Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu"

(COM(2018) 630 final — 2018/0328 (COD))

(2019/C 159/10)

Ziņotājs: **Antonio LONGO**

Līdzziņotājs: **Alberto MAZZOLA**

Apspriešanās	Eiropadome, 5.10.2018. Eiropas Parlaments, 1.10.2018.
Juridiskais pamats	Līguma par Eiropas Savienības darbību 173. panta 3. punkts, 188. un 304. pants
Atbildīgā specializētā nodaļa	Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa
Pieņemts specializētās nodaļas sanāksmē	9.1.2019.
Pieņemts plenārsesijā	23.1.2019.
Plenārsesija Nr.	540
Balsojuma rezultāts (par/pret/atturas)	143/5/2

1. Secinājumi un ieteikumi

1.1. Eiropas Ekonomikas un sociālo lietu komiteja (EESK) atzinīgi vērtē Komisijas iniciatīvu un uzskata, ka tā ir būtiska, lai izstrādātu industriālo kiberdrošības stratēģiju, un stratēģiski nozīmīga, lai panāktu stabilu un plašu digitālo autonomiju. Šie aspekti ir nepieciešami, lai stiprinātu Eiropas aizsardzības mehānismus notiekošajā kiberkarā, kas var apdraudēt politiskās, ekonomiskās un sociālās sistēmas.

1.2. Komiteja atzīmē, ka nevienā kiberdrošības stratēģijā nevar ignorēt jautājumu par visu lietotāju plašu informētību un drošu rīcību.

1.3. EESK atbalsta priekšlikuma vispārējos mērķus un apzinās, ka par īpašajiem darbības aspektiem būs jāveic turpmāka analīze. Tomēr, tā kā tā ir regula, Komiteja uzskata, ka pārvaldības, finansēšanas un jau noteiktu mērķu sasniegšanas konkrētie sensitīvie aspekti būtu jānosaka iepriekš. Svarīga nozīme ir tam, lai paredzamais tīkls un centrs būtu pēc iespējas lielākā mērā balstīts uz dalībvalstu kiberspējām un īpašajām zināšanām un lai kompetences nebūtu koncentrētas izveidojamajā centrā. Nedrīkst arī pieļaut paredzamā centra un tīkla darbību pārklāšanos ar pašreizējiem sadarbības mehānismiem un organizācijām.

1.4. EESK atbalsta sadarbības paplašināšanu ar industrijas aprindām, pamatojoties uz stingrām saistībām zinātnes un ieguldījumu jomā, tostarp nākotnē iekļaujot tās Valdē. Eiropas Komisijas, dalībvalstu un industrijas trīspusējās sadarbības gadījumā jāparedz tikai tādu trešo valstu uzņēmumu klātbūtne, kuri jau sen izveidoti Eiropas teritorijā un ir pilnībā iesaistīti Eiropas tehnoloģiskajā un industriālajā bāzē, turklāt uz tiem jāattiecina atbilstīgi pārbaudes un kontroles mehānismi, kā arī prasība par atbilstību savstarpīguma principam un pienākums ievērot slepenību.

1.5. Kiberdrošībai ir jābūt visu dalībvalstu kopējām saistībām, un tāpēc tām ir jāpiedalās Valdē saskaņā ar procedūrām, kas ir jānosaka. Kā dalībvalstu finansiālo ieguldījumu varētu izmantot ES līdzekļu piešķīrumu katrai no tām.

1.6. Priekšlikumā vajadzētu labāk paskaidrot, kā Centrs spēs iejaukties, lai koordinētu programmas "Digitālā Eiropa"un pamatprogrammas "Apvārsnis Eiropa"finansējumu, un jo īpaši saskaņā ar kādām pamatnostādnēm tiks sagatavoti un piešķirti iespējamie iepirkuma līgumi. Šis aspekts ir būtisks, lai izvairītos no dublēšanās vai pārklāšanās. Turklāt, lai palielinātu finansējumu, ir ieteicams paplašināt sinerģiju ar citiem ES finanšu instrumentiem (piemēram, reģionālajiem fondiem, struktūrfondiem, Eiropas infrastruktūras savienošanas instrumentu (EISI), Eiropas Aizsardzības fondu (EAF), *InvestEU* u. c.).

1.7. EESK uzskata, ka ir būtiski definēt Eiropas Centra un valstu centru sadarbības un attiecību veidus. Turklāt ir svarīgi, lai valstu centrus finansētu ES, vismaz attiecībā uz administratīvajām izmaksām, tādējādi veicinot administratīvo un kompetenču saskaņošanu nolūkā mazināt plaisu starp Eiropas valstīm.

