Eiropas Ekonomikas un sociālo lietu komitejas atzinums par tematu "Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika"

(pašiniciatīvas atzinums)

(2023/C 293/04)

Ziņotājs: ***Anastasis YIAPANIS***

Līdzziņotājs: ***Alberto MAZZOLA***

Pilnsapulces lēmums	20.9.2022.
Juridiskais pamats	Reglamenta 52. panta 2. punkts
	Pašiniciatīvas atzinums
Atbildīgā specializēta nodaļa	Rūpniecības pārmaiņu konsultatīvā komisija (*CCMI*)
Pieņemts specializētās nodaļas sanāksmē	27.3.2023.
Pieņemts plenārsesijā	14.6.2023.
Plenārsesija Nr.	579
Balsojuma rezultāts	
(par/pret/atturas)	208/1/2

1. **Secinājumi un ieteikumi**

1.1. Eiropas Ekonomikas un sociālo lietu komiteja (EESK) atbalsta ierosināto ES kiberaizsardzības politiku, taču bija cerējusi, ka organizētai pilsoniskajai sabiedrībai tiks piešķirta nozīmīgāka loma šo priekšlikumu izstrādē. Komiteja uzskata, ka šobrīd ir grūti novērtēt, vai kopīgajā paziņojumā izklāstītās turpmākās iniciatīvas tiks īstenotas un vai tajās paredzētie rezultāti tiks sasniegti. Tā mudina ES iestādes un dalībvalstis prioritāru nozīmi piešķirt paziņotajām iniciatīvām un tās ātri virzīt.

1.2. EESK uzsver, ka ir vajadzīgi papildu pasākumi, lai uzlabotu ES spēju atklāt kiberdraudus, un aicina pētniecības un izstrādes finansējumu novirzīt progresīvu ES spēju attīstīšanai. Privātā un publiskā sektora sadarbība ir būtiska, un tā nedrīkst būt vienvirziena. EESK uzskata, ka ES koordinācija ir nepieciešama, lai novērstu sadrumstalotību un nodrošinātu sadarbību un kopīgas investīcijas dalībvalstu vidū.

1.3. EESK atbalsta ES Kiberaizsardzības koordinācijas centra izveidi un iesaka dalībvalstīm apņemties nodrošināt spējas ātri reaģēt 24 stundas diennaktī un 7 dienas nedēļā, izvērtēt ES kiberkrīžu reaģēšanas mehānismu kibergatavību un veiktspēju, īpašu uzmanību pievēršot gan militārajām spējām, gan kritiskajām nozarēm, kā noteikts Eiropas Parlamenta un Padomes Direktīvā (ES) 2022/2555 ([1]) (TID 2 direktīva). Komiteja atbalsta Eiropas Kiberdrošības kompetences centra (*European Cybersecurity Competence Centre* jeb *ECCC*) pilnvaru paplašināšanu, lai palīdzētu ES Kiberaizsardzības koordinācijas centra darbā.

1.4. EESK uzskata, ka Savienības kiberdrošības stratēģiskās autonomijas un suverenitātes stiprināšanas nolūkā būtu jāizstrādā vai no privātā sektora jāpārņem reāllaika testēšanas un informācijas apmaiņas dinamiska platforma, lai apzinātu pašreizējo spēju nepilnības. To var izmantot arī paraugprakses apmaiņai, ziņošanai par kiberincidentiem un tam, lai Eiropas Savienībā izveidotu visu kibernoziedznieku sarakstu.

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

1.5. EESK uzsver nepieciešamību labāk sagatavoties kiberuzbrukumiem (piemēram, tādiem kā Krievijas uzbrukumi Ukrainā), kas vērsti it īpaši pret kritisko infrastruktūru. Sadarbība starp civilajām un militārajām ekosistēmām ir būtiska, lai efektīvi pārvarētu krīzes, nodrošinātu sadarbspēju un novērstu centienu un investīciju dublēšanos, citstarp izmantojot simulētus testa kiberuzbrukumus.

