvalstīs;

28. aicina dalībvalstis reģionālā līmenī ieviest specializētas tiesas, lai nodrošinātu efektīvāku sodīšanu par uzbrukumiem informācijas sistēmām; uzsver, ka ir nepieciešams sekmēt valstu tiesību aktu pielāgošanu, lai tie būtu saderīgi ar tehnikas un lietojumu attīstību;

29. aicina Komisiju turpināt izstrādāt saskaņotu un efektīvu Eiropas pieeju, lai izvairītos no liekām iniciatīvām un iedrošinātu un atbalstītu dalībvalstu centienus izveidot sadarbības mehānismus un pastiprināt informācijas apmaiņu; uzskata, ka ir jānosaka minimālais obligātās sadarbības un līdzdalīšanās līmenis starp dalībvalstīm;

30. mudina dalībvalstis izstrādāt valsts ārkārtas rīcības plānus un krīžu pārvaldības plānos un riska analīzē iekļaut kiberkrīžu pārvaldību; uzsver, ka svarīgi ir pienācīgi apmācīt

publisko struktūru darbiniekus par kiberdrošības pamatjautājumiem un jo īpaši svarīgi ir mācību struktūrās piedāvāt piemērotas mācības tiesu un drošības iestāžu locekļiem; aicina *ENISA* un citas attiecīgās iestādes palīdzēt dalībvalstīm apvienot līdzekļus un tos kopīgi izmantot, kā arī izvairīties no dublēšanās;

31. mudina dalībvalstis padarīt pētniecību un izstrādi par vienu no galvenajiem kiberdrošības un kiberaizsardzības pīlāriem un veicināt informācijas sistēmu aizsardzības inženieru apmācību; aicina dalībvalstis izpildīt savas saistības palielināt aizsardzības izdevumus pētniecībai un izstrādei līdz vismaz 2 %, īpašu uzmanību pievēršot kiberdrošībai un kiberaizsardzībai;

32. aicina Komisiju un dalībvalstis iesniegt programmas, lai veidotu un sekmētu privāto lietotāju un komerclietotāju izpratni par interneta, informācijas sistēmu un komunikāciju tehnoloģiju lietošanas vispārēju drošību; iesaka Komisijai šajā sakarībā uzsākt publisku Eiropas mēroga izglītības iniciatīvu; aicina dalībvalstis iekļaut zināšanas par kiberdrošību skolu mācību programmās pēc iespējas jaunāku klašu skolēniem;

Publiskā un privātā sektora sadarbība

33. uzsver būtisko nozīmi, kāda ir saturīgai un papildinošai sadarbībai kiberdrošības jomā starp publiskā sektora iestādēm un privāto sektoru gan ES, gan valstu līmenī, lai radītu savstarpēju uzticību; apzinās, ka, turpmāk palielinot attiecīgu publiskā sektora iestāžu uzticamību un efektivitāti, tiks veicināta uzticības palielināšanās un kritiskās informācijas apmaiņa;

34. aicina privātā sektora partnerus apsvērt integrētās drošības risinājumus jaunu produktu, ierīču, pakalpojumu un lietojumu izstrādē un prasa ieviest stimulus uzņēmumiem, kuri izstrādā jaunus produktus, ierīces un lietojumus, kuros integrēta drošība ir galvenā iezīme; prasa izstrādāt obligātus pārredzamības standartus un atbildības mehānismus attiecībā uz sadarbību ar privāto sektoru, lai novērstu un apkarotu kiberuzbrukumus;

35. uzsver, ka informācijas kritiskās infrastruktūras aizsardzība ir iekļauta Eiropas Savienības iekšējās drošības stratēģijā saistībā ar pilsoņu un uzņēmumu drošības līmeņu paaugstināšanu kibertelpā;

36. aicina izveidot pastāvīgu dialogu ar minētajiem partneriem par informācijas sistēmu vislabāko izmantošanu un elastību, kā arī par atbildības dalīšanu, kas nepieciešama šo sistēmu drošai un pareizai darbībai;

37. dalībvalstīm, ES iestādēm un privātajam sektoram sadarbībā ar *ENISA* būtu jāveic pasākumi, lai palielinātu informācijas sistēmu drošību un integritāti, novērstu uzbrukumus un mazinātu uzbrukumu ietekmi; atbalsta Komisijas centienus piedāvāt obligātus kiberdrošības standartus un sertificēšanas sistēmas uzņēmumiem, kā arī nodrošināt pareizus stimulus, lai veicinātu privātā sektora centienus uzlabot drošību;

38. aicina Komisiju un dalībvalstu valdības mudināt privāto sektoru un pilsoniskās sabiedrības pārstāvjus savos krīžu pārvaldības plānos un riska analīzē iekļaut kiberkrīžu pārvaldības jautājumu; turklāt aicina ieviest visiem darbiniekiem paredzētas mācības izpratnes veidošanai par būtiskiem kiberdrošības un kiberhigiēnas aspektiem;

39. aicina Komisiju sadarbībā ar dalībvalstīm un visām attiecīgajām aģentūrām un struktūrām izstrādāt pamatnostādnes un instrumentus ātras informācijas apmaiņas sistēmai, kas nodrošinātu anonimitāti, ja tiek ziņots par kiberpārkāpumiem privātajā sektorā, ļautu publiskā sektora dalībniekiem vienmēr saņemt jaunāko informāciju un sniegtu palīdzību, ja tā vajadzīga.

