Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Priekšlikums Eiropas Parlamenta un Padomes regulai par *ENISA* – ES Kiberdrošības aģentūru – un Regulas (ES) 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akts")"

(COM(2017) 477 final/2 – 2017/0225 (COD))

(2018/C 227/13)

Ziņotājs: **Alberto MAZZOLA**

Līdzziņotājs: **Antonio LONGO**

Apspriešanās	Eiropas Parlaments, 23.10.2017.
	Eiropas Savienības Padome, 25.10.2017.
Juridiskais pamats	Līguma par Eiropas Savienības darbību 114. pants
Atbildīgā specializētā nodaļa	Transporta, enerģētikas, infrastruktūras un informācijas sabiedrības specializētā nodaļa
Pieņemts specializētās nodaļas sanāksmē	5.2.2018.
Datums, kad pieņemts plenārsesijā	14.2.2018.
Plenārsesija Nr.	532
Balsojuma rezultāts	206/1/2
(par/pret/atturas)	

1. **Secinājumi un priekšlikumi**

1.1. EESK uzskata, ka *ENISA* jaunās pastāvīgās pilnvaras, ko ierosinājusi Komisija, būtiski palīdzēs uzlabot Eiropas sistēmu izturētspēju. Tomēr ar to saistītais *ENISA* piešķirtais provizoriskais budžets un resursi nebūs pietiekami aģentūras pilnvaru izpildei.

1.2. EESK iesaka visām dalībvalstīm izveidot atsevišķu un *ENISA* pielīdzināmu partneriestādi, jo vairums dalībvalstu to vēl nav izdarījušas.

1.3. EESK arī uzskata, ka no spēju veidošanas viedokļa par *ENISA* prioritāti būtu jānosaka pasākumi, kas vērsti uz atbalstu e-pārvaldei ([1]). Svarīga ir personu, organizāciju un objektu ES un pasaules mēroga digitālā identitāte, un par prioritāti būtu jāizvirza identitātes zādzības un tiešsaistes krāpniecības apkarošana.

1.4. EESK iesaka, lai *ENISA* sniedz regulārus ziņojumus par dalībvalstu kibergatavību, primāri pievēršoties Kiberdrošības direktīvas II pielikumā nosauktajām jomām. Ikgadējās Eiropas kibermācībās būtu jānovērtē dalībvalstu gatavība un Eiropas mehānisma, kas paredzēts reaģēšanai kiberkrīžu gadījumā, efektivitāte, kā arī jāsagatavo ieteikumi.

1.5. EESK atbalsta ierosinājumu izveidot kiberdrošības kompetences tīklu. Šo tīklu uzturētu Kiberdrošības pētniecības un kompetences centrs. Minētais tīkls varētu stiprināt Eiropas digitālo suverenitāti, attīstīdams konkurētspējīgu Eiropas rūpniecisko pamatu svarīgākajām tehnoloģiskajām spējām, balstoties uz tādas līgumiskas publiskā un privātā sektora partnerības darbu, kura būtu jāattīsta par trīspusēju kopuzņēmumu.

1.6. Viens no svarīgākajiem kibernegadījumu iemesliem ir cilvēka faktors. EESK uzskata, ka ir jāveido spēcīgas pamata kiberprasmes un jāuzlabo kiberhigiēna, šajā nolūkā sabiedrībā un uzņēmumos izmantojot arī izpratnes uzlabošanas kampaņas. EESK atbalsta ES sertificētu mācību programmu vidējās izglītības iestādēm un profesionāļiem.

([1]) Digitālais vienotais tirgus / vidusposma pārskats.

1.7. EESK uzskata, ka Eiropas digitālajā vienotajā tirgu ir nepieciešama arī vienveidīga kiberdrošības noteikumu interpretācija, tostarp savstarpēja atzīšana starp dalībvalstīm, un ka kopīgas pamatprasības varētu nodrošināt dažādām nozarēm paredzēts sertifikācijas satvars un sertifikācijas sistēmas. Tomēr atšķirīgām nozarēm to darbības veida dēļ ir jānodrošina atšķirīgas pieejas. Tāpēc EESK uzskata, ka šajā procesā būtu jāiesaista ES nozaru aģentūras (Eiropas Aviācijas drošības aģentūra (*EASA*), Eiropas Dzelzceļa aģentūra (*ERA*), Eiropas Zāļu aģentūra (*EMA*) u. c.) un dažos gadījumos, ar *ENISA* piekrišanu, lai nodrošinātu saskaņotību, tām būtu jādeleģē kiberdrošības sistēmu izstrāde. IT drošības standartu obligātais minimums būtu jāpieņem sadarbībā ar Eiropas Standartizācijas komiteju, Eiropas Elektrotehnikas standartizācijas komiteju un Eiropas telesakaru standartu institūtu (*CEN, Cenelec* un ETSI).

1.8. Veidojot iecerēto Eiropas Kiberdrošības sertifikācijas grupu, ko atbalsta *ENISA*, par tās dalībniekiem būtu jākļūst valstu sertifikācijas pārraudzības iestādēm, privātā sektora ieinteresētajām personām, tostarp operatoriem no dažādām pielietojuma jomām, kā arī zinātnes aprindu un pilsoniskās sabiedrības dalībniekiem.

1.9. EESK uzskata, ka minētajai aģentūrai, Komisijas uzdevumā veicot revīzijas un inspekcijas, būtu jāpārrauga valstu sertifikācijas uzraudzības iestāžu sniegums un lēmumu pieņemšana un ka regulā būtu jānosaka pienākumi un sankcijas par standartu neievērošanu.