1.6. EESK uzskata, ka investīcijas kiberaizsardzības jomā prioritāri būtu jānovirza ES iedzīvotāju un kritiskās infrastruktūras aizsardzībai, piemēram, jāizmanto uzticami aparatūras un programmatūras piegādātāji. Komiteja uzstāj, ka ir savlaicīgi jāatjaunina prioritātes un investīcijas, par kurām jāvienojas ES un dalībvalstīm, piedaloties attiecīgajām privātajām ieinteresētajām personām.

1.7. Eiropas Savienībai ir jāsaglabā un jāattīsta nepieciešamās spējas, lai sargātu savu digitālo ekonomiku, sabiedrību, demokrātiju un kritiskās tehnoloģijas un sniegtu svarīgus kiberdrošības pakalpojumus. Lai rūpētos par ES stratēģisko autonomiju, ir būtiski samazināt atkarību no trešām valstīm. EESK uzskata, ka ir svarīgi, lai ES pieņemtu vidēja termiņa koncepciju attiecībā uz autonomiju svarīgu tehnoloģiju ziņā, un stingri atbalsta to, ka pētniecības un ražošanas iekārtas būtu jāizgatavo ES reģistrētiem uzņēmumiem un jāparedz atbilstoša Eiropas rūpniecības politika, kas vērsta uz autonomu kiberekosistēmu.

1.8. Mazajiem un vidējiem uzņēmumiem (MVU) būtu jāsaņem mērķēts atbalsts un piekļuve finansēšanas programmām, kas palielina to noturību pret kiberuzbrukumiem, kā arī jāsaņem palīdzība, apmācības un izglītības iespējas par kiberriskiem un par aizsardzību pret tiem. Eiropas Savienībai būtu jānodrošina stimulējošs mehānisms, kas dod iespēju MVU pakāpeniski iepazīties ar šo tematu un radīt novatoriskus MVU.

1.9. EESK atbalsta ieceri izveidot Kiberprasmju akadēmiju un aicina Eiropas Komisiju koordinēt un finansēt plaša mēroga apmācības un profesionālās izglītības mācību programmas, kurās tiktu iesaistītas visas dalībvalstis un kuru mērķis būtu nodrošināt kvalificētu darbaspēku visām kiberaizsardzības aģentūrām un organizācijām, kā arī privātiem civilajiem tīkliem.

1.10. Komiteja uzskata, ka ir būtiski palielināt iedzīvotāju informētību par kiberdrošību, lai samazinātu kiberuzbrukumu ietekmi, un aicina izstrādāt kiberdrošības izglītības programmas un mūžizglītības programmas, kas vērstas uz kiberprasmju un kiberzināšanu uzlabošanu. EESK atbalsta kiberdrošības integrēšanu visās turpmākajās ES publiskās politikas jomās un plašas sabiedrības informēšanu par kiberdraudiem.

1.11. EESK uzskata, ka cieša sadarbība ar NATO sabiedrotajiem militārajās jomās jākoncentrē uz pilnīgu koordināciju un savstarpīgumu, kopīgiem pētniecības, izstrādes un inovācijas projektiem, paraugprakses apmaiņu, plašām apmācības programmām un kiberuzbrukumu simulācijām ar galveno mērķi paplašināt kopīgās reaģēšanas spējas.

1.12. Komiteja aicina Augsto pārstāvi izanalizēt pašreizējos divpusējos dialogus par kiberjautājumiem un iesaistīties papildu diskusijās ar citām valstīm un attiecīgajām starptautiskajām organizācijām, lai, īpašu uzsvaru liekot uz savstarpīgumu, izveidotu pasaules mēroga sistēmu starptautisko tiesību ievērošanai kibertelpā. Komiteja uzskata, ka, pateicoties spēcīgam pamatam demokrātisko pamatbrīvību jomā, ES ir piemērota, lai uzņemtos vadību starptautiskajās diskusijās par kiberdrošības nākotni – it īpaši tajās, kas notiek Apvienoto Nāciju Organizācijā.

