Eiropas Parlaments
2019-2024

Ārlietu komiteja

2023/0109(COD)

27.10.2023

ATZINUMS

Sniegusi Ārlietu komiteja

Rūpniecības, pētniecības un enerģētikas komitejai

par priekšlikumu Eiropas Parlamenta un Padomes regulai, kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberapdraudējumu un kiberincidentus, tiem sagatavoties un uz tiem reaģēt (COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Atzinuma sagatavotājs: *Dragoş Tudorache*

PA_Legam

Grozījums Nr. 1

Regulas priekšlikums
1. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(1) Informācijas un komunikācijas tehnoloģiju lietošana un ***izmantošana visās saimnieciskās dzīves nozarēs*** ir kļuvušas par fundamentāliem aspektiem ***laikā***, ***kad*** mūsu pārvaldes, uzņēmumi un pilsoņi ir cits ar citu pāri nozarēm un robežām saistīti un ***savstarpēji*** atkarīgi vairāk nekā jebkad agrāk.	(1) Informācijas un komunikācijas tehnoloģiju lietošana un ***atkarība no tām*** ir kļuvušas par fundamentāliem aspektiem ***visos saimniecisko***, ***kā arī militāro darbību sektoros, jo*** mūsu pārvaldes, uzņēmumi un pilsoņi***, kā arī militārie un aizsardzības aktori*** ir cits ar citu pāri nozarēm un robežām ***savstarpēji*** saistīti un atkarīgi vairāk nekā jebkad agrāk.

Grozījums Nr. 2

Regulas priekšlikums
2. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(2) Aug kiberincidentu apjoms, biežums un ietekme, ieskaitot uzbrukumus piegādes ķēdēm, un to mērķis ir kiberspiegošana, izspiedējprogrammu izmantošana vai darbības traucēšana. Tie ievērojami apdraud tīklu un informācijas sistēmu darbību. Ņemot vērā strauji mainīgo apdraudējuma ainu, draudoši plaši kiberincidenti, kas izraisa būtisku pārrāvumu vai kaitējumu kritiskajai infrastruktūrai, prasa labāku gatavību visos Savienības kiberdrošības satvara līmeņos. Apdraudējums ir plašāks par Krievijas militāro agresiju pret Ukrainu – ticams, ka tas saglabāsies, jo pašreizējā ģeopolitiskajā saspīlējumā iesaistījušies daudzi valstu atbalstīti kriminmāli un hakeristiski subjekti. Tādi kiberincidenti var kavēt sabiedrisku pakalpojumu sniegšanu un saimniecisku darbību, arī kritiskās vai ļoti kritiskās nozarēs, radīt būtiskus finansiālus zaudējumus, mazināt lietotāju uzticēšanos, radīt būtisku kaitējumu Savienības ekonomikai un pat veselībai un dzīvībai	(2) Aug kiberincidentu apjoms, biežums un ietekme, ieskaitot uzbrukumus piegādes ķēdēm, un to mērķis ir kiberspiegošana, izspiedējprogrammu izmantošana vai darbības traucēšana. Tie ievērojami apdraud tīklu un informācijas sistēmu darbību. Ņemot vērā strauji mainīgo apdraudējuma ainu, draudoši plaši kiberincidenti, kas izraisa būtisku pārrāvumu vai kaitējumu kritiskajai infrastruktūrai, prasa labāku gatavību visos Savienības kiberdrošības satvara līmeņos. ***Šī apdraudējuma nopietnība vēl vairāk aktualizējās sakarā ar to, ka mūsu kontinentā atkal notiek karš. Šis*** apdraudējums ir plašāks par Krievijas militāro agresiju pret Ukrainu – ticams, ka tas saglabāsies, jo pašreizējā ģeopolitiskajā saspīlējumā iesaistījušies daudzi valstu atbalstīti kriminmāli un hakeristiski subjekti. Tādi kiberincidenti var kavēt sabiedrisku pakalpojumu sniegšanu un saimniecisku darbību, arī kritiskās vai ļoti kritiskās nozarēs, radīt būtiskus finansiālus

bīstamas sekas. Bez tam kiberincidenti ir neprognozējami, jo tie mēdz rasties un izplesties pavisam īsā laikā, tos neierobežo nekāda ģeogrāfiska platība un tie notiek vienlaicīgi vai vienā mirklī izplatās daudzās valstīs.

zaudējumus, mazināt lietotāju uzticēšanos, radīt būtisku kaitējumu Savienības ekonomikai un ***drošībai un varētu*** pat ***izraisīt*** veselībai un dzīvībai bīstamas sekas***, iespējams, apdraudot vietējos un valsts drošības objektus***. Bez tam kiberincidenti ir neprognozējami, jo tie mēdz rasties un izplesties pavisam īsā laikā, tos neierobežo nekāda ģeogrāfiska platība un tie notiek vienlaicīgi vai vienā mirklī izplatās daudzās valstīs. ***Kiberdrošība ir svarīga, lai aizsargātu mūsu Eiropas vērtības un nodrošinātu mūsu demokrātiju darbību, aizsargājot mūsu vēlēšanu infrastruktūru un demokrātiskās procedūras no jebkādas ārvalstu iejaukšanās.***

Grozījums Nr. 3

Regulas priekšlikums
2.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(2a) Kiberdrošībai ir izšķiroša nozīme, lai nodrošinātu mūsu Savienības drošību un novērstu to, ka ļaunprātīgi valstiski un nevalstiski rīcībspēki apdraud mūsu demokrātiju, ekonomiku un drošību. Nedrīkst pieļaut sadrumstalotu vidi, jo šāda situācija nebūtu piemērota pieeja, sevišķi saskaroties ar nākotnes liela mēroga kiberuzbrukumiem, kas vērsti pret vairākām dalībvalstīm vienlaikus vai transnacionālu kritisko infrastruktūru. Tādēļ ir jānosaka Savienības struktūra, kas darbotos kā koordinācijas platforma visiem pašreizējiem un turpmākajiem kiberdrošības instrumentiem, fondiem un mehānismiem.