1.10. EESK uzskata, ka no sertifikācijas nevar izslēgt pienācīgu marķēšanas sistēmu, kas būtu jāpiemēro arī importētiem produktiem, lai palielinātu patērētāju uzticēšanos.

1.11. Eiropai būtu jāpalielina ieguldījumi, kombinējot dažādus ES fondus, valstu fondus un privātā sektora investīcijas un spēcīgā publiskā un privātā sektora sadarbībā virzoties uz stratēģiskiem mērķiem, tostarp pašreizējā un nākamajā pētniecības pamatprogrammā izveidojot ES kiberdrošības fondu inovācijai, pētniecībai un izstrādei. Eiropai turklāt vajadzētu izveidot fondu kiberdrošības pasākumu īstenošanai, atverot jaunu finansējuma atzaru pašreizējā un nākamajā Eiropas infrastruktūras savienošanas instrumentā, kā arī nākamajā ESIF 3.0.

1.12. EESK skatījumā ir nepieciešams drošības līmeņa obligātais minimums "parastām" "cilvēku interneta" ierīcēm. Šajā gadījumā sertificēšana ir galvenā metode augstāka drošības līmeņa nodrošināšanai. Lietu interneta drošībai vajadzētu būtu prioritātei.

2. **Kiberdrošības pašreizējais satvars**

2.1. Kiberdrošība ir kritiski svarīga gan labklājībai un valsts drošībai, gan arī mūsu demokrātijas, brīvību un vērtību funkcionēšanai. "Kiberdrošība ir ekosistēma, kurā likumiem, organizācijām, prasmēm, sadarbībai un tehniskai īstenošanai ir jābūt harmonijā, un tikai tad tā būs visefektīvākā," norādīts ANO Globālās kiberdrošības indeksā. Tur arī piebilsts, ka kiberdrošība "ir jautājums, pret kuru valstu lēmumu pieņēmēji sāk izturēties arvien nopietnāk".

2.2. Interneta revolūcijas dēļ arvien lielāka kļūst nepieciešamība pēc drošas ekosistēmas. Šī revolūcija ir ne tikai mainījusi uzņēmumu un patērētāju (B2C) attiecības tādās jomās kā mediji, mazumtirdzniecība un finanšu pakalpojumi; tā pārveido arī ražošanu, enerģētiku, lauksaimniecību, transportu un citas ekonomikas ražojošās nozares, kuras kopumā veido aptuveni divas trešdaļas no pasaules iekšzemes kopprodukta, kā arī sabiedrisko pakalpojumu infrastruktūru un cilvēku attiecības ar publisko pārvaldi.

2.3. Digitālā vienotā tirgus stratēģija ir vērsta uz piekļuves uzlabošanu precēm, pakalpojumiem un saturam, digitālajiem tīkliem un pakalpojumiem piemērota tiesiskā regulējuma veidošanu un uz to ieguvumu izmantošanu, ko sniedz uz datiem balstīta ekonomika. Ir aplēsts, ka šī stratēģija ES ekonomikai varētu ienest 415 miljardus EUR gadā. Tiek prognozēts, ka līdz 2022. gadam privātajā sektorā pietrūks 350 000 speciālistu ar profesionālām kiberdrošības prasmēm ([2]).

([2]) OV JOIN/2017/0450 final.

2.4. 2014. gadā veiktā pētījumā tika lēsts, ka kibernoziedzības ekonomiskā ietekme 2013. gadā sasniedza 0,41 % no ES IKP (t. i. aptuveni 55 miljardus EUR) ([3]).

2.5. Īpašais Eirobarometra apsekojums 464a par eiropiešu attieksmi pret kiberdrošību liecina, ka 73 % interneta lietotāju uztrauc fakts, ka tīmekļa vietnes varētu tiešsaistē sniegto personisko informāciju neuzglabāt droši, un 65 % uztrauc tas, ka publiskās iestādes to varētu neuzglabāt droši. Lielākā daļa respondentu ir nobažījušies, ka viņi varētu kļūt par dažādu veidu kibernoziegumu upuriem, bet visvairāk viņus biedē ļaunprogrammatūra viņu ierīcēs (69 %), identitātes zādzība (69 %), kā arī krāpšana ar bankas kartēm un krāpšana internetbankā (66 %) ([4]).

2.6. Līdz šim tiesiskais regulējums nav spējis tikt līdzi digitālajai inovācijai, un piemērots regulējums soli pa solim tiek veidots ar dažādiem tiesību aktiem: Elektronisko sakaru kodeksa pārskatīšana, Vispārīgā datu aizsardzības regula, Direktīva par tīklu un informācijas sistēmu drošību (Kiberdrošības direktīva), Regula par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū (*eIDAS* regula), ES un ASV privātuma vairogs, Direktīva par krāpšanas un viltošanas apkarošanu attiecībā uz bezskaidras naudas maksāšanas līdzekļiem u. c.

2.7. Līdztekus "ES Kiberdrošības aģentūrai" *ENISA* kiberdrošības jautājumus risina daudzas citas organizācijas: Eiropols; *Cert-EU* (Eiropas Savienības datorapdraudējumu reaģēšanas vienība); ES Izlūkošanas un situāciju centrs (*EU INTCEN*); Eiropas Aģentūra lielapjoma IT sistēmu darbības pārvaldībai brīvības, drošības un tiesiskuma telpā (*eu-LISA*); informācijas apmaiņas un analīzes centri (*ISAC*), Eiropas Kiberdrošības organizācija (*ECSO*), Eiropas Aizsardzības aģentūra (EAA); NATO Kopējais kiberaizsardzības izcilības centrs un ANO valdību ekspertu grupa (ANO valdību ekspertu grupa attiecībā uz attīstību informācijas un telesakaru jomā starptautiskās drošības kontekstā).