1.13. Eiropas Savienībai būtu jāieņem stingra nostāja pret jebkāda veida iedzīvotāju sociālās vērtēšanas sistēmu. EESK skaidri norāda, ka patiesa demokrātija nevar pastāvēt bez iedarbīgas persondatu aizsardzības, un uzskata, ka atbildīga un efektīva datu pārvaldība ir būtiska, lai hipersavienojamība kļūtu par konkurences priekšrocību.

2. **Ievads un vispārīgas piezīmes**

2.1. Sabiedrības digitālā izvēršanās ir saistīta ar daudziem kiberdrošības apdraudējumiem, ko rada tehnoloģiska modernizācija. Dažos pēdējos gados kiberuzbrukumu skaits un sarežģītība ir ievērojami pieauguši, radot draudus gan publisko, gan privāto struktūru drošībai. Neatkarīgi no tā, vai runa ir par izspiedējprogrammatūru, ļaunprogrammatūru, uz e-pastu vērstiem uzbrukumiem, datu aizsardzības pārkāpumiem, dezinformāciju, izkliedētā pakalpojumu atteikuma (*distributed denial-of-service* jeb *DDoS*) uzbrukumiem vai cita veida uzbrukumiem, tie visi konsekventi un pastāvīgi apdraud ES drošību kopumā.

2.2. EESK atzinīgi vērtē kopīgo paziņojumu "ES kiberaizsardzības politika" ([2]) un uzskata, ka tagad ir pienācis laiks steidzami un koordinēti rīkoties ES līmenī, iesaistot gan civilās, gan militārās kibertelpas ekosistēmas un nodrošinot pienācīgu satvaru investīcijām kiberaizsardzības spējās. Tomēr Komiteja norāda, ka paziņojumā izskan tikai apņemšanās rīkoties un ir iekļauts saraksts ar turpmākajām ES iniciatīvām, kuras būtu jāīsteno, un uzskata, ka nav iespējams novērtēt, vai šīs turpmākās saistības patiešām tiks izpildītas, jo turpmākās sarunas starp abiem likumdevējiem, protams, ietekmēs ES kiberdrošības rīcības plāna galīgo iznākumu.

2.3. Uz *KA-SAT* satelītu tīklu tēmētais Krievijas uzbrukums, kas izjauca saziņu starp Ukrainas militārajiem spēkiem, un nesenais skandāls, kurā bija iesaistīts *Éric Léandri*, kas dažu aizsardzības uzņēmumu uzdevumā veica kiberspiegošanu, noliek kiberdrošības jautājumu ES drošības apraudējumu saraksta augšgalā. Lai gan Vispārīgā datu aizsardzības regula (VDAR) ir stabils ES tiesību akts, kas ir spēkā vairākus gadus, ir skaidrs, ka arvien pieaugošais pieejamo datu apjoms ir neaizsargāts, un risks, ka trešās personas pārkāps likumības robežu, katru dienu kļūst lielāks.

2.4. Tā kā kiberuzbrukumi ir transnacionāli, ir nepieciešama ES koordinācija, lai mazinātu pašreizējo sadrumstalotību un nodrošinātu, ka dalībvalstis ir gatavas sadarboties un kopīgi investēt. Tas ir īpaši svarīgi attiecībā uz turpmākiem gadījumiem, kad par mērķi varētu kļūt viena dalībvalsts un visām pārējām vajadzētu būt iespējai sniegt tūlītēju atbalstu.