1.8. Komiteja atkārtoti uzsver cilvēkkapitāla nozīmi un cer, ka Kompetenču centrs sadarbībā ar universitātēm, pētniecības centriem un augstākās izglītības centriem varēs veicināt izglītību un apmācību saskaņā ar izcilības standartiem, tostarp izmantojot īpašus augstāko un vidējo izglītības iestāžu kursus. Tāpat ir svarīgi nodrošināt īpašu atbalstu jaunuzņēmumiem un MVU.

1.9. EESK uzskata, ka būtiski ir sīkāk precizēt attiecīgās kompetences jomas un robežas starp Centra un Eiropas Savienības Tīklu un informācijas drošības aģentūras (*ENISA*) pilnvarām, skaidri nosakot sadarbības un savstarpējā atbalsta veidus un izvairoties no kompetenču pārklāšanās un darba dublēšanas. Līdzīgas problēmas rodas arī ar citām kiberdrošības struktūrām, piemēram, Eiropas Aizsardzības aģentūru (EAA), Eiropolu un ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienību (*CERT-EU*), un ir ieteicams izveidot virkni strukturēta dialoga mehānismu starp šīm dažādām struktūrām.

2. **Kiberdrošības pašreizējais raksturojums**

2.1. Kiberdrošība ir viens no ES darba kārtības galvenajiem jautājumiem, jo tas ir neaizstājams elements iestāžu, uzņēmumu un iedzīvotāju aizsardzībā, kā arī nepieciešams instruments demokrātijas stabilitātes nodrošināšanai. Starp visvairāk satraucošajām parādībām jāmin strauja ļaunprogrammatūru izplatības palielināšanās tīklā, izmantojot automātiskas sistēmas – no 130 tūkstošiem 2007. gadā līdz 8 miljoniem 2017. gadā. Turklāt Savienība ir kiberdrošības produktu un risinājumu neto importētājs, un tas rada ekonomiskās konkurētspējas un civilās un militārās drošības problēmas.

2.2. Kaut arī Eiropas Savienībai ir būtiskas zināšanas un pieredze kiberdrošības jomā, nozares industrija, universitātes un pētniecības centri joprojām ir sadrumstaloti, nesaskaņoti un atdalīti no kopējās attīstības stratēģijas. Tas ir saistīts ar to, ka netiek pietiekami atbalstītas attiecīgās kiberdrošības nozares (piemēram, enerģija, kosmoss, aizsardzība un transports), kā arī netiek veicināta sinerģija starp civilo un aizsardzības kiberdrošību.

2.3. Lai risinātu arvien pieaugošās problēmas, Savienība 2013. gadā izstrādāja kiberdrošības stratēģiju, ar kuru veicināt uzticamu, drošu un atvērtu kiberdrošības ekosistēmu ([1]). Pēc tam 2016. gadā tika pieņemti pirmie īpašie pasākumi tīklu un informācijas sistēmu drošībai ([2]). Šis virziens ir radījis publiskā un privātā sektora partnerību kiberdrošības jomā (*cPPP*).

2.4. 2017. gada kopīgajā paziņojumā "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību" ([3]) tika atzīts, ka ir jānodrošina būtisku kiberdrošības tehnoloģisko spēju saglabāšana un attīstīšana, lai aizsargātu digitālo vienoto tirgu un jo īpaši kritiskos tīklus un informācijas sistēmas, kā arī sniegtu svarīgākos kiberdrošības pakalpojumus.

([1]) JOIN(2013) 1 final.

([2]) Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

([3]) JOIN(2017) 450 final.

2.5. Tāpēc Savienībai ir jābūt spējīgai nodrošināt savu digitālo resursu un procesu aizsardzību un konkurēt pasaules kiberdrošības tirgū, līdz tā sasniedz stabilu un plašu digitālo autonomiju ([4]).

3. Eiropas Komisijas priekšlikumi

3.1. Kompetenču centra (turpmāk "Centra") mērķis ir sekmēt un koordinēt Nacionālo centru tīkla darbību, kā arī sniegt atbalstu kiberdrošības kompetenču kopienai, tādējādi veicinot kiberdrošības tehnoloģiskās darba kārtības virzību un atvieglojot iespējas izmantot šādi iegūtu lietpratību.