2.8. Integrēta drošība ir svarīgs augstas kvalitātes preču un pakalpojumu nosacījums: viedierīces nemaz nav tik viedas, ja tās nav drošas. Tas pats attiecas uz viedām automašīnām, viedām pilsētām un viedām slimnīcām – tām visām ir nepieciešama integrēta drošība attiecībā uz ierīcēm, sistēmām, arhitektūru un pakalpojumiem.

2.9. 2017. gada 19. un 20. oktobrī Eiropadome aicināja pieņemt vienotu pieeju ES kiberdrošības jomā atbilstoši ierosinātajai reformu paketei, aicinot īstenot kopēju pieeju kiberdrošībai: "digitālajai pasaulei ir vajadzīga uzticēšanās, un uzticēšanos var panākt tikai tad, ja mēs nodrošinām proaktīvāku integrēto drošību visās digitālajās rīcībpolitikās, gādājam par produktu un pakalpojumu adekvātu drošības sertifikāciju un palielinām savu spēju novērst, nepieļaut un atklāt kiberuzbrukumus un reaģēt uz tiem" ([5]).

2.10. Eiropas Parlaments 2017. gada 17. maija rezolūcijā "uzsver nepieciešamību pēc drošības no viena gala līdz otram visā finanšu pakalpojumu vērtības ķēdē; norāda uz dažādajiem lielajiem riskiem, ko rada kiberuzbrukumi, kuri vērsti pret mūsu finanšu tirgus infrastruktūru, lietu internetu, valūtām un datiem; (..) aicina EUI (..) regulāri pārskatīt spēkā esošos standartus, kas attiecas uz finanšu institūciju ar IKT saistītajiem riskiem; turklāt (..) aicina EUI izstrādāt pamatnostādnes par šādu risku uzraudzību; uzsver (ka), liela nozīme ir tehnoloģiskajai zinātībai (EUI); (..) ([6])."

2.11. EESK jau vairākkārt ir bijušas iespējas pievērsties šim tematam ([7]), tostarp Tallinas samita laikā rīkotajā konferencē par e-pārvaldes turpmāko attīstību ([8]), un tā ir izveidojusi pastāvīgu izpētes grupu "Digitalizācijas programma".

([3]) Komisijas dienestu darba dokuments – ietekmes novērtējums, kas pievienots dokumentam "Priekšlikums Eiropas Parlamenta un Padomes regulai", 1/6 daļa, 21. lpp., Briselē, 2017. gada 13. septembrī.

([4]) Īpašais Eirobarometra apsekojums 464a – *Wave EB87.4* – Eiropiešu attieksme pret kiberdrošību, 2017. gada septembris.

([5]) Eiropadomes 2017. gada 19. oktobra secinājumi.

([6]) EP rezolūcija 17.05.2017. – A8-0176/2017.

([7]) Digitālais vienotais tirgus / vidusposma pārskats. OV C 75, 10.3.2017., 124. lpp., OV C 246, 28.7.2017., 8. lpp., OV C 345, 13.10.2017., 52. lpp., OV C 288, 31.8.2017., 62. lpp., OV C 271, 19.9.2013., 133. lpp.

([8]) EESK paziņojums presei Nr.°31/2017 Pilsoniskās sabiedrības debates ar nākamo ES prezidentvalsti Igauniju par e-pārvaldi un kiberdrošību: https://www.eesc.europa.eu/en/news-media/press-releases/civil-society-debates-e-government-and-cybersecurity-incomingestonian-presidency.

3. **Komisijas priekšlikumi**

3.1. Kiberdrošības tiesību aktu kopums ietver kopīgu paziņojumu, ar kuru tiek pārskatīta iepriekšējā Eiropas kiberdrošības stratēģija (2013), kā arī Kiberdrošības aktu, kas vērsts uz *ENISA* jaunajām pilnvarām un ierosināto sertifikācijas satvaru.

3.2. Stratēģijas struktūru veido trīs galvenās nodaļas: noturība, novēršana un starptautiskā sadarbība. Nodaļa par novēršanu galvenokārt vērsta uz kibernoziedzības jautājumiem, tostarp uz Budapeštas konvenciju. Starptautiskās sadarbības nodaļā skatīta kiberaizsardzība, kiberdiplomātija un sadarbība ar NATO.

3.3. Priekšlikumā ir izklāstītas jaunas iniciatīvas, piemēram:

— spēcīgākas ES kiberdrošības aģentūras izveide,

— ES mēroga kiberdrošības sertifikācijas sistēmas ieviešana,

— ātra Direktīvas par tīklu un informācijas sistēmu drošību (TID direktīvas) īstenošana.

3.4. Nodaļā par noturību piedāvāti ar kiberdrošību saistīti pasākumi, kas konkrēti vērsti uz: tirgus jautājumiem, TID direktīvu, ātru reakciju ārkārtas situācijās, ES kompetences veidošanu, izglītību un apmācību kiberprasmju un kiberhigiēnas jomā, kā arī izpratni.

3.5. Līdztekus tam ar Kiberdrošības aktu ir ierosināts izveidot Eiropas kiberdrošības sertifikācijas satvaru IKT produktiem un pakalpojumiem.