3. **Jārīkojas kopā, lai nodrošinātu spēcīgāku kiberaizsardzību**

3.1. Komiteja pieņem zināšanai pieteiktās vērienīgās iniciatīvas, kuru mērķis ir izveidot ES Kiberaizsardzības koordinācijas centru, izstrādāt *CyDEf-X* projektu, radīt kiberdraudu ātrās reaģēšanas vienības, sagatavot ES kiberdrošības solidaritātes iniciatīvu un izpētīt iespēju, kā izstrādāt IKT produktu, pakalpojumu un procesu kiberdrošības sertifikācijas shēmas. EESK iesaka visām dalībvalstīm apņemties būt gatavām nodrošināt ātru reaģēšanu 24 stundas diennaktī 7 dienas nedēļā, ES Koordinācijas centru iesaistīt regulāru ziņojumu novērtēšanā un sagatavošanā par dalībvalstu kibergatavību un Eiropas kiberkrīžu reaģēšanas mehānisma efektivitāti un galveno uzmanību pievērst gan militārajām spējām, gan kritiskajām nozarēm, kas apzinātas TID 2 direktīvā. Katrā dalībvalstī vajadzētu būt īpaši apmācītiem speciālistiem, kas varētu reaģēt kiberincidentu gadījumā, un tām būtu regulāri jāpārbauda savas spējas reaģēt citā dalībvalstī.

3.2. Lai gan paziņojumā ir sniegts plašs pakāpenisku uzlabojumu saraksts, EESK cerēja, ka tiks izstrādāts skaidrs ceļvedis šo iniciatīvu īstenošanai ar skaidru pārvaldību un iesniegšanas un pieņemšanas termiņiem. Turklāt Komiteja cerēja, ka minēto priekšlikumu izstrādē lielāka nozīme tiks piešķirta organizētai pilsoniskajai sabiedrībai.

3.3. EESK uzskata, ka dalībvalstīm ir jāstiprina savas iekšējās spējas vērsties pret kiberdraudiem, vienlaikus iesaistoties sadarbības projektos un apmainoties ar informāciju un paraugpraksi ar kolēģiem citās dalībvalstīs. Ir steidzami jāiegulda kiberaizsardzības spējās un paātrinātā tehnoloģiju izvēršanā ([3]) visās dalībvalstīs un kopējā sagatavotībā atklāt kiberuzbrukumus, atgūties no tiem un aizstāvēties pret tiem. Komiteja uzskata, ka Savienības kiberdrošības autonomijas atbalstīšanas nolūkā ir jāizstrādā vai no privātā sektora jāpārņem reāllaika testēšanas un informācijas apmaiņas platforma, kas būtu dinamiska un kuras mērķis būtu apzināt pašreizējās trūkstošās spējas.

3.4. EESK piekrīt viedoklim, ka pašreizējā stadijā militārām kibertelpas operācijām arī turpmāk vajadzētu būt dalībvalstu kompetencē; Komiteja atbalsta pieteikto sadarbību starp ES militārajām datorapdraudējumu reaģēšanas vienībām (*milCERTs*), datordrošības incidentu reaģēšanas vienībām (*CSIRTs*) un ES iestāžu, biroju un aģentūru datorapdraudējumu reaģēšanas vienībām (*CERT-EU*).

3.5. Nesen pieņemtajā TID 2 direktīvā un Direktīvā par kritisko vienību noturību (*Critical Entities Resilience Directive* jeb *CER*) ([4]) jau ir noteikti konkrēti valsts un nozaru pienākumi ES kiberaizsardzības satvaram. Ir vajadzīga turpmāka rīcība, lai uzlabotu ES kolektīvās atklāšanas spējas, un EESK aicina veikt investīcijas pētniecībā un izstrādē, lai attīstītu progresīvas ES spējas.

([2]) Komisijas paziņojums "ES kiberaizsardzības politika".
([3]) Piemēram, NATO iniciatīva aizsardzības inovācijas paātrināšanai Ziemeļatlantijas reģionā (*DIANA*).
([4]) *CER* direktīva.