3.2. Konkrēti, Kompetenču centrs, piešķirot dotācijas un rīkojot iepirkumus, īstenos programmas "Digitālā Eiropa"un pamatprogrammas "Apvārsnis Eiropa"attiecīgās daļas. Ņemot vērā citur pasaulē veiktās ievērojamās investīcijas kiberdrošības jomā un vajadzību koordinēt un apvienot nozares resursus Eiropā, Kompetenču centru ierosināts veidot kā Eiropas partnerību ar divkāršu juridisko pamatu, kas tādējādi ļaus Savienībai, dalībvalstīm un/vai industrijai vienkāršāk veikt kopīgas investīcijas.

3.3. Priekšlikumā ir noteikts, ka Kompetenču centra un Tīkla darbībās dalībvalstīm jāsniedz proporcionāli atbilstošs ieguldījums. ES paredzētais finansējums ir aptuveni 2 miljardi EUR no programmas "Digitālā Eiropa"; no pamatprogrammas "Apvārsnis Eiropa"paredzētā summa vēl jānosaka; kopējais dalībvalstu ieguldījums ir vismaz ES ieguldījuma apmērā.

3.4. Galvenā lēmumu pieņemšanas struktūra ir Valde, kurā pārstāvētas visas dalībvalstis, taču balsošanas tiesības tajā ir tikai tām dalībvalstīm, kuras piedalās ar savu finansiālo ieguldījumu. Balsošanas mehānisms veidots pēc divkāršā balsu vairākuma principa, kas paredz, ka jābūt nodrošinātiem 75 % finansiālā ieguldījuma un 75 % balsu. Komisijai ir 50 % balsu. Lai uzturētu dialogu ar uzņēmumiem, patērētājiem un citām ieinteresētajām personām, Valdei palīdz Industriālā un zinātniskā konsultatīvā padome.

3.5. Cieši sadarbojoties ar Nacionālo koordinācijas centru tīklu un kiberdrošības kompetenču kopienu, Kompetenču centrs būtu galvenā īstenošanas struktūra attiecībā uz ES finanšu līdzekļiem, kas atvēlēti kiberdrošībai saskaņā ar ierosināto programmu "Digitālā Eiropa"un pamatprogrammu "Apvārsnis Eiropa".

3.6. Nacionālie koordinācijas centri būtu jāizvēlas dalībvalstīm. Šajos centros vajadzētu būt attīstītai vai arī tieši pieejamai tehnoloģiskai lietpratībai kiberdrošības jomā, jo īpaši tādās sfērās kā kriptogrāfija, IKT drošības pakalpojumi, ielaušanās atklāšana, sistēmu drošība, tīklu drošība, programmatūras un lietojumprogrammu drošība, kā arī drošības un privātuma cilvēciskie un sabiedriskie aspekti. Tāpat centriem būtu jāspēj efektīvi iesaistīties un nodrošināt koordināciju ar industriju un publisko sektoru, tostarp iestādēm, kas izraudzītas saskaņā ar Direktīvu (ES) 2016/1148.

4. Vispārīgas piezīmes

4.1. EESK atzinīgi vērtē Komisijas iniciatīvu un uzskata, ka tā ir stratēģiski nozīmīga kiberdrošības attīstībai un paredz īstenot lēmumus, kas 2017. gada septembrī pieņemti Tallinas samitā. Tajā valstu un valdību vadītāji aicināja Savienību "*līdz 2025. gadam kļūt par pasaules līderi kiberdrošības jomā, lai nodrošinātu mūsu pilsoņu, patērētāju un uzņēmumu uzticēšanos, pārliecību un aizsardzību tiešsaistē, kā arī nodrošinātu likumā reglamentētu bezmaksas internetu*".

4.2. EESK atkārtoti uzsver, ka notiek īsts un reāls kiberkarš, kas var apdraudēt politiskās, ekonomiskās un sociālās sistēmas, uzbrūkot iestāžu IT sistēmām, kritiskām infrastruktūrām (enerģētika, transports, bankas un finanšu iestādes) un uzņēmumiem, kā arī ar viltus ziņām ietekmējot vēlēšanu un demokrātijas procesus kopumā ([5]). Tāpēc ir nepieciešama augsta līmeņa izpratne, kā arī stingra un savlaicīga reakcija. Šo iemeslu dēļ ir jāizstrādā skaidra un labi pamatota industriālā kiberdrošības stratēģija kā neatņemams priekšnoteikums digitālās autonomijas sasniegšanai. EESK uzskata, ka darba programmā prioritāte jāpiešķir jomām, kas noteiktas Direktīvā (ES) 2016/1148, ko piemēro valsts vai privātiem uzņēmumiem, kuri sniedz būtiskus pakalpojumus, ņemot vērā to nozīmi sabiedrībā ([6]).