Grozījums Nr. 4

Regulas priekšlikums
3. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(3) Ir jāstiprina rūpniecības un pakalpojumu nozaru konkurētspēja Savienībā visā digitalizētajā ekonomikā un jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā tirgus kiberdrošību. Trijos dažādos konferences par Eiropas nākotni[16] priekšlikumos ir ieteikts palielināt pilsoņu, uzņēmumu un vienību, kuras darbina kritisko infrastruktūru, noturību pret augošo kiberdrošības apdraudējumu, kas spēj nodarīt postu sabiedrībai un tautsaimniecībai. Tāpēc vajag ieguldīt infrastruktūrā un pakalpojumos, kas palīdzēs veicīgāk atklāt kiberapdraudējumu un kiberincidentus un uz tiem reaģēt, un palīdzēt dalībvalstīm labāk sagatavoties ievērojamiem un plašiem kiberincidentiem un dot tiem pretsparu. Savienībai arī jāpalielina savas spējas šajās jomās, galvenokārt datu ***vākšanai*** un ***kiberapdraudējuma*** un ***kiberincidentu analīzei***.	(3) Ir jāstiprina rūpniecības un pakalpojumu nozaru konkurētspēja Savienībā visā digitalizētajā ekonomikā un jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā tirgus kiberdrošību. Trijos dažādos konferences par Eiropas nākotni[16] priekšlikumos ir ieteikts palielināt pilsoņu, uzņēmumu un vienību, kuras darbina kritisko infrastruktūru, noturību pret augošo kiberdrošības apdraudējumu, kas spēj nodarīt postu sabiedrībai un tautsaimniecībai. Tāpēc vajag ieguldīt infrastruktūrā un pakalpojumos, kas palīdzēs veicīgāk atklāt kiberapdraudējumu un kiberincidentus un uz tiem reaģēt, un palīdzēt dalībvalstīm labāk sagatavoties ievērojamiem un plašiem kiberincidentiem un dot tiem pretsparu. Savienībai ***būtu*** arī jāpalielina savas spējas šajās jomās, galvenokārt datu ***par kiberapdraudējumiem un kiberincidentiem vākšanā*** un ***analīzē, kā arī spēja proaktīvi rīkoties*** un ***izlēmīgi reaģēt uz kiberapdraudējumiem un kiberincidentiem***.
_____	_____
https://futureu.europa.eu/lv/?locale=lv	https://futureu.europa.eu/lv/?locale=lv

Grozījums Nr. 5

Regulas priekšlikums
4. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(4) Savienība jau ir noteikusi vairākus pasākumus, kam jāmazina kritisko infrastruktūru un vienību neaizsargātība un jāuzlabo to noturība pret kiberapdraudējumu, to vidū: Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555[17], Komisijas Ieteikums (ES) 2017/1584[18], Eiropas Parlamenta un Padomes Direktīva 2013/40/ES[19] un	(4) Savienība jau ir noteikusi vairākus pasākumus, kam jāmazina kritisko infrastruktūru un vienību neaizsargātība un jāuzlabo to noturība pret kiberapdraudējumu, to vidū: Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555[17], Komisijas Ieteikums (ES) 2017/1584[18], Eiropas Parlamenta un Padomes Direktīva 2013/40/ES[19] un

Eiropas Parlamenta un Padomes Regula (ES) 2019/881[20]. Bez tam Padomes ieteikumā par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai dalībvalstis tiek aicinātas veikt steidzamus un efektīvus pasākumus un lojāli, efektīvi, solidāri un koordinēti sadarboties savā starpā, ar Komisiju un citām attiecīgajām publiskajām iestādēm, kā arī ar attiecīgajām vienībām, lai pamatpakalpojumu sniegšanai iekšējā tirgū izmantoto kritisko infrastruktūru padarītu noturīgāku.

[17] 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 (OV L 333, 27.12.2022.).

Eiropas Parlamenta un Padomes Regula (ES) 2019/881[20]. Bez tam Padomes ieteikumā par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai dalībvalstis tiek aicinātas veikt steidzamus un efektīvus pasākumus un lojāli, efektīvi, ***proaktīvi,*** solidāri un koordinēti sadarboties savā starpā, ar Komisiju un citām attiecīgajām publiskajām iestādēm, kā arī ar attiecīgajām vienībām, lai pamatpakalpojumu sniegšanai iekšējā tirgū izmantoto kritisko infrastruktūru padarītu noturīgāku. ***Turklāt Savienība 2022. gada martā apstiprināja un sāka īstenot Stratēģisko kompasu drošībai un aizsardzībai, kurā cita starpā galvenā uzmanība pievērsta kiberdrošības stiprināšanai un starptautiskās sadarbības uzlabošanai ar līdzīgi domājošiem sabiedrotajiem un demokrātiskajiem partneriem, jo īpaši šajā jautājumā. Turklāt kiberdrošība bija viens no centrālajiem punktiem nesen, proti, 2023. gada janvārī, sagatavotajā Trešajā kopīgajā deklarācijā par ES un NATO sadarbību. Jo īpaši ES un NATO darba grupas galīgajā novērtējuma ziņojumā tika ieteikts pilnībā izmantot sinerģijas starp ES un NATO[1], tostarp paraugprakses apmaiņu starp civilajiem un militārajiem dalībniekiem par attiecīgo ar kibertelpu saistītās politikas un tiesību aktu īstenošanu.***

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

[17] 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 (OV L 333, 27.12.2022.).

[18] Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (OV L 239, 19.9.2017., 36. lpp.).

[19] Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI (OV L 218, 14.8.2013., 8. lpp.).

[20] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

[18] Komisijas Ieteikums (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm (OV L 239, 19.9.2017., 36. lpp.).

[19] Eiropas Parlamenta un Padomes Direktīva 2013/40/ES (2013. gada 12. augusts) par uzbrukumiem informācijas sistēmām, un ar kuru aizstāj Padomes Pamatlēmumu 2005/222/TI (OV L 218, 14.8.2013., 8. lpp.).

[20] Eiropas Parlamenta un Padomes Regula (ES) 2019/881 (2019. gada 17. aprīlis) par ENISA (Eiropas Savienības Kiberdrošības aģentūra) un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju, un ar ko atceļ Regulu (ES) Nr. 526/2013 (Kiberdrošības akts) (OV L 151, 7.6.2019., 15. lpp.).

Grozījums Nr. 6

Regulas priekšlikums
6. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(6) 2022. gada 10. novembrī pieņemtajā Kopīgajā paziņojumā par ES kiberaizsardzības politiku[22] tika izziņota ES kiberdrošības solidaritātes iniciatīva ar šādiem mērķiem: kopīgu ES spēju atklāt kiberapdraudējumu, apzināties stāvokli un reaģēt stiprināšana, veicinot ES drošības operāciju centru (DOC) infrastruktūras izvēršanu, atbalstot ES līmeņa kiberdrošības rezervju pakāpenisku izveidi ar pakalpojumiem no uzticamiem privātiem pakalpojumu sniedzējiem un iespējamas kritisko vienību neaizsargātības pārbaudi uz ES riska novērtēšanas pamata.	(6) 2022. gada 10. novembrī pieņemtajā Kopīgajā paziņojumā par ES kiberaizsardzības politiku[22] tika izziņota ES kiberdrošības solidaritātes iniciatīva ar šādiem mērķiem: kopīgu ES spēju atklāt kiberapdraudējumu, apzināties stāvokli un reaģēt stiprināšana, veicinot ES drošības operāciju centru (DOC) infrastruktūras izvēršanu, atbalstot ES līmeņa kiberdrošības rezervju pakāpenisku izveidi ar pakalpojumiem no uzticamiem privātiem pakalpojumu sniedzējiem un iespējamas kritisko vienību neaizsargātības pārbaudi uz ES riska novērtēšanas pamata. ***Turklāt, kā uzsvērts Padomes secinājumos par ES kiberaizsardzības politiku[1], arī strauji mainīgā kiberapdraudējumu aina un tehnoloģiskās attīstības ātrā gaita parāda, ka ir jāuzlabo civilā un militārā***

koordinācija un sadarbība.