4. **Nodrošināt ES aizsardzības ekosistēmu**

4.1. EESK uzskata, ka raksturīgie sarežģījumi un strauji mainīgie tehniskie izaicinājumi ir pārveidojuši aizsardzības ekosistēmu un ka kiberdrošība ir kļuvusi par kopīgu jautājumu gan militārajā, gan civilajā sektorā, kā arī ES iedzīvotāju vidū. Sadarbība starp civilajām un militārajām ekosistēmām tagad ir svarīgāka nekā jebkad agrāk, un tai būtu jāsniedz ieguvumi efektīvākā krīzes pārvarēšanā, pastāvīgā progresā un sadarbspējas jomā, un jāizvairās no vienu un to pašu centienu un investīciju dublēšanas vai pavairošanas. Dalībvalstīm vajadzētu būt gatavām veikt valsts kritiskās infrastruktūras spriedzes testus, lai novērtētu un palielinātu noturību pret turpmākiem kiberuzbrukumiem.

4.2. EESK uzskata, ka investīcijas kiberaizsardzībā ir prioritāri jānovirza ES iedzīvotāju un kritiskās infrastruktūras aizsardzībai. Ņemot vērā digitālās pārveides ātrumu un straujo apdraudējuma situācijas attīstību, Komiteja stingri mudina ES un dalībvalstis vienoties par prioritāšu un investīciju savlaicīgu atjaunināšanu un rūpīgi apspriesties ar attiecīgajām privātajām ieinteresētajām personām. Lietu interneta (*Internet of Things* jeb *IoT*) ierīces bieži vien nav tik aizsargātas kā tradicionālās ierīces, un EESK aicina garantēt obligāto drošības līmeņa minimumu, izmantojot identitātes un piekļuves pārvaldības (*IDAM*) platformas. Tā kā sertifikācija ir svarīgs veids, kā nodrošināt augstāku drošības līmeni, Komiteja aicina jaunajā ES sertifikācijas koncepcijā vairāk uzsvērt lietu interneta drošību.

4.3. Eiropas Savienībai ir jāveido noturība pret kiberuzbrukumiem un jārada efektīva kiberatturēšana. Kritiskā infrastruktūra ir jāaizsargā pret jebkāda veida kiberuzbrukumiem, šim nolūkam izmantojot arī ES aizsardzības sistēmas. Komiteja uzskata, ka ES stratēģiskajās interesēs ir nodrošināt, ka Savienība saglabā un attīsta būtiskās spējas, lai aizsargātu savu digitālo ekonomiku, sabiedrību un demokrātiju, panāktu pilnīgu digitālo suverenitāti, kas ir vienīgais veids, kā aizsargāt kritiskās tehnoloģijas un sniegt efektīvus svarīgākos kiberdrošības pakalpojumus. ES stratēģiskās autonomijas interesēs ir arī būtiski samazināt atkarību no trešām valstīm. EESK uzskata, ka šajā procesā būtu jāiesaista ES nozaru aģentūras (*ENISA*, *EASA*, *ERA*, *EMA*, *EBA*, *ESA*, *HADEA* u. c.) un jāsniedz tām norādījumi kiberdrošības shēmu izstrādē.

4.4. Covid-19 pandēmija ir paātrinājusi digitālo pārkārtošanos un pārveidojusi tradicionālo darbu par hibrīddarbu un/vai attālinātu darbu, radot jaunas darba attiecības un vēlmes, kā arī jaunu kategoriju, proti, digitālos nomadus, kuru skaits pieaug. EESK atzīmē straujās darba tirgus pārmaiņas, kuru dēļ uzņēmumi ir pieņēmuši nulles uzticēšanās arhitektūru, izmantojot identitātes piekļuves pārvaldības (*Identity Access Management* jeb *IAM*) un privileģētas piekļuves pārvaldības (*Privileged Access Management* jeb *PAM*) risinājumus. Komiteja uzskata, ka šāda veida uzņēmumu resursu pārvaldība paver iespēju jauniem risinājumiem saistībā ar kiberdraudiem, un atzīst, ka ir jāatbalsta privātais sektors, lai stiprinātu to inovatīvo digitālo risinājumu drošības līmeni.