3.6. Kiberdrošības aktā ierosināts arī nostiprināt lomu, ko *ENISA* pilda kā ES kiberdrošības aģentūra, un piešķirt tai pastāvīgas pilnvaras. Papildus pašreizējiem uzdevumiem plānots, ka *ENISA* pildīs jaunus atbalsta un koordinācijas uzdevumus, kas saistīti ar atbalstu TID direktīvas, ES kiberdrošības stratēģijas, plāna (*Blueprint*) īstenošanai, spēju veidošanu, zināšanu, informētības un izpratnes veicināšanu, tādus ar tirgu saistītus uzdevumus kā atbalsts standartizācijai un sertifikācijai, pētniecībai un inovācijai, Eiropas mēroga kiberdrošības mācībām un sekretariāta nodrošināšana datordrošības incidentu reaģēšanas vienības (*CSIRT*) tīklam.

4. **Vispārīgas piezīmes – pārskats**

4.1. ***Konteksts: noturība***

4.1.1. *Vienots kiberdrošības tirgus*

Rūpības pienākums. Ierosinātais "rūpības pienākuma" princips, kas kopīgajā paziņojumā minēts saistībā ar drošu dzīves cikla izstrādes procesu izmantošanu, ir interesanta koncepcija, kas būtu jāattīsta kopīgi ar ES rūpniecību un kas varētu palīdzēt nonākt pie visaptverošas pieejas attiecībā uz atbilstību ES tiesību aktiem. Turpmākajā attīstībā būtu jāņem vērā drošība pēc noklusējuma.

Atbildība: ar sertifikācijas palīdzību būs vieglāk noteikt atbildību strīda gadījumā.

4.1.2. TID direktīva: enerģētika, transports, bankas/finanses, veselība, ūdens apgāde, digitālā infrastruktūra, e-tirdzniecība.

EESK skatījumā pilna un efektīva TID direktīvas īstenošana ir svarīga, lai nodrošinātu kritiski svarīgo nacionālo sektoru noturību.

EESK ir pārliecināta, ka dalīšanās ar informāciju starp publiskā un privātā sektora dalībniekiem būtu jāstiprina, izmantojot informācijas apmaiņas un analīzes centrus (*ISAC*). Balstoties uz pašlaik izmantotā mehānisma novērtēšanu/analīzi, būtu jāizveido piemērots mehānisms konfidenciālas informācijas drošai apmaiņai *ISAC* ietvaros, kā arī starp *CSIRT* un *ISAC*.

4.1.3. *Steidzama reaģēšana ārkārtas situācijās*

Kiberdrošības plāna pieeja nodrošinātu efektīvu procesu, kas ES un dalībvalsts līmenī ļautu operatīvi reaģēt uz plaša mēroga incidentu. Komiteja uzsver nepieciešamību iesaistīt privāto sektoru; operatīvās reaģēšanas mehānismā būtu jāņem vērā arī pamatpakalpojumu sniedzēji, jo viņi varētu sniegt vērtīgu informāciju par draudiem un/vai atbalstu draudu atklāšanā vai novēršanā un plaša mēroga krīžu gadījumā.

Kopīgajā paziņojumā ir ierosināts kiberincidentus integrēt ES krīžu pārvarēšanas mehānismos. Lai gan EESK izprot, ka uzbrukuma gadījumā ir vajadzīga kolektīva reakcija un solidaritāte, ir nepieciešama labāka izpratne, kā to īstenot, jo kiberdraudi parasti izplatās starp valstīm. Dalīties ar instrumentiem, kas tiek izmantoti ārkārtas situācijās valstīs, lokālas vajadzības gadījumā būtu iespējams tikai daļēji.

4.1.4. *ES kompetences attīstīšana*

Lai ES patiešām būtu konkurētspējīga pasaules mērogā un lai izveidotu stabilu tehnoloģisko bāzi, ir svarīgi izveidot saskaņotu ilgtermiņa satvaru, kas aptvertu visus kiberdrošības vērtību ķēdes posmus. Šajā saistībā, lai veidotu Eiropas kiberdrošības vērtību ķēdi, izšķiroši svarīga ir Eiropas reģionālo ekosistēmu sadarbība. EESK atzinīgi vērtē ierosinājumu izveidot kiberdrošības kompetences tīklu.

Ar šā tīkla palīdzību būtu iespējams atbalstīt Eiropas digitālo suverenitāti, veidojot konkurētspējīgu Eiropas rūpniecības bāzi un mazinot atkarību no zinātības, kas pamattehnoloģiju spēju jomā ir izveidota ārpus ES, nodrošināt tehniskas mācības, seminārus un pat būtiskas kiberhigiēnas mācības profesionāļiem un neprofesionāļiem, kā arī, balstoties uz līgumiskās PPP darbu, stiprināt nacionālo publiskā un privātā sektora organizāciju tīkla veidošanu, lai veicinātu tirgus attīstību Eiropā. "Līgumiskās PPP pilnveides rezultātā ir jānotiek tās optimizācijai, adaptācijai un ekspansijai" (EE-BG-AT triju prezidentvalstu Kiberdrošības darba programma), izveidojot trīspusēju (Komisija, dalībvalstis, uzņēmumi) kopuzņēmumu.

Lai tīkls būtu efektīvs un Eiropas līmenī sasniegtu ierosinātos mērķus, tā pamatā vajadzētu būt labi definētai pārvaldības sistēmai.