[1] Padomes secinājumi par ES kiberaizsardzības politiku, kurus Padome apstiprināja 2023. gada 22. maija sanāksmē (9618/23).

---

[22] Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika", JOIN/2022/49 final.

---

[22] Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika", JOIN/2022/49 final.

Grozījums Nr. 7

Regulas priekšlikums
6.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(6a) Ņemot vērā, ka robežas starp civilo un militāro pasauli kļūst arvien neskaidrākas un abās tiek izmantoti vieni un tie paši kiberrīki un tehnoloģijas, digitālajai jomai ir vajadzīga visaptveroša un holistiska pieeja. Ja notiek plaša mēroga kiberdrošības incidents un krīze, kurā iesaistīta vairāk nekā viena dalībvalsts, būtu jānodrošina pienācīga krīžu pārvarēšana un pārvaldība. Šādām struktūrām būtu jāorganizē informācijas apmaiņa, koordinācija un sadarbība ar Savienības ārējās drošības un krīžu militārās pārvarēšana struktūrām un dalībvalstu struktūrām, kas atbild par drošību un aizsardzību (kiberaizsardzības kopiena). Tam vajadzētu attiekties arī uz kopējās drošības un aizsardzības politikas operācijām un misijām, ko Savienība veic, lai nodrošinātu mieru un stabilitāti kaimiņvalstīs un ārpus tām.

Grozījums Nr. 8

Regulas priekšlikums
7. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(7) Ir jāstiprina kiberapdraudējuma un kiberincidentu atklāšana un stāvokļa apzināšanās visā Savienībā un solidaritāte, uzlabojot dalībvalstu un Savienības gatavību un spējas reaģēt uz ievērojamiem un plašiem kiberincidentiem. Tādēļ Eiropas mērogā jāievieš DOC infrastruktūra (Eiropas kibervairogs), lai veidotu un uzlabotu kopīgas spējas atklāt apdraudējumu un apzināties stāvokli; jāiedibina kiberavārijas mehānisms, kas palīdzētu dalībvalstīm sagatavoties ievērojamiem un plašiem kiberincidentiem, uz tiem reaģēt un no tiem tūlīt atkopties; jāiedibina kiberincidentu izskatīšanas mehānisms konkrētu ievērojamu vai plašu kiberincidentu izskatīšanai un novērtēšanai. Šīs darbības neskar Līguma par Eiropas Savienības darbību (LESD) 107. un 108. pantu.	(7) Ir jāstiprina kiberapdraudējuma un kiberincidentu atklāšana un stāvokļa apzināšanās visā Savienībā un solidaritāte, uzlabojot dalībvalstu un Savienības gatavību un spējas reaģēt uz ievērojamiem un plašiem kiberincidentiem. Tādēļ Eiropas mērogā jāievieš DOC infrastruktūra (Eiropas kibervairogs), lai veidotu un uzlabotu kopīgas spējas atklāt apdraudējumu un apzināties stāvokli; ***būtu*** jāiedibina kiberavārijas mehānisms, kas palīdzētu dalībvalstīm sagatavoties ievērojamiem un plašiem kiberincidentiem, ***arī tādiem, kuros iesaistītas vairākas dalībvalstis,*** uz tiem reaģēt un no tiem tūlīt atkopties. ***Ja iespējams un nepieciešams, kiberavārijas mehānismam būtu jāorganizē informācijas apmaiņa un sadarbība ar dalībvalstu aizsardzības iestādēm, un tam būtu jāsaņem atbalsts no ES iestādēm, struktūrām un aģentūrām (ES kiberaizsardzības kopiena);*** jāiedibina kiberincidentu izskatīšanas mehānisms konkrētu ievērojamu vai plašu kiberincidentu izskatīšanai un novērtēšanai***. Šādām jaunām struktūrām būtu arī jāatbalsta ES KDAP operācijas un misijas***. Šīs darbības neskar Līguma par Eiropas Savienības darbību (LESD) 107. un 108. pantu.

Grozījums Nr. 9

Regulas priekšlikums
11. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(11) Pareizai finanšu pārvaldībai vajadzīgi īpaši noteikumi par neizmantoto saistību un maksājumu apropriāciju pārnešanu uz priekšu. Ievērojot principu Savienības budžetu noteikt katru gadu, šai regulai, ņemot vērā kiberdrošības vides neprognozējamo, ārkārtējo un specifisko dabu, ir jāparedz iespējas pārnest uz	(11) Pareizai finanšu pārvaldībai vajadzīgi īpaši noteikumi par neizmantoto saistību un maksājumu apropriāciju pārnešanu uz priekšu. Ievērojot principu Savienības budžetu noteikt katru gadu, šai regulai, ņemot vērā kiberdrošības vides neprognozējamo, ārkārtējo un specifisko dabu, ir jāparedz iespējas pārnest uz

priekšu neizmantotus līdzekļus, kuri pārsniedz Finanšu regulā noteiktos, tā maksimalizējot kiberavārijas mehānisma spēju atbalstīt dalībvalstis kiberapdraudējuma efektīvā apkarošanā.	priekšu neizmantotus līdzekļus, kuri pārsniedz Finanšu regulā noteiktos, tā maksimalizējot kiberavārijas mehānisma spēju atbalstīt dalībvalstis kiberapdraudējuma efektīvā apkarošanā. ***Šie īpašie noteikumi arī ļautu sniegt ilgāka termiņa finansiālu atbalstu nākamās paaudzes īpaši drošu rīku un infrastruktūras kopīgam iepirkumam, lai uzlabotu kolektīvās atklāšanas spējas, izmantojot jaunāko mākslīgo intelektu (MI) un datu analīzi.***

Grozījums Nr. 10

Regulas priekšlikums
13. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(13) Katrai dalībvalstij valsts līmenī jānorīko publiska struktūra, dodot tai uzdevumu attiecīgajā dalībvalstī koordinēt kiberapdraudējuma atklāšanas darbības. Šiem DOC valsts līmenī jābūt par uzziņas avotu un vārteju dalībai Eiropas kibervairogā un jānodrošina, ka informācija par kiberapdraudējumu no publiskām un privātām vienībām tiek valsts līmenī efektīvi un racionalizēti izplatīta un apkopota.	(13) Katrai dalībvalstij valsts līmenī jānorīko publiska struktūra, dodot tai uzdevumu attiecīgajā dalībvalstī koordinēt kiberapdraudējuma atklāšanas darbības. Šiem DOC valsts līmenī jābūt par uzziņas avotu un vārteju dalībai Eiropas kibervairogā un jānodrošina, ka informācija par kiberapdraudējumu no publiskām un privātām vienībām tiek valsts līmenī efektīvi un racionalizēti izplatīta un apkopota. ***Ja iespējams un nepieciešams, DOC būtu arī jāļauj piedalīties aizsardzības vienībām, izveidojot "aizsardzības pīlāru" attiecībā uz pārvaldību un kopīgotās informācijas veidu, kā izklāstīts Kopīgajā paziņojumā par ES kiberaizsardzības politiku[1] un ko atbalsta Augstais pārstāvis.*** ***[1] Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika", JOIN/2022/49 final.***