4.5. EESK pauž nožēlu par Komisijas apgalvojumu, ka "sadarbībā ar dalībvalstīm varētu izstrādāt īstenošanas plānu", un uzskata, ka šāds īstenošanas plāns ir obligāts. EESK uzskata, ka tas būtu jāizstrādā kopīgi ar dalībvalstīm un jāīsteno pēc iespējas ātrāk. Komiteja ir nobažījusies par Komisijas pieņemto vājo nostāju un mudina ES iestādes un dalībvalstis veicināt ātru progresu paziņoto iniciatīvu īstenošanā.

5. **Investīcijas kiberaizsardzības spējās**

5.1. Tā kā tehniskā attīstība norit strauji, kibertelpa ir kļuvusi par jaunāko karadarbības jomu pēc sauszemes, jūras, gaisa un kosmosa telpas. Tā ir radījusi arī lielas noziedzības iespējas ļaunprātīgiem kiberaktoriem – sākot ar neatkarīgiem hakeriem līdz profesionāliem noziedzniekiem un pat valstiskiem dalībniekiem.

5.2. Investīcijas pētniecībā un izstrādē ir ļoti svarīgas, un EESK atzinīgi vērtē to, ka programmā "Digitālā Eiropa", Eiropas Aizsardzības fondā, pamatprogrammā "Apvārsnis Eiropa" un valstu atveseļošanas programmās pašlaik tam ir atvēlēti īpaši līdzekļi. Tomēr Komiteja atzinīgi vērtētu plānus, kas būtu vairāk transnacionāli un kuros galvenā uzmanība pievērsta sadarbībai un sadarbspējai starp kiberaizsardzības sistēmām visās dalībvalstīs, kā arī lielākai sinerģijai starp finansēšanas instrumentiem, kas atbalstītu it sevišķi inovatīvus MVU.

5.3. Komiteja norāda, ka, kā jau 2020. gadā tika paziņots ES Kiberdrošības stratēģijā, kopējās kibervienības izveides termiņš ir šogad, un gaida ziņas par procesa pabeigšanu un ES gatavību reaģēt uz plaša mēroga kiberincidentiem. EESK sagaida, ka tā uzlabos ES situācijas apzināšanos un vispārējo spēju reaģēt un atgūties.

5.4. EESK atbalsta *ECCC* pilnvaru paplašināšanu, lai atbalstītu ES Kiberaizsardzības koordinācijas centra darbību. Turklāt šis tīkls varētu atbalstīt Eiropas digitālo suverenitāti, attīstot konkurētspējīgu Eiropas rūpniecisko pamatu svarīgām tehnoloģiskajām spējām, kuras daļēji balstītos uz līgumisku publiskā un privātā sektora partnerību (PPP) ietvaros veikto darbu. PPP ir izrādījušās visefektīvākais veids, kā uzlabot visas digitālās ekosistēmas kiberdrošību, taču tās nedrīkst būt vienvirziena: publiskā sektora iestādēm ir jādala savi izlūkdati ar privāto sektoru.

5.5. EESK norāda: lai novērstu, ka ar kvantu datoru starpniecību notiek uzlaušanas mēģinājumi, Eiropas Savienībai ir nekavējoties jāiegulda tādās progresīvās tehnoloģijās kā pēckvantu kriptogrāfija. Komiteja uzskata, ka Eiropai vidējā termiņā ir jākoncentrējas uz autonomiju, un stingri iestājas par to, lai pētniecības un ražošanas iekārtas attīstītu ES reģistrēti uzņēmumi. EESK uzskata, ka ir svarīgi palielināt ES resursus pētniecībai un inovācijai digitalizācijas jomā un atbalstīt operatoru un piegādātāju investīcijas jaunās tehniskās drošības funkcijās, kas cita starpā saistītas ar jaunām tendencēm, piemēram, paplašināto realitāti un metaversu. Konkrētāk, Eiropā ir svarīgi izveidot izkliedēto mākoņdatošanas infrastruktūru, pamatojoties uz Eiropas noteikumiem par tādiem jautājumiem kā datu uzglabāšana un apstrāde ([5]).