Eiropas līmenī šis tīkls būtu jāatbalsta Kiberdrošības pētniecības un kompetences centram, kas savienotu pašreizējos valstu kompetences centrus visā ES. Kiberdrošības pētniecības un kompetences centram būtu ne tikai jākoordinē un jāpārvalda pētniecība tāpat kā citos kopuzņēmumos, bet arī jāpaver efektīvas attīstības iespējas Eiropas kiberdrošības ekosistēmai, kas veicinātu ES inovācijas ieviešanu un izvēršanu.

4.2. ***Konteksts: novēršana***

4.2.1. Kibernoziedzības apkarošana ir valsts un Eiropas līmeņa augsta prioritāte, kuras īstenošanā nepieciešama spēcīga politiskā apņemšanās. Novēršanas darbības būtu jāveic, balstoties uz spēcīgu publiskā un privātā sektora partnerību, lai izveidotu efektīvu informācijas un ekspertzināšanu apmaiņu gan valsts, gan Eiropas līmenī. Būtu jāizskata iespēja paplašināt Eiropola darbību datorkriminālistikā un kiberpārraudzībā.

4.3. ***Konteksts: starptautiskā sadarbība***

4.3.1. Uzticēšanās pilnas sadarbības veidošana un uzturēšana ar trešām valstīm kiberdiplomātijas un uzņēmējdarbības partnerības jomā ir priekšnosacījums Eiropas spējai veikt preventīvus pasākumus pret liela mēroga kiberuzbrukumiem, tos novērst un reaģēt to gadījumā. Eiropai būtu jāstiprina sadarbība ar ASV, Ķīnu, Izraēlu, Indiju un Japānu. Modernizējot ES eksporta kontroli, būtu jāizvairās no cilvēktiesību pārkāpumiem un tehnoloģiju ļaunprātīgas izmantošanas, kas kaitē pašas ES drošībai, bet būtu arī jārūpējas, lai ES rūpniecība neciestu trešo valstu piedāvājumu dēļ. Attiecībā uz pievienošanās valstīm būtu jāparedz *ad hoc* stratēģija, lai tās sagatavotos sensitīvu datu pārrobežu apmaiņai, un būtu jāparedz arī iespēja tām novērotāja statusā piedalīties dažās darbībās *ENISA* valstīs – tās varētu sarindot atkarībā no gatavības cīnīties pret kibernoziedzību, un varētu sagatavot arī "melno sarakstu".

4.3.2. EESK atzinīgi vērtē kiberaizsardzības iekļaušanu iespējamā ES Kiberdrošības kompetences centra ieplānotajā otrajā posmā. Šā iemesla dēļ Eiropa tikmēr varētu pievērsties divējāda lietojuma kompetenču veidošanai, tostarp izmantot Eiropas Aizsardzības fondu un nodarboties ar kiberaizsardzības mācību un izglītības platformas izveidi, kas paredzēta 2018. gadā. Ņemot vērā abās pusēs apzināto potenciālu un draudus, EESK uzskata, ka ir jāattīsta ES un NATO sadarbība, un Eiropas rūpniecībai ir uzmanīgi jāseko līdzi ES un NATO sadarbības norisēm kiberdrošības standartu paaugstinātas sadarbspējas jomā un citām sadarbības formām ES pieejas kiberaizsardzībai kontekstā.

4.4. ***ES sertifikācijas satvars***

4.4.1. EESK uzskata, ka Eiropai ir jārisina kiberdrošības sadrumstalotības problēma, interpretējot noteikumus vienveidīgi, tostarp izmantojot savstarpēju atzīšanu starp dalībvalstīm atbilstīgi vienotam satvaram, lai atvieglotu digitālā vienotā tirgus aizsardzību. Sertifikācijas satvarā varētu noteikt kopīgas pamatprasības (attiecīgā gadījumā ar īpašiem noteikumiem augstākos līmeņos), tādējādi nodrošinot sinerģiju starp vertikāliem sektoriem un mazinot pašreizējo sadrumstalotību.

4.4.2. EESK atzinīgi vērtē ES kiberdrošības sertifikācijas satvara un sertifikācijas shēmu izveidi dažādām nozarēm, balstoties uz atbilstīgām prasībām un sadarbībā ar galvenajām ieinteresētajām personām. Tomēr būtu jāņem vērā tādi svarīgi elementi kā laiks līdz laišanai tirgū un sertifikācijas izmaksas, kā arī kvalitāte un drošība. Sertifikācijas shēmas tiks izveidotas ar mērķi palielināt drošību atbilstoši pašreizējām vajadzībām un zināšanām par apdraudējumu: lai varētu veikt nepieciešamo aktualizēšanu, šīs shēmas būtu jāveido elastīgas un paplašināmas. Atšķirīgās nozarēs to darbības veida dēļ ir jānodrošina dažādas pieejas. Tāpēc EESK uzskata, ka procesā būtu jāiesaista ES nozaru aģentūras (*EASA*, *EBA*, *ERA*, *EMA* u. c.) un dažos gadījumos, ar *ENISA* piekrišanu – lai izvairītos no pārklāšanās un saskaņotības trūkuma – tām būtu jādeleģē kiberdrošības shēmu izstrāde.

4.4.3. Komitejai ir svarīgi, lai sertifikācijas satvara pamatā būtu kopīgi definēti un iespēju robežās starptautiski atzīti Eiropas kiberdrošības un IKT standarti. Attiecībā uz grafiku un valstu prerogatīvām ES standartu obligātais minimums IT drošības jomā būtu jāpieņem sadarbībā ar *CEN*/*Cenelec*/ETSI. Profesionālie standarti būtu vērtējami pozitīvi, taču tiem nevajadzētu būt tiesiski saistošiem vai ierobežot konkurenci.