Grozījums Nr. 11

Regulas priekšlikums
14. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(14) Eiropas kibervairoga sastāvā jāizveido vairāki pārrobežu kiberdrošības operāciju centri (“pārrobežu DOC”). Tajos apvienojami valstu DOC no vismaz trim dalībvalstīm, lai no pārrobežu apdraudējuma atklāšanas un informācijas kopīgošanas un pārvaldības būtu pilnīgs ieguvums. Pārrobežu DOC vispārīgajam mērķim jābūt stiprināt spējas analizēt, novērst un atklāt kiberdrošības apdraudējumu un atbalstīt kvalitatīvu izlūkdatu par kiberdrošības apdraudējumiem sagatavošanu, galvenokārt – daloties datos no dažādiem publiskiem vai privātiem avotiem, kā arī uzticamā vidē kopīgojot un koplietojot modernākos rīkus un kopīgi attīstot atklāšanas, analīzes un novēršanas spējas. Tiem jānodrošina jaunas papildu spējas, izmantojot un savstarpēji papildinot esošos DOC un datorincidentu reaģēšanas vienības (“CSIRT”) un citus attiecīgus drošībniekus.	(14) Eiropas kibervairoga sastāvā jāizveido vairāki pārrobežu kiberdrošības operāciju centri (“pārrobežu DOC”). Tajos apvienojami valstu DOC no vismaz trim dalībvalstīm, ***tostarp “aizsardzības pīlārs”,*** lai no pārrobežu apdraudējuma atklāšanas un informācijas kopīgošanas un pārvaldības būtu pilnīgs ieguvums. Pārrobežu DOC vispārīgajam mērķim jābūt stiprināt spējas analizēt, novērst un atklāt kiberdrošības apdraudējumu un atbalstīt kvalitatīvu izlūkdatu par kiberdrošības apdraudējumiem sagatavošanu, galvenokārt – daloties datos no dažādiem publiskiem vai privātiem ***un — ja nepieciešams un iespējams — militāriem*** avotiem***, ievērojot pietiekamus norādījumus par informācijas kopīgošanu***, kā arī uzticamā vidē kopīgojot un koplietojot modernākos rīkus un kopīgi attīstot atklāšanas, analīzes un novēršanas spējas. Tiem jānodrošina jaunas papildu spējas, izmantojot un savstarpēji papildinot esošos DOC un datorincidentu reaģēšanas vienības (“CSIRT”) un citus attiecīgus drošībniekus.

Grozījums Nr. 12

Regulas priekšlikums
15. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(15) Valstī kiberapdraudējuma novērošanu, atklāšanu un analīzi parasti nodrošina publisko un privāto vienību DOC apvienojumā ar CSIRT. Turklāt saskaņā ar Direktīvu (ES) 2022/2555 CSIRT apmainās ar informāciju CSIRT tīklā. Pārrobežu DOC jābūt jaunai spējai,	(15) Valstī kiberapdraudējuma novērošanu, atklāšanu un analīzi parasti nodrošina publisko un privāto vienību DOC apvienojumā ar CSIRT. Turklāt saskaņā ar Direktīvu (ES) 2022/2555 CSIRT apmainās ar informāciju CSIRT tīklā. Pārrobežu DOC jābūt jaunai spējai,

kas papildinātu CSIRT tīklu, sakopojot un kopīgojot publisku un privātu vienību datus par kiberdrošības apdraudējumu, tādu datu vērtību paaugstinot ar ekspertīzēm un kopīgi iegādātām infrastruktūrām un pašiem modernākajiem rīkiem, un veicinot Savienības spēju un ***tehnoloģiskās suverenitātes*** attīstību.	kas papildinātu CSIRT tīklu, sakopojot un kopīgojot publisku un privātu vienību datus par kiberdrošības apdraudējumu, tādu datu vērtību paaugstinot ar ekspertīzēm un kopīgi iegādātām infrastruktūrām un pašiem modernākajiem rīkiem, un veicinot Savienības spēju un ***noturības*** attīstību.

Grozījums Nr. 13

Regulas priekšlikums
16. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(16) Pārrobežu DOC jābūt centrālam punktam, kurā iespējams plaši sakopot attiecīgus datus un kiberapdraudējuma izlūkdatus, un jāizplata informācija par apdraudējumu lielā, daudzveidīgā dalībnieku kopā (piemēram, datorapdraudējuma reaģēšanas vienību ("CERT"), CSIRT, informācijas apmaiņas un analīzes centru (ISAC), kritisko infrastruktūru operatoru vidū). Informācijā, ar kuru apmainās pārrobežu DOC dalībnieki, var būt dati no tīkliem un sensoriem, apdraudējuma izlūkdatu plūsmas, aizskāruma rādītāji un kontekstualizēta informācija par kiberincidentiem, apdraudējumu un vājajām vietām. Pārrobežu DOC arī jānoslēdz sadarbības nolīgumi ar citiem pārrobežu DOC.	(16) Pārrobežu DOC jābūt centrālam punktam, kurā iespējams plaši sakopot attiecīgus datus un kiberapdraudējuma izlūkdatus, un jāizplata informācija par apdraudējumu lielā, daudzveidīgā dalībnieku kopā (piemēram, datorapdraudējuma reaģēšanas vienību ("CERT"), CSIRT, informācijas apmaiņas un analīzes centru (ISAC), kritisko infrastruktūru operatoru***, kā arī kiberaizsardzības kopienas*** vidū). Informācijā, ar kuru apmainās pārrobežu DOC dalībnieki, var būt dati no tīkliem un sensoriem, apdraudējuma izlūkdatu plūsmas, aizskāruma rādītāji un kontekstualizēta informācija par kiberincidentiem, apdraudējumu un vājajām vietām. Pārrobežu DOC arī jānoslēdz sadarbības nolīgumi ar citiem pārrobežu DOC ***un militāro datorapdraudējumu reaģēšanas vienību operatīvo tīklu (MICNET), kad tas tiks izveidots***.