5.6. Būtu jāpievērš īpaša uzmanība MVU, un vajadzētu nodrošināt to piekļuvi finansēšanas programmām, kas uzlabotu to gatavību kiberuzbrukumiem, kā arī piekļuvi palīdzības, apmācības un izglītības programmām, kas tiem palīdzētu izprast kiberriskus un to, kā sevi aizsargāt. Eiropas Savienībai būtu jānodrošina stimulējošs mehānisms, kas dotu iespēju MVU pakāpeniski iepazīties ar šo tematu.

5.7. Komisija lēš, ka pašreizējais prasmju trūkums kiberdrošības jomā ir pusmiljons cilvēku, un EESK atzinīgi vērtē priekšlikumu izveidot Kiberprasmju akadēmiju. Ir skaidrs, ka centieni dalībvalstu līmenī nav pietiekami, lai mazinātu prasmju trūkumu, tāpēc Komiteja ierosina, ka Komisija līdztekus akadēmijas izveidei izmanto Eiropas Prasmju gada sniegto izdevību, kā arī koordinē un finansē ES līmenī plaša mēroga apmācības programmas un profesionālās izglītības un apmācības jeb PIA programmas, kurās iesaistītas visas dalībvalstis un kuras ir vērstas uz kvalificēta darbaspēka nodrošināšanu visām kiberaizsardzības aģentūrām un struktūrām, kā arī privātiem civilajiem tīkliem. Īpaša uzmanība jāpievērš darbaspēka apmācībai, it īpaši zinātnes, tehnoloģijas, inženierzinātnes un matemātikas (*STEM*) jomā.

5.8. Turklāt EESK uzskata, ka ir būtiski palielināt iedzīvotāju informētību par kiberdrošību, lai samazinātu kiberuzbrukumu ietekmi, it īpaši attiecībā uz pamata kibernoziegumiem, kas vērsti pret plašu sabiedrības daļu. Komiteja aicina kiberdrošības jomā izstrādāt kiberdrošības izglītības programmas un mūžizglītības apmācības programmas, kas būtu vērstas uz kiberprasmju uzlabošanu un padarītu kiberdrošību pazīstamāku un pievilcīgāku iedzīvotājiem, it īpaši jaunākajai paaudzei. EESK atbalsta kiberdrošības apsvērumu integrēšanu visās turpmākajās ES publiskās politikas jomās un plašas sabiedrības informēšanu par kiberdraudiem, tostarp izmantojot bezmaksas apmācības programmas visiem iedzīvotājiem, mobilo tālruņu bezmaksas informācijas lietotnes vai arī komunicēšanu visizdevīgākajā televīzijas raidīšanas laikā. Līdztekus šīm darbībām visos sabiedrības līmeņos ir jāveicina plaša kultūras attīstība virzībā uz kiberdrošības principiem atbilstošu pieeju.

5.9. EESK uzskata, ka ir būtiski novērtēt piegādātāju riska profilu un piemērot attiecīgus ierobežojumus tiem, ko uzskata par ļoti riskantiem, – tostarp nepieciešamos aizliegumus, kurus attiecina uz nozīmīgākajiem aktīviem un lietotnēm, kas koordinētajā riska novērtējumā ES līmenī atzīti par būtiskiem un jutīgiem, kā arī sertificēt uzticamus aparatūras un programmatūras piegādātājus.