([4]) OV C 227, 28.6.2018., 86. lpp.

([5]) Informatīvais ziņojums "Plašsaziņas līdzekļu izmantošana sociālo un politisko procesu ietekmēšanai ES un Austrumu kaimiņvalstīs", *I. Vareikytė*, 2014.

([6]) OV C 227, 28.06.2018., 86. lpp.

4.3. Komiteja atzīmē, ka nevienā kiberdrošības stratēģijā nevar ignorēt jautājumu par visu lietotāju plašu informētību un drošu rīcību. Tādēļ katra tehnoloģiskā iniciatīva ir jāpapildina ar atbilstīgām informācijas un izpratnes veicināšanas kampaņām, lai veidotu digitālās drošības kultūru ([7]).

4.4. EESK atbalsta priekšlikuma vispārējos mērķus un apzinās, ka par īpašajiem darbības aspektiem būs jāveic turpmāka analīze. Tomēr, tā kā tā ir regula, Komiteja uzskata, ka pārvaldības, finansēšanas un jau noteiktu mērķu sasniegšanas konkrētie sensitīvie aspekti būtu jānosaka iepriekš. Svarīga nozīme ir tam, lai paredzamais tīkls un centrs būtu pēc iespējas lielākā mērā balstīts uz dalībvalstu kiberspējām un īpašajām zināšanām un lai kompetences nebūtu koncentrētas izveidojamajā centrā. Nedrīkst arī pieļaut paredzamā centra un tīkla darbību pārklāšanos ar pašreizējiem sadarbības mehānismiem un organizācijām.

4.5. EESK atgādina, ka atzinumā TEN/646 par kiberdrošības aktu ([8]) tā ierosināja trīspusēju PPP sadarbību starp Eiropas Komisiju, dalībvalstīm un industriju (tai skaitā arī MVU), savukārt pašreizējā struktūra, kuras juridiskā forma ir jāuzlabo, būtībā paredz publiskā un privātā sektora partnerību starp Eiropas Komisiju un dalībvalstīm.

4.6. EESK atbalsta sadarbības paplašināšanu ar industrijas aprindām, pamatojoties uz stingrām saistībām zinātnes un ieguldījumu jomā, tostarp nākotnē iekļaujot tās Valdē. Industriālās un zinātniskās konsultatīvās padomes izveide nevar garantēt pastāvīgu dialogu ar uzņēmumiem, patērētājiem un citām ieinteresētajām personām. Turklāt Komisijas ieskicētajā jaunajā kontekstā nav skaidrs, kāda loma būs pēc Komisijas ierosmes 2016. gada jūnijā izveidotajai Eiropas Kiberdrošības organizācijai (*ECSO*), kas partnerībā veic tādas pašas funkcijas kā Komisija un kuras tīkla kapitālu un zināšanas nevajadzētu izkliedēt.

4.6.1. Trīspusējas sadarbības gadījumā ir svarīgi pievērst uzmanību trešo valstu uzņēmumiem. EESK jo īpaši uzsver, ka šai sadarbībai vajadzētu būt balstītai uz stingru mehānismu, lai novērstu tādu trešo valstu uzņēmumu klātbūtni, kuri varētu apdraudēt Savienības drošību un autonomiju. Šajā sakarā būtu jāpiemēro arī attiecīgās klauzulas, kas definētas Eiropas aizsardzības rūpniecības attīstības programmā ([9]).

4.6.2. Tajā pašā laikā EESK atzīst, ka daži trešo valstu uzņēmumi, kuri jau sen izveidoti Eiropas teritorijā un ir pilnībā iesaistīti Eiropas tehnoloģiskajā un industriālajā bāzē, varētu būt ļoti noderīgi ES projektiem, un tiem vajadzētu būt iespējai piekļūt šiem projektiem ar nosacījumu, ka dalībvalstis uz šādiem uzņēmumiem attiecina atbilstīgus pārbaudes un kontroles mehānismus un ka tie ievēro savstarpīguma principu un pienākumu ievērot slepenību.