Grozījums Nr. 14

Regulas priekšlikums
17. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(17) Stāvokļa vienota apzināšanās attiecīgu iestāžu vidū ir nepieciešams priekšnoteikums visas Savienības gatavībai un koordinācijai ievērojamos un plašos kiberincidentos. Lai atbalstītu plašu kiberincidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru attiecīgas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām un aģentūrām, ar Direktīvu (ES) 2022/2555 ir izveidots EU-CyCLONe. Ieteikumā (ES) 2017/1584 par koordinētu reaģēšanu uz plašiem kiberincidentiem un krīzēm ir aplūkota visu attiecīgo subjektu loma. Direktīva (ES) 2022/2555 arī atsaucas uz Komisijas pienākumiem Savienības civilās aizsardzības mehānismā (UCPM), kas izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES, kā arī analītisku ziņojumu sniegšanā integrētajam krīzes politiskās reaģēšanas mehānismam (IPCR) ar Īstenošanas lēmumu (ES) 2018/1993 noteiktajā kārtībā. Tāpēc apstākļos, kad pārrobežu DOC iegūst informāciju, kas saistīta ar iespējamu vai notiekošu plašu kiberincidentu, tiem jāsniedz attiecīga informācija EU-CyCLONe, CSIRT tīklam un Komisijai. Proti, kopīgojamajā informācijā attiecīgos apstākļos var būt tehniska informācija, informācija par uzbrucēja vai potenciālā uzbrucēja dabu un motīviem un augstāka līmeņa netehniska informācija par iespējamu vai notiekošu plašu kiberincidentu. Šajā sakarā pienācīgi jāievēro princips “tiem, kam jāzina” un kopīgotās informācijas potenciālais jutīgums.	(17) Stāvokļa vienota apzināšanās attiecīgu iestāžu vidū ir nepieciešams priekšnoteikums visas Savienības gatavībai un koordinācijai ievērojamos un plašos kiberincidentos. Lai atbalstītu plašu kiberincidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru attiecīgas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām un aģentūrām, ar Direktīvu (ES) 2022/2555 ir izveidots EU-CyCLONe. Ieteikumā (ES) 2017/1584 par koordinētu reaģēšanu uz plašiem kiberincidentiem un krīzēm ir aplūkota visu attiecīgo subjektu loma. Direktīva (ES) 2022/2555 arī atsaucas uz Komisijas pienākumiem Savienības civilās aizsardzības mehānismā (UCPM), kas izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES, kā arī analītisku ziņojumu sniegšanā integrētajam krīzes politiskās reaģēšanas mehānismam (IPCR) ar Īstenošanas lēmumu (ES) 2018/1993 noteiktajā kārtībā. Tāpēc apstākļos, kad pārrobežu DOC iegūst informāciju, kas saistīta ar iespējamu vai notiekošu plašu kiberincidentu, tiem jāsniedz attiecīga informācija EU-CyCLONe, CSIRT tīklam***, kiberaizsardzības kopienai*** un Komisijai. Proti, kopīgojamajā informācijā attiecīgos apstākļos var būt tehniska informācija, informācija par uzbrucēja vai potenciālā uzbrucēja dabu un motīviem un augstāka līmeņa netehniska informācija par iespējamu vai notiekošu plašu kiberincidentu. Šajā sakarā pienācīgi jāievēro princips “tiem, kam jāzina” un kopīgotās informācijas potenciālais jutīgums.

Grozījums Nr. 15

Regulas priekšlikums
19. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(19) Lai uzticamā vidē nodrošinātu plašu datu apmaiņu par kiberdrošības apdraudējumu no dažādiem avotiem, vienībām, kuras piedalās Eiropas kibervairogā, jābūt apgādātām ar pašiem modernākajiem un ļoti drošiem rīkiem, iekārtām un infrastruktūru. Tam jāļauj uzlabot kolektīvās atklāšanas spējas un laikus brīdināt iestādes un attiecīgās vienības, it īpaši – izmantojot jaunākās mākslīgā intelekta un datu analīzes tehnoloģijas.	(19) Lai uzticamā vidē nodrošinātu plašu datu apmaiņu par kiberdrošības apdraudējumu no dažādiem avotiem, vienībām, kuras piedalās Eiropas kibervairogā, jābūt apgādātām ar pašiem modernākajiem un ļoti drošiem rīkiem, iekārtām un infrastruktūru***, izslēdzot kritisko produktu ar digitāliem elementiem piegādātājus, kuri rada augstu risku***. Tam jāļauj uzlabot kolektīvās atklāšanas spējas un laikus brīdināt iestādes un attiecīgās vienības, it īpaši – izmantojot jaunākās mākslīgā intelekta un datu analīzes tehnoloģijas. ***MI izmantošanā būtu jāparedz cilvēka virsvadība un jānodrošina pietiekams MI pratības līmenis, nepieciešamais atbalsts un pilnvaras šīs funkcijas veikšanai.***

Grozījums Nr. 16

Regulas priekšlikums
19.a apsvērums (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(19a) Saskaņā ar Regulu [XX/XXXX (Kibernoturības akts)] vienībām, kas piedalās Eiropas kibervairogā, būtu jāievēro arī šajā regulā noteiktās prasības attiecībā uz visiem produktiem ar digitāliem elementiem. Ņemot vērā pieaugošos ekonomiskās atkarības radītos riskus, ir nepieciešams ar vienotu stratēģisku satvaru ES ekonomiskajai drošībai samazināt tādu kritiski svarīgo produktu piegādātāju izvēles iespēju, kuri rada augstu risku. Atkarība no tādiem kritiski svarīgu produktu ar digitāliem elementiem piegādātājiem, kuri rada augstu risku, ir saistīta ar stratēģisku risku, kam būtu jāpievēršas Savienības līmenī, jo īpaši attiecībā uz to, vai valsts iesaistās ekonomiskajā spiegošanā vai ekonomiskajā piespiešanā un tās tiesību

	akti nosaka patvaļīgu piekļuvi jebkāda veida uzņēmuma darbībām vai datiem, jo īpaši tad, ja kritiskie produkti ir paredzēti Direktīvā (ES) 2022/2555 minēto būtisko vienību lietošanai.

Grozījums Nr. 17

Regulas priekšlikums
20. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(20) Vācot un kopīgojot datus un ar tiem apmainoties, Eiropas kibervairogam jāstiprina Savienības tehnoloģiskā suverenitāte. Kvalitatīvu kūrētu datu sakopošanai arī jāveicina progresīvu mākslīgā intelekta un datu analīzes tehnoloģiju attīstība. Tā jāsekmē, Eiropas kibervairogu savienojot ar Eiropas augstas veiktspējas datošanas infrastruktūru, kas izveidota ar Padomes Regulu (ES) 2021/1173[25].	(20) Vācot un kopīgojot datus un ar tiem apmainoties, Eiropas kibervairogam ***būtu*** jāstiprina Savienības tehnoloģiskā suverenitāte***, tās stratēģiskā autonomija, konkurētspēja un noturība***. Kvalitatīvu kūrētu datu sakopošanai arī jāveicina progresīvu mākslīgā intelekta un datu analīzes tehnoloģiju attīstība. Tā jāsekmē, Eiropas kibervairogu savienojot ar Eiropas augstas veiktspējas datošanas infrastruktūru, kas izveidota ar Padomes Regulu (ES) 2021/1173[25].
[25] Padomes Regula (ES) 2021/1173 (2021. gada 13. jūlijs) par Eiropas Augstas veiktspējas datošanas kopuzņēmuma izveidi un ar ko atceļ Regulu (ES) 2018/1488 (OV L 256, 19.7.2021., 3. lpp.).	[25] Padomes Regula (ES) 2021/1173 (2021. gada 13. jūlijs) par Eiropas Augstas veiktspējas datošanas kopuzņēmuma izveidi un ar ko atceļ Regulu (ES) 2018/1488 (OV L 256, 19.7.2021., 3. lpp.).