6. **Partneri kopīgu problēmu risināšanai**

6.1. Tas, cik lielā mērā dažādas dalībvalstis ir sagatavotas turpmākiem kiberuzbrukumiem, ļoti atšķiras. EESK uzskata, ka pirmais tūlītējais solis ir izveidot ES iekšēju paraugprakses saziņas platformu, kas dalībvalstīm, kuras ir progresīvākas kiberjautājumos, dotu iespēju dalīties zināšanās ar citām valstīm un veicināt tūlītēju izmantošanu tajās. Tas palīdzētu uzlabot valstu struktūru savstarpējo uzticēšanos. Turklāt Komiteja uzskata, ka ir vajadzīga ciešāka sadarbība starp valsts un nevalstiskajiem dalībniekiem visā ES, lai uzlabotu produktu un pakalpojumu kiberdrošību iekšējā tirgū. EESK ierosina izveidot arī kopīgu ES platformu ziņošanai par kiberincidentiem, kā arī ES melno sarakstu ar visiem kibernoziedzības aktīvistiem.

([5]) Piemēram, *Gaia-X*, kas ir Francijas un Vācijas iniciatīva.

6.2. EESK uzskata, ka cieša sadarbība ar mūsu NATO sabiedrotajiem militārajā jomā ir jākoncentrē ne tikai uz spēju veidošanu un agrīnu atklāšanu, bet arī uz kopīgiem pētniecības, izstrādes un inovācijas projektiem, paraugprakses un ekspertu apmaiņu, apjomīgām apmācības programmām un kiberuzbrukumu simulācijām. Par galveno mērķi būtu jāizvirza kopīgo reaģēšanas spēju paplašināšana un sinerģijas turpmāku hibrīddraudu apkarošanai saskaņā ar Varšavas kopīgo deklarāciju (2016) un Briseles kopīgo deklarāciju (2018). ES un NATO sadarbība vēl aizvien sniedz vairākas iespējas, ko var izmantot, un tūlītējs progress var būtiski uzlabot mūsu iedzīvotāju un sabiedrības drošību.

6.3. Komiteja uzskata, ka diskusijām globālā mērogā un ar mūsu starptautiskajiem partneriem būtu jārada pamats tādas globālas un atvērtas kibertelpas veicināšanai, kurā tiek aizsargātas cilvēktiesības, pamatbrīvības un tiesiskums, un jākoncentrējas uz saistošu starptautisku standartu izstrādi nozarēs, kur notiek strauja digitālā attīstība. EESK iesaka Augstajam pārstāvim pārskatīt pašreizējos divpusējos dialogus par kiberjautājumiem un iesaistīties turpmākās sarunās ar citām valstīm un attiecīgajām starptautiskajām organizācijām, lai, pamatojoties uz stingru savstarpīguma nosacījumu, veicinātu pasaules mēroga sistēmu, ko izmantot starptautisko tiesību piemērošanai kibertelpā.

6.4. Noslēgumā Komiteja piebilst, ka ES, pateicoties demokrātisko pamatbrīvību jomā ieliktajiem stingrajiem pamatiem, vislabāk var vadīt starptautiskās debates par kiberdrošības nākotni, it īpaši ANO diskusiju laikā. Eiropas Savienībai ir jāiesaistās arī cīņā pret totalitāriem režīmiem, kas veic iedzīvotāju datu uzraudzību un pārkāpj viņu tiesības un brīvības, un tai ir stingri jāvēršas pret jebkāda veida iedzīvotāju sociālās vērtēšanas sistēmu. EESK skaidri norāda, ka patiesa demokrātija nevar pastāvēt bez iedarbīgas persondatu aizsardzības, un uzskata, ka atbildīga un efektīva datu pārvaldība ir būtiska, lai hipersavienojamība kļūtu par priekšrocību.

Briselē, 2023. gada 14. jūnijā

Eiropas Ekonomikas un sociālo lietu komitejas
priekšsēdētājs
Oliver RÖPKE