4.4.4. Skaidra ir nepieciešamība atbildību saistīt ar dažādiem apdrošināšanas līmeņiem, kas balstīti uz apdraudējuma ietekmi. Dialoga uzsākšana ar apdrošināšanas uzņēmumiem varētu pozitīvi ietekmēt efektīvu kiberdrošības prasību pieņemšanu atkarībā no piemērošanas jomas. EESK skatījumā uzņēmumi, kuri tiecas pēc "augsta apliecinājuma līmeņa", būtu jāatbalsta un jāstimulē, īpaši attiecībā uz dzīvībai svarīgām ierīcēm un sistēmām.

4.4.5. Ņemot vērā kopš Direktīvas 85/374/EEK ([9]) pieņemšanas aizgājušo laiku un pašreizējās tehnoloģiskās norises, EESK aicina Komisiju apsvērt, vai būtu lietderīgi direktīvas darbības jomā iekļaut dažus scenārijus, kas izklāstīti izskatāmajā regulas priekšlikumā, lai garantētu drošākus produktus ar augstu aizsardzības līmeni.

4.4.6. EESK uzskata, ka iecerētās un *ENISA* atbalstītās Eiropas Kiberdrošības sertifikācijas grupas sastāvā vajadzētu būt valstu sertifikācijas pārraudzības iestādēm, privātā sektora ieinteresētajām personām un operatoriem no dažādām pielietojuma jomām, lai nodrošinātu visaptverošu sertifikācijas shēmu veidošanu. Papildus būtu jāparedz sadarbība starp šo grupu un sektora pārstāvības apvienībām no ES/EEZ (piemēram, līgumiskās PPP, banku, transporta, enerģētikas joma, federācijas u. c.), nozīmējot ekspertus. Šai grupai būtu jāspēj vērtēt Eiropas sasniegumus sertifikācijā (galvenokārt pamatojoties uz *SOG-IS* savstarpējās atzīšanas nolīgumu, valstu shēmām un privātām shēmām) un jātiecas aizsargāt Eiropas konkurētspējas priekšrocības.

([9]) OV L 210, 7.8.1985, 29. lpp.

4.4.7. EESK ierosina šai ieinteresēto personu grupai uzdot kopīgi ar Eiropas Komisiju sagatavot sertifikācijas shēmas. Nozaru prasības arī būtu jānosaka, savstarpēji vienojoties publiskajām un privātajām (lietotāji un pakalpojumu sniedzēji) ieinteresētajām personām.

4.4.8. Grupai turklāt būtu regulāri jāpārskata sertifikācijas shēmas, izskatot katras nozares prasības un nepieciešamības gadījumā shēmas jāpielāgo.

4.4.9. EESK atbalsta atteikšanos no valstu sertifikācijas shēmām, kad būs ieviesta Eiropas shēma, kā ierosināts regulas 49. pantā. vienotais tirgus nevar darboties ar atšķirīgiem un konkurējošiem valstu noteikumiem. Tāpēc EESK iesaka uzskaitīt visas valstu shēmas.

4.4.10. EESK iesaka Komisijai sākt rīkoties, lai veicinātu kiberdrošības sertifikāciju un sertifikātus Eiropas Savienībā, un atbalstīt to atzīšanu visos starptautiskajos tirdzniecības nolīgumos.

4.5. ***ENISA***

4.5.1. EESK uzskata, ka *ENISA* jaunās pastāvīgās pilnvaras, ko ierosinājusi Komisija, būtiski palīdzēs uzlabot Eiropas sistēmu izturētspēju. Tomēr ar to saistītais *ENISA* piešķirtais provizoriskais budžets un resursi var būt nepietiekami aģentūras pilnvaru izpildei.

4.5.2. EESK mudina visas dalībvalstis izveidot atsevišķu un *ENISA* pielīdzināmu partneriestādi, jo vairums dalībvalstu to vēl nav izdarījušas. Būtu jāveicina strukturēta programma valsts ekspertu norīkošanai darbā *ENISA*, lai atbalstītu paraugprakses apmaiņu un stiprinātu uzticēšanos. Komiteja arī iesaka Komisijai nodrošināt, ka tiek apkopoti un kopīgoti dalībvalstu pašreizējās labās prakses piemēri un efektīvi pasākumi.

4.5.3. EESK arī uzskata, ka no spēju veidošanas viedokļa par *ENISA* prioritāti būtu jānosaka pasākumi, kas vērsti uz atbalstu e-pārvaldei ([10]). Svarīga ir personu, organizāciju, uzņēmumu un objektu ES un pasaules mēroga digitālā identitāte, un par prioritāti būtu jāizvirza tiešsaistes krāpniecības, kā arī identitātes zādzības un rūpniecības intelektuālā īpašuma zādzības apkarošana.

4.5.4. *ENISA* būtu arī jāsniedz regulāri ziņojumi par dalībvalstu kibergatavību, primāri pievēršoties Kiberdrošības direktīvas II pielikumā nosauktajām jomām. Ikgadējās Eiropas kibermācībās būtu jānovērtē dalībvalstu gatavība un Eiropas mehānisma, kas paredzēts reaģēšanai kiberkrīžu gadījumā, efektivitāte, kā arī jāsagatavo ieteikumi.