Grozījums Nr. 18

Regulas priekšlikums
25. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(25) Kiberavārijas mehānismam jāparedz atbalsts dalībvalstīm, papildinot to pasākumus un resursus, un citas pastāvošas atbalsta iespējas, kad jāreaģē uz ievērojamiem un plašiem kiberincidentiem un nekavējoties jāatkopjas no tiem,	(25) Kiberavārijas mehānismam jāparedz atbalsts dalībvalstīm, papildinot to pasākumus un resursus, un citas pastāvošas atbalsta iespējas, kad jāreaģē uz ievērojamiem un plašiem kiberincidentiem un nekavējoties jāatkopjas no tiem,

piemēram, pakalpojumi, ko sniedz Eiropas Savienības Kiberdrošības aģentūra (“ENISA”) saskaņā ar tās pilnvarām, koordinēta reaģēšana un CSIRT tīkla palīdzība, EU-CyCLONe sniegtais seku mazināšanas atbalsts, kā arī dalībvalstu savstarpējā palīdzība, arī LES 42. panta 7. punkta kontekstā, PESCO ātrās kiberreaģēšanas ***vienībām26*** un ātrās hibrīdreaģēšanas ***vienībām***. Tam jāapmierina vajadzība nodrošināt, ka ir pieejami specializēti līdzekļi, kas atbalsta gatavību kiberincidentiem un reaģēšanu uz tiem visā Savienībā un trešās valstīs.

piemēram, pakalpojumi, ko sniedz Eiropas Savienības Kiberdrošības aģentūra (“ENISA”) saskaņā ar tās pilnvarām, koordinēta reaģēšana un CSIRT tīkla palīdzība, EU-CyCLONe sniegtais seku mazināšanas atbalsts, kā arī dalībvalstu savstarpējā palīdzība, arī LES 42. panta 7. punkta kontekstā, PESCO ātrās kiberreaģēšanas ***vienības[1], jaunais PESCO projekta Kibertelpas un informācijas telpas koordinācijas centrs (CIDCC) un ES Kiberaizsardzības koordinācijas centrs (EUCDCC), kas atbilstīgi ierosinājumam pārņemtu tā funkcijas,*** un ātrās hibrīdreaģēšanas ***vienības***. Tam jāapmierina vajadzība nodrošināt, ka ir pieejami specializēti līdzekļi, kas atbalsta gatavību kiberincidentiem un reaģēšanu uz tiem visā Savienībā un trešās valstīs***, jo īpaši ES kandidātvalstīs, kuras ir pieskaņojušās ES kopējai ārpolitikai un drošības politikai un kopējai drošības un aizsardzības politikai, atbalstot tās kiberspēju veidošanā un uzlabojot minēto kandidātvalstu savstarpējo pārrobežu un reģionālo sadarbību kiberjomā***.

[1] Padomes Lēmums (KĀDP) 2017/2315 (2017. gada 11. decembris), ar ko izveido pastāvīgo strukturēto sadarbību (PESCO) un nosaka iesaistīto dalībvalstu sarakstu.

---

[26] Padomes Lēmums (KĀDP) 2017/2315 (2017. gada 11. decembris), ar ko izveido pastāvīgo strukturēto sadarbību (PESCO) un nosaka iesaistīto dalībvalstu sarakstu.

[26] Padomes Lēmums (KĀDP) 2017/2315 (2017. gada 11. decembris), ar ko izveido pastāvīgo strukturēto sadarbību (PESCO) un nosaka iesaistīto dalībvalstu sarakstu.

Grozījums Nr. 19

Regulas priekšlikums
26. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(26) Šis instruments neskar procedūras un regulējumu, kuru mērķis ir koordinēt	(26) Šis instruments neskar procedūras un regulējumu, kuru mērķis ir koordinēt

Savienības līmeņa reaģēšanu krīzēs, it īpaši UCPM[27], IPCR[28], un Direktīvu (ES) 2022/2555. Tas var veicināt vai papildināt darbības, kuras tiek īstenotas LES 42. panta 7. punkta sakarā vai LESD 222. pantā noteiktajos apstākļos. ***Attiecīgā gadījumā*** šā instrumenta izmantošana jākoordinē arī ar kiberdiplomātijas rīkkopas pasākumu īstenošanu.	Savienības līmeņa reaģēšanu krīzēs, it īpaši UCPM[27], IPCR[28], un Direktīvu (ES) 2022/2555. Tas var veicināt vai papildināt darbības, kuras tiek īstenotas LES 42. panta 7. punkta sakarā vai LESD 222. pantā noteiktajos apstākļos. Šā instrumenta izmantošana ***būtu*** jākoordinē arī ar kiberdiplomātijas rīkkopas pasākumu īstenošanu***, uzlabojot sadarbību stratēģiskā, operatīvā un tehniskā līmenī starp kiberaizsardzības kopienu un citām kiberkopienām, jo īpaši, lai stiprinātu spējas pret kiberdrošības apdraudējumiem no valstīm ārpus Savienības, tostarp ierobežojošus pasākumus, ko var izmantot, lai novērstu ļaunprātīgas kiberdarbības un reaģētu uz tām***.
[27] Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu (OV L 347, 20.12.2013., 924. lpp.).	[27] Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu (OV L 347, 20.12.2013., 924. lpp.).
[28] Integrētus krīzes situāciju politiskās reaģēšanas mehānismus (IPCR), un saskaņā ar Komisijas Ieteikumu (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.	[28] Integrētus krīzes situāciju politiskās reaģēšanas mehānismus (IPCR), un saskaņā ar Komisijas Ieteikumu (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.