4.7. Kiberdrošībai ir jābūt visu dalībvalstu kopējām saistībām, un tāpēc tām ir jāpiedalās Valdē saskaņā ar procedūrām, kas ir jānosaka. Tāpat svarīgi ir, lai visas dalībvalstis finansiāli un pienācīgā veidā atbalstītu Komisijas iniciatīvu. Kā dalībvalstu finansiālo ieguldījumu varētu izmantot ES līdzekļu piešķirumu katrai no tām.

4.8. EESK piekrīt, ka katra dalībvalsts var iecelt savu pārstāvi Eiropas Kompetenču centra Valdē. Komiteja iesaka skaidri definēt valstu pārstāvju kompetences profilus, integrējot stratēģisko un tehnoloģisko lietpratību ar vadības, administratīvajām un budžeta veidošanas prasmēm.

4.9. Priekšlikumā vajadzētu labāk paskaidrot, kā Centrs varēs iesaistīties, lai koordinētu programmas "Digitālā Eiropa"un pamatprogrammas "Apvārsnis Eiropa"finansējumu, par ko joprojām notiek sarunas, un jo īpaši saskaņā ar kādām pamatnostādnēm tiks sagatavoti un piešķirti iespējamie iepirkuma līgumi. Šis aspekts ir būtisks, lai izvairītos no dublēšanās vai pārklāšanās. Turklāt, lai palielinātu finansējumu, ir ieteicams paplašināt sinerģiju ar citiem ES finanšu instrumentiem (piemēram, reģionālajiem fondiem, struktūrfondiem, EISI, EAF, *InvestEU*). Komiteja cer, ka Nacionālo centru tīkls tiks iesaistīts līdzekļu pārvaldē un koordinācijā.

([7]) OV C 227, 28.06.2018., 86. lpp.
([8]) OV C 227, 28.06.2018., 86. lpp.
([9]) COM(2017) 294.

4.10. EESK atzīmē, ka konsultatīvās komitejas sastāvā vajadzētu būt 16 locekļiem un ka nav izklāstīti mehānismi, kā šī komiteja varētu vērsties pie uzņēmumiem, universitātēm, pētniecības centriem un patērētājiem. Komiteja uzskata: būtu lietderīgi un atbilstīgi, ka minētās komitejas locekļus raksturotu augsts zināšanu līmenis šajā jomā un tie līdzsvaroti pārstāvētu dažādas iesaistītās nozares.

4.11. EESK uzskata, ka ir svarīgi definēt Eiropas Centra un valstu centru sadarbības un attiecību veidus. Turklāt ir svarīgi, lai valstu centrus finansētu ES, vismaz attiecībā uz administratīvajām izmaksām, tādējādi veicinot administratīvo un kompetenču saskaņošanu nolūkā mazināt plaisu starp Eiropas valstīm.

4.12. Saskaņā ar saviem iepriekšējiem atzinumiem ([10]) EESK uzsver izglītības un cilvēkresursu apmācības nozīmi kiberdrošības jomā atbilstoši izcilības standartiem, tostarp īpašos skolu, universitātes un pēcdiploma studiju kursos. Tāpat ir svarīgi nodrošināt pienācīgu finansiālu atbalstu nozares MVU un jaunizveidotajiem uzņēmumiem ([11]), kas ir būtiski jaunāko pētījumu attīstībai.

4.13. EESK uzskata, ka būtiski ir sīkāk precizēt attiecīgās kompetences jomas un robežas starp Centra un *ENISA* pilnvarām, skaidri nosakot sadarbības un savstarpējā atbalsta veidus un izvairoties no kompetenču pārklāšanās un darba dublēšanas ([12]). Regulas priekšlikumā paredzēts, ka Valdē kā pastāvīgs novērotājs piedalās *ENISA* pārstāvis, taču šāda klātbūtne negarantē strukturētu dialogu starp abām struktūrām. Līdzīgas problēmas rodas arī ar citām kiberdrošības struktūrām, piemēram, EAA, Eiropolu un *CERT-EU*. Šajā sakarā interesants šķiet saprašanās memorands, kas 2018. gada maijā parakstīts starp ENISA, EAA, Eiropolu un *CERT-EU*.

Briselē, 2019. gada 23. janvārī

Eiropas Ekonomikas un sociālo lietu komitejas

priekšsēdētājs

Luca JAHIER

([10]) OV C 451, 16.12.2014., 25. lpp.
([11]) OV C 227, 28.06.2018., 86. lpp.
([12]) OV C 227, 28.06.2018., 86. lpp.