4.5.5. EESK raizējas par to, ka resursi operatīvai sadarbībai ir pārāk ierobežoti, un tas attiecas arī uz *CSIRT* tīklu.

4.5.6. Runājot par uzdevumiem, kuri saistīti ar tirgu, EESK uzskata, ka sadarbības stiprināšana ar dalībvalstīm un oficiāla kiberdrošības aģentūru tīkla izveide nodrošinātu atbalstu ieinteresēto personu sadarbībai ([11]). Laiks līdz nonākšanai tirgū ir ļoti īss, un ES uzņēmumiem ir ārkārtīgi svarīgi būt konkurētspējīgiem šajā jomā, savukārt *ENISA* ir jāspēj attiecīgi reaģēt. EESK skatījumā *ENISA* tāpat kā citas ES aģentūras varētu nākotnē piemērot nodevu un maksu sistēmu. EESK raizējas, ka kompetenču konkurence starp ES un valstu aģentūrām varētu, kā tas jau ir noticis citās jomās, aizkavēt atbilstošu ES regulatīvā satvara īstenošanu un kaitēt ES vienotajam tirgum.

4.5.7. EESK atzīmē, ka ar pētniecību un inovāciju un ar starptautisko sadarbību saistītie uzdevumi pašlaik ir minimāli.

([10]) Digitālais vienotais tirgus / vidusposma pārskats.
([11]) OV C 75, 10.3.2017., 124. lpp.

4.5.8. EESK uzskata, ka kiberdrošība būtu regulāri jāapspriež tieslietu un iekšlietu aģentūru kopējās sanāksmēs un ka *ENISA* būtu regulāri jāsadarbojas ar Eiropolu.

4.5.9. Tā kā kiberjoma ir ļoti inovatīva, standarti ir rūpīgi jāapsver, lai novērstu šķēršļus inovācijai, kurai ir nepieciešams dinamisks satvars; iespēju robežās būtu jānodrošina turp- un atpakaļsaderība, lai aizsargātu gan iedzīvotājus, gan uzņēmumu ieguldījumus.

4.5.10. Ņemot vērā valstu sertifikācijas pārraudzības iestāžu nozīmi, EESK iesaka, ka jau ar šo regulu vajadzētu izveidot to iestāžu oficiālo tīklu, kuras ir pilnvarotas risināt pārrobežu problēmas ar *ENISA* atbalstu. Šo tīklu vēlāk varētu pārveidot par vienotu aģentūru.

4.5.11. Uzticēšanās ir ārkārtīgi svarīga, taču *ENISA* nedrīkst ne pieņemt lēmumus, ne izstrādāt revīzijas ziņojumus. EESK uzskata, ka minētajai aģentūrai, Komisijas uzdevumā veicot revīzijas un inspekcijas, būtu jāpārrauga valstu sertifikācijas uzraudzības iestāžu sniegums un lēmumu pieņemšana.

4.5.12. *ENISA* valdē novērotāja statusā būtu jāpiedalās arī rūpniecības un patērētāju organizāciju pārstāvjiem.

4.6. ***Nozare, MVU, finansējums/ieguldījumi un inovatīvi uzņēmējdarbības modeļi***

4.6.1. *Nozare un ieguldījumi*

Lai palielinātu to ES uzņēmumu konkurētspēju, kuri darbojas IKT jomā, pasākumi ir jāvērš uz lielāku atbalstu IKT nozares, tostarp MVU, izaugsmei un konkurētspējai.

Eiropai būtu jāpalielina ieguldījumi, kombinējot dažādus ES fondus, valstu fondus un privātā sektora investīcijas un spēcīgā publiskā un privātā sektora sadarbībā virzoties uz stratēģiskiem mērķiem. Būtu jāpalielina ieguldījumu līmenis kritiski svarīgās jomās, un šie ieguldījumi būtu jābalsta, pašreizējā un nākamajā pētniecības pamatprogrammā izveidojot ES kiberdrošības fondu inovācijai, pētniecībai un izstrādei. Eiropai turklāt vajadzētu izveidot fondu kiberdrošības pasākumu īstenošanai, atverot jaunu finansējuma atzaru pašreizējā un nākamajā Eiropas infrastruktūras savienošanas instrumentā, kā arī nākamajā ESIF 3.0.

Būtu jārada stimuli, kas mudinātu ES dalībvalstis, kad vien iespējams, iegādāties Eiropas risinājumus un izvēlēties Eiropas piegādātājus, ja tādi ir, it īpaši sensitīvam lietojumam. Eiropai būtu jāveicina to Eiropas kiberlīderu izaugsme, kuri būtu spējīgi konkurēt globālā tirgū.

4.6.2. *MVU*

Ņemot vērā tirgus sadrumstalotību, ir nepieciešama lielāka skaidrība par klientu pieprasījumu, lai uzlabotu atbilstību tirgus prasībām. Bez strukturēta pieprasījuma MVU un jaunuzņēmumi nevar strauji augt. Šajā kontekstā būtu vēlams izveidot Eiropas kiberdrošības MVU centru.

Kiberdrošības tehnoloģija mainās strauji, un MVU, pateicoties to elastīgumam, var sniegt konkurētspējas saglabāšanai nepieciešamos progresīvos risinājumus. Pretstatā trešām valstīm ES joprojām meklē MVU piemērotu uzņēmējdarbības modeli.

Varētu izstrādāt īpašas jaunuzņēmumiem un MVU paredzētas shēmas, lai palīdzētu segt sertifikācijas izmaksas un tādējādi pārvarēt lielās grūtības piesaistīt finansējumu tehnoloģiskajai un komerciālajai attīstībai.