Grozījums Nr. 20

Regulas priekšlikums
28. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(28) Direktīvā (ES) 2022/2555 ir noteikts, ka dalībvalstīm jāizraugās vai jāizveido viena vai vairākas kiberkrīzes pārvaldības iestādes un jānodrošina, ka tām ir pietiekami resursi savu uzdevumu efektīvai un lietderīgai pildīšanai. Tajā arī noteikts, ka dalībvalstīm ir jāapzina spējas, līdzekļi un procedūras, ko var izmantot krīzes gadījumā, kā arī jāpieņem valsts	(28) Direktīvā (ES) 2022/2555 ir noteikts, ka dalībvalstīm jāizraugās vai jāizveido viena vai vairākas kiberkrīzes pārvaldības iestādes un jānodrošina, ka tām ir pietiekami resursi savu uzdevumu efektīvai un lietderīgai pildīšanai. Tajā arī noteikts, ka dalībvalstīm ir jāapzina spējas, līdzekļi un procedūras, ko var izmantot krīzes gadījumā, kā arī jāpieņem valsts

plāns reaģēšanai uz plašiem kiberincidentiem un kiberkrīzēm, kurā ir noteikti plašu kiberincidentu un kiberkrīžu pārvaldības mērķi un kārtība. Dalībvalstīm arī jāizveido viena vai vairākas CSIRT, kurām uzticēti kiberincidentu risināšanas pienākumi saskaņā ar skaidri definētu procesu un aptverot vismaz nozares, apakšnozares un vienību veidus, kas ir minētās direktīvas darbības jomā, un sev jānodrošina pietiekami resursi savu uzdevumu faktiskai izpildei. Šī regula neskar Komisijas funkciju nodrošināt, ka dalībvalstis pilda Direktīvā (ES) 2022/2555 noteiktos pienākumus. Kiberavārijas mehānismam jāpalīdz veikt darbības, kuru mērķis ir stiprināt gatavību, kā arī reaģēšanas darbības kiberincidentā, lai mazinātu ievērojamu un plašu kiberincidentu ietekmi, atbalstītu tūlītēju atkopšanos un/vai atjaunotu būtiskāko dienestu darbību.	plāns reaģēšanai uz plašiem kiberincidentiem un kiberkrīzēm, kurā ir noteikti plašu kiberincidentu un kiberkrīžu pārvaldības mērķi un kārtība. Dalībvalstīm arī jāizveido viena vai vairākas CSIRT, kurām uzticēti kiberincidentu risināšanas pienākumi saskaņā ar skaidri definētu procesu un aptverot vismaz nozares, apakšnozares un vienību veidus, kas ir minētās direktīvas darbības jomā, un sev jānodrošina pietiekami resursi savu uzdevumu faktiskai izpildei. Šī regula neskar Komisijas funkciju nodrošināt, ka dalībvalstis pilda Direktīvā (ES) 2022/2555 noteiktos pienākumus. Kiberavārijas mehānismam jāpalīdz veikt darbības, kuru mērķis ir stiprināt gatavību, kā arī reaģēšanas darbības kiberincidentā, lai mazinātu ievērojamu un plašu kiberincidentu ietekmi, atbalstītu tūlītēju atkopšanos un/vai atjaunotu būtiskāko dienestu darbību***, pienācīgi izmantojot virkni aizsardzības iespēju, kas pieejamas civilajām un militārajām kopienām***.

Grozījums Nr. 21

Regulas priekšlikums
29. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(29) Lai gatavības darbību ietvaros veicinātu konsekventu pieeju un stiprinātu drošību visā Savienībā un tās iekšējā tirgū, jāsniedz atbalsts koordinētai tādu vienību kiberdrošības pārbaudei un novērtēšanai, kuras darbojas saskaņā ar Direktīvu (ES) 2022/2555 apzinātās ļoti kritiskās nozarēs. Šajā nolūkā Komisijai ar ENISA atbalstu un sadarbībā ar TID sadarbības grupu, kas izveidota ar Direktīvu (ES) 2022/2555, regulāri jānosaka attiecīgās nozares vai apakšnozares, kurām jābūt tiesīgām saņemt finansiālu atbalstu koordinētai pārbaudei Savienības līmenī. Nozares vai apakšnozares jāizraugās no Direktīvas (ES) 2022/2555 I pielikuma (“Sevišķi kritiskās	(29) Lai gatavības darbību ietvaros veicinātu konsekventu pieeju un stiprinātu drošību visā Savienībā un tās iekšējā tirgū, jāsniedz atbalsts koordinētai tādu vienību kiberdrošības pārbaudei un novērtēšanai, kuras darbojas saskaņā ar Direktīvu (ES) 2022/2555 apzinātās ļoti kritiskās nozarēs. Šajā nolūkā Komisijai ar ENISA atbalstu un sadarbībā ar TID sadarbības grupu, kas izveidota ar Direktīvu (ES) 2022/2555, regulāri jānosaka attiecīgās nozares vai apakšnozares, kurām jābūt tiesīgām saņemt finansiālu atbalstu koordinētai pārbaudei Savienības līmenī. ***Attiecīgā gadījumā Eiropas Ārējās darbības dienests (EĀDD), jo īpaši ar ES Izlūkošanas centra***

nozares”). Koordinētās pārbaudes pamatā jābūt kopīgiem riska scenārijiem un metodikai. Nozaru atlasē un riska scenāriju izstrādē jāņem vērā attiecīgie Savienības mēroga riska novērtējumi un riska scenāriji, ieskaitot izvairīšanos no dublēšanās, piemēram, riska izvērtēšana un riska scenāriji, kurus izmantot aicināts Padomes secinājumos par Eiropas Savienības pozīcijas izstrādi kiberlietās, kas jāveic Komisijai, Augstajam pārstāvim un TID sadarbības grupai, koordinējoties ar attiecīgām civilām un militārām struktūrām un aģentūrām un izveidotiem tīkliem, to vidū EU-CyCLONe, kā arī sakaru tīklu un infrastruktūru riska novērtējums, kas pieprasīts Nevēras kopīgajā ministru aicinājumā un ko veic TID sadarbības grupa ar Komisijas un ENISA atbalstu un sadarbībā ar Eiropas Elektronisko sakaru regulatoru iestādi (BEREC), koordinētā riska novērtēšana, kas veicama saskaņā ar Direktīvas (ES) 2022/2555 22. pantu, un digitālās darbības noturības pārbaude, kas paredzēta Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554***29***. Nozaru atlasē jāņem vērā arī Padomes ieteikums par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai.