40. uzsver, ka ES jāveicina konkurētspējīga un novatoriska tirgus izveide kiberdrošībai Eiropas Savienībā, lai MVU varētu labāk darboties šajā jomā, dodot ieguldījumu ekonomikas izaugsmes palielināšanā un jaunu darbavietu radīšanā;

Starptautiskā sadarbība

41. aicina EĀDD izvēlēties aktīvu pieeju kiberdrošībai un integrēt kiberdrošības aspektu visās tā darbībās, jo īpaši attiecībā uz trešām valstīm; aicina paātrināt sadarbību un informācijas apmaiņu par to, kā risināt kiberdrošības jautājumus ar trešām valstīm;

42. uzsver, ka visaptverošas ES kiberdrošības stratēģijas pabeigšana ir priekšnosacījums tādas efektīvas starptautiskas sadarbības izveidei kiberdrošības jomā, kāda ir nepieciešama kiberdraudu pārrobežu raksturiezīmju dēļ;

43. aicina dalībvalstis, kuras vēl nav parakstījušas vai ratificējušas Eiropas Padomes Konvenciju par kibernoziegumiem (Budapeštas konvenciju), nekavējoties to izdarīt; atbalsta Komisijas un EĀDD centienus popularizēt konvenciju un tās vērtības trešo valstu starpā;

44. apzinās starptautiski akceptētas un saskaņotas reakcijas nepieciešamību, atbildot uz kiberdraudiem; tādēļ aicina Komisiju, EĀDD un dalībvalstis visos forumos un jo īpaši Apvienoto Nāciju Organizācijā uzņemties vadību centienos panākt plašāku starptautisku sadarbību un galīgu vienošanos par kopēju definīciju uzvedības normām kibertelpā un arī veicināt sadarbību, lai sagatavotu kiberieroču kontroles nolīgumus;

45. mudina īstenot zināšanu apmaiņu kiberdrošības jomā ar *BRICS* valstīm un citām jaunietekmes valstīm, lai izpētītu iespējamas kopīgas reakcijas iespējas, atbildot uz pieaugošu kibernoziedzību, kiberdraudiem un kiberuzbrukumiem gan civilajā, gan militārajā līmenī;

46. mudina EĀDD un Komisiju izvēlēties aktivitāti veicinošu pieeju attiecīgajos starptautiskajos forumos un organizācijās, jo īpaši ANO, EDSO, ESAO un Pasaules Bankā, lai piemērotu spēkā esošos starptautiskos tiesību aktus un panāktu vienprātību attiecībā uz valsts atbildīgas uzvedības normām saistībā ar kiberdrošību un aizsardzību un saskaņotu dalībvalstu nostājas nolūkā veicināt ES pamatvērtības un politiku kiberdrošības un kiberaizsardzības jomā;

47. aicina Padomi un Komisiju diskusijās, attiecībās un sadarbības nolīgumos ar trešām valstīm, jo īpaši tajos, kuros paredzēta sadarbība vai apmaiņas tehnoloģiju jomā, uzstājīgi iestāties par obligātām prasībām attiecībā uz kibernoziedzības un kiberuzbrukumu novēršanu un apkarošanu; un obligātiem informācijas sistēmas drošības standartiem;

48. aicina Komisiju veicināt un atbalstīt, ja vajadzīgs, trešo valstu centienus pilnveidot savas

kiberdrošības un kiberaizsardzības spējas;

Sadarbība ar NATO

49. vēlreiz atkārto, ka, pamatojoties uz kopīgām vērtībām un stratēģiskām interesēm, Eiropas Savienībai un NATO ir īpaša atbildība un pienākums efektīvāk un ciešākā sadarbībā pievērsties pieaugošām kiberdrošības problēmām, meklējot iespējamus savstarpējus papildinājumus, bez dublēšanas un ievērojot attiecīgi savu atbildību;

50. uzsver nepieciešamību apvienot spēkus un kopīgi darboties praktiskā līmenī, ņemot vērā ES un NATO savstarpēji papildinošo pieeju kiberdrošībai un kiberaizsardzībai; uzsver ciešākas koordinācijas nepieciešamību, jo īpaši saistībā ar plānošanu, tehnoloģiju, mācībām un aprīkojumu attiecībā uz kiberdrošību un kiberaizsardzību;

51. pamatojoties uz pašreizējiem papildinošajiem pasākumiem aizsardzības spēju attīstībā, mudina visas attiecīgās struktūras Eiropas Savienībā, kas nodarbojas ar kiberdrošību un kiberaizsardzību, padziļināt savu praktisko sadarbību ar NATO, lai apmainītos ar pieredzi un mācītos, kā pilnveidot ES sistēmu elastīgumu;

Sadarbība ar Amerikas Savienotajām Valstīm

52. uzskata, ka ES un ASV būtu jāpadziļina savstarpējā sadarbība, lai stātos pretī kiberuzbrukumiem un kibernoziegumiem, jo pēc 2010. gada ES un ASV augstākā līmeņa sanāksmes Lisabonā tā ir kļuvusi par transatlantisko attiecību prioritāti;

53. 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 kiberdrošības jautājumus ietvert transatlantiskās politikas dialogā;

54. atzinīgi vērtē to, ka Komisija un ASV valdība ES un ASV darba grupas vadībā kopīgi izstrādāja kopēju programmu un ceļvedi kopīgām/sinhronizētām starpkontinentālām kibermācībām 2012./2013. gadā; ņem vērā pirmās atlantiskās kibermācības, kas notika 2011. gadā;

55. uzsver, ka ASV un ES, kuras nodrošina lielāko kibertelpu un lietotāju skaitu, ir jāsadarbojas, lai aizsargātu savu pilsoņu tiesības un brīvības izmantot kibertelpu; uzsver, ka valsts drošība ir galvenais mērķis, taču kibertelpai ir jābūt gan drošai, gan aizsargātai;

56. uzdod priekšsēdētājam nosūtīt šo rezolūciju Padomei, Komisijai, AP/PV, kā arī EAA, *ENISA* un NATO.

KOMITEJAS GALĪGAIS BALSOJUMS

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