4.7. ***Cilvēkfaktors: patērētāju izglītošana un aizsardzība***

4.7.1. EESK norāda, ka Komisijas priekšlikumā nav pienācīgi ņemti vērā cilvēki kā galvenie digitālo procesu virzītāji – vai nu būdami labumguvēji, vai arī galvenie kiberincidentu izraisītāji.

4.7.2. Jāveido spēcīgas pamata kiberprasmes un jāuzlabo kiberhigiēna, kā arī izpratne sabiedrībā un uzņēmumos. Lai sasniegtu šo rezultātu, būtu jāapsver tādi līdzekļi kā tam paredzēti ieguldījumi, laiks augsta līmeņa pasniedzēju sagatavošanai un efektīvas informētības palielināšanas kampaņas. Lai īstenotu šos triju veidu pasākumus, kopīgā pieejā ir jāiesaistās valsts un reģionālajām iestādēm (atbildīgām par efektīvu izglītības programmu sagatavošanu un par ieguldījumiem tajās), kā arī uzņēmumiem un MVU.

4.7.3. Būtu jāizskata iespēja, aktīvi iesaistoties *ENISA* un tās valstu līdziniekiem, radīt ES sertificētu mācību programmu vidusskolām un profesionāļiem. Turklāt, izstrādājot izglītības programmas ar mērķi uzlabot nodarbinātības līmeņus kiberdrošības jomā, būtu jāņem vērā dzimumu līdztiesība.

4.7.4. EESK uzskata, ka sertifikācijā jāiekļauj pienācīga sistēma gan datoraparatūras, gan programmatūras marķēšanai, kādu izmanto arī attiecībā uz daudziem citiem produktiem (piemēram, energoproduktiem). Tādam instrumentam būtu triju veidu priekšrocības: tas samazinātu izmaksas uzņēmumiem, mazinātu tirgus sadrumstalotību, ko rada valstu līmenī jau pieņemtās dažādās sertifikācijas sistēmas, un palīdzētu patērētājiem izprast iegādātās preces kvalitāti un īpašības. Šajā saistībā ir svarīgi, lai arī no trešām valstīm importētie produkti būtu pakļauti tādiem pašiem sertifikācijas un marķēšanas mehānismiem. EESK uzskata, ka *ad hoc* logo izveide varētu būt lietderīga, lai patērētājus un lietotājus nekavējoties informētu par iegādāto produktu vai par to vietņu uzticamību, kurās tiek veikta tirdzniecība vai kurās ir paredzēta sensitīvu datu pārsūtīšana.

4.7.5. *ENISA* būtu jāuzņemas svarīgais daudzlīmeņu informēšanas un izpratnes veicināšanas darbs, lai vairotu zināšanas par "drošu" apiešanos ar digitālo tehniku un lietotāju uzticēšanos internetam. Šajā nolūkā ir jāiesaista uzņēmumu un patērētāju apvienības un citas digitālo pakalpojumu jomā strādājošas organizācijas.

4.7.6. Papildus Kiberdrošības aktam, kā ierosināts atzinumā INT/828, EESK uzskata, ka ir ļoti svarīgi pēc iespējas ātrāk sākt īstenot plašu ES mēroga programmu, kas veltīta digitālajai izglītībai un apmācībai, lai nodrošinātu visiem iedzīvotājiem instrumentus labākai pārejas pārvarēšanai. Kaut arī EESK apzinās valstu konkrēto kompetenci šajā jautājumā, tā jo īpaši cer, ka šo programmu sāks īstenot skolās, uzlabojot skolotāju zināšanas, pielāgojot mācību programmas un didaktiku digitālajām tehnoloģijām (ieskaitot e-mācības), kā arī nodrošinot visiem jauniešiem augstas kvalitātes apmācību. Šī programma dabiski turpināsies ar mūžizglītību, kuras mērķis ir pielāgot vai atjaunināt visu darbinieku prasmes ([12]).

5. **Īpašas piezīmes**

5.1. ***Jaunās tehnoloģijas un risinājumi: lietu internets***

Satīkloto ierīču daudzums pastāvīgi palielinās, un gaidāms, ka komponentu, sistēmu un risinājumu digitalizācijas un palielinātas savienojamības dēļ to skaits daudzkārt pārsniegs zemes iedzīvotāju skaitu. Šī tendence rada jaunas iespējas kibernoziedzniekiem, īpaši tāpēc, ka lietu interneta ierīces bieži vien nav tikpat labi aizsargātas kā parastās ierīces.

Eiropas drošības standarti dažādās vertikālēs, kurās tiek izmantotas lietu interneta ierīces, var samazināt izstrādē ieguldīto darbu, laiku un budžetu visiem nozares dalībniekiem satīkloto produktu vērtības ķēdē.

Arī "parastām" cilvēku interneta (*Internet of People*) ierīcēm varētu būt nepieciešams sava veida minimālais drošības līmenis, ko nodrošinātu Identitātes piekļuves pārvaldība (*IDAM*), "ielāpi" un ierīču pārvaldība. Tā kā sertificēšana ir svarīga metode drošības līmeņa paaugstināšanai, jaunajā ES sertifikācijas pieejā lielāks uzsvars būtu jāliek uz lietu interneta drošību.

Briselē, 2018. gada 14. februārī

Eiropas Ekonomikas un sociālo lietu komitejas priekšsēdētājs
Georges DASSIS

([12]) Digitālais vienotais tirgus / vidusposma pārskats.