(INTCEN) un tā Hibrīddraudu analīzes vienības starpniecību, ar Eiropas Savienības Militārā štāba (ESMŠ) Izlūkošanas direktorāta atbalstu vienotajā izlūkdatu analīzes procedūrā (SIAC), arī būtu jāiesaista, lai sniegtu atjauninātus novērtējumus un tādējādi palīdzētu identificēt nozares vai apakšnozares***, kuras būtu*** jāizraugās no Direktīvas (ES) 2022/2555 I pielikuma (“Sevišķi kritiskās nozares”). Koordinētās pārbaudes pamatā jābūt kopīgiem riska scenārijiem un metodikai***. Šīm pārbaudēm vajadzētu būt arī svarīgām, lai uzlabotu sadarbību starp civilām un militārām vienībām. Tādēļ, organizējot mācības, Komisijai, EĀDD un ENISA būtu sistemātiski jāapsver citu kiberkopienu, piemēram, Eiropas Aizsardzības aģentūras (EAA), dalībnieku un citu attiecīgo struktūru iesaistīšana.*** Nozaru atlasē un riska scenāriju izstrādē jāņem vērā attiecīgie Savienības mēroga riska novērtējumi un riska scenāriji, ieskaitot izvairīšanos no dublēšanās, piemēram, riska izvērtēšana un riska scenāriji, kurus izmantot aicināts Padomes secinājumos par Eiropas Savienības pozīcijas izstrādi kiberlietās, kas jāveic Komisijai, Augstajam pārstāvim un TID sadarbības grupai, koordinējoties ar attiecīgām civilām un militārām struktūrām un aģentūrām un izveidotiem tīkliem, to vidū EU-CyCLONe, kā arī sakaru tīklu un infrastruktūru riska novērtējums, kas pieprasīts Nevēras kopīgajā ministru aicinājumā un ko veic TID sadarbības grupa ar Komisijas un ENISA atbalstu un sadarbībā ar Eiropas Elektronisko sakaru regulatoru iestādi (BEREC), koordinētā riska novērtēšana, kas veicama saskaņā ar Direktīvas (ES) 2022/2555 22. pantu, un digitālās darbības noturības pārbaude, kas paredzēta Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554***[1]***. Nozaru atlasē jāņem vērā arī Padomes ieteikums par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai.

[1] Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011.

---

[29] Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011.

---

[29] Eiropas Parlamenta un Padomes Regula (ES) 2022/2554 (2022. gada 14. decembris) par finanšu nozares digitālās darbības noturību un ar ko groza Regulas (EK) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 un (ES) 2016/1011.

Grozījums Nr. 22

Regulas priekšlikums
32. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(32) Kiberavārijas mehānismam jāatbalsta palīdzība, ko dalībvalstis sniedz dalībvalstij, kuru skāris ievērojams vai plašs kiberincidents, ieskaitot CSIRT tīklu, kas noteikts Direktīvas (ES) 2022/2555 15. pantā. Jāļauj dalībvalstīm, kuras sniedz palīdzību, iesniegt lūgumus segt izmaksas, kas saistītas ar ekspertu vienību nosūtīšanu savstarpējai palīdzībai. Atlīdzināmajās izmaksās var būt kiberdrošības ekspertu ceļa, uzturēšanās un dienas naudas izdevumi.	(32) Kiberavārijas mehānismam jāatbalsta palīdzība, ko dalībvalstis sniedz dalībvalstij, kuru skāris ievērojams vai plašs kiberincidents, ieskaitot CSIRT tīklu, kas noteikts Direktīvas (ES) 2022/2555 15. pantā. ***Būtu*** jāļauj dalībvalstīm, kuras sniedz palīdzību, iesniegt lūgumus segt izmaksas, kas saistītas ar ekspertu vienību nosūtīšanu savstarpējai palīdzībai***, nodrošinot efektīvu koordināciju starp attiecīgajām ES programmām un instrumentiem, tostarp Eiropas Miera mehānismu (EMM), KĀDP un NDICI, kad tiek sniegta palīdzība trešām valstīm, jo īpaši Ukrainai un Moldovai***. Atlīdzināmajās izmaksās var būt kiberdrošības ekspertu ceļa, uzturēšanās un dienas naudas izdevumi.

Grozījums Nr. 23

Regulas priekšlikums
33. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(33) Lai atbalstītu reaģēšanas un tūlītējas atkopšanas darbības ievērojamu vai plašu kiberincidentu gadījumos, pakāpeniski jāveido Savienības līmeņa kiberdrošības rezerves, kas sastāv no pārvaldīto drošības pakalpojumu privāto sniedzēju pakalpojumiem. ES kiberdrošības rezervēm jānodrošina dienestu pieejamība un gatavība. Pakalpojumiem no ES kiberdrošības rezervēm jāpalīdz valstu iestādēm papildus darbībām valsts līmenī sniegt palīdzību skartajām vienībām, kuras darbojas kritiskās vai ļoti kritiskās nozarēs. Pieprasot atbalstu no ES kiberdrošības rezervēm, dalībvalstīm jāprecizē atbalsts, kas skartajai vienībai sniegts valsts līmenī, un tas jāņem vērā, novērtējot dalībvalsts pieprasījumu. Ar līdzīgiem nosacījumiem pakalpojumus no ES kiberdrošības rezervēm var izmantot arī Savienības iestāžu, struktūru un aģentūru atbalstīšanai.	(33) Lai atbalstītu reaģēšanas un tūlītējas atkopšanas darbības ievērojamu vai plašu kiberincidentu gadījumos, pakāpeniski jāveido Savienības līmeņa kiberdrošības rezerves, kas sastāv no pārvaldīto drošības pakalpojumu privāto sniedzēju pakalpojumiem. ES kiberdrošības rezervēm jānodrošina dienestu pieejamība un gatavība. Pakalpojumiem no ES kiberdrošības rezervēm jāpalīdz valstu iestādēm papildus darbībām valsts līmenī sniegt palīdzību skartajām vienībām, kuras darbojas kritiskās vai ļoti kritiskās nozarēs. Pieprasot atbalstu no ES kiberdrošības rezervēm, dalībvalstīm jāprecizē atbalsts, kas skartajai vienībai sniegts valsts līmenī, un tas jāņem vērā, novērtējot dalībvalsts pieprasījumu. Ar līdzīgiem nosacījumiem pakalpojumus no ES kiberdrošības rezervēm var izmantot arī Savienības iestāžu, struktūru un aģentūru***, tostarp KDAP misiju,*** atbalstīšanai.

Grozījums Nr. 24

Regulas priekšlikums
34. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(34) Lai izvēlētos privātos pakalpojumu sniedzējus pakalpojumu sniegšanai ES kiberdrošības rezervju sakarā, ir jānosaka minimālo kritēriju kopums, kas iekļaujams uzaicinājumā iesniegt piedāvājumus, lai atlasītu šos pakalpojumu sniedzējus, tādējādi nodrošinot, ka tiek apmierinātas to dalībvalstu iestāžu un vienību vajadzības, kuras darbojas kritiskās vai ļoti kritiskās nozarēs.	(34) Lai izvēlētos privātos pakalpojumu sniedzējus pakalpojumu sniegšanai ES kiberdrošības rezervju sakarā, ir jānosaka minimālo kritēriju kopums, kas iekļaujams uzaicinājumā iesniegt piedāvājumus, lai atlasītu šos pakalpojumu sniedzējus, tādējādi nodrošinot, ka tiek apmierinātas to dalībvalstu iestāžu un vienību vajadzības, kuras darbojas kritiskās vai ļoti kritiskās nozarēs***, ņemot vērā arī riskus, kas saistīti ar pakalpojumu sniedzēju no stratēģiskām konkurentvalstīm dalību, kas var radīt ekonomiskās drošības riskus, kā arī***

ietekmi uz Savienības stratēģisko drošību.

Grozījums Nr. 25

Regulas priekšlikums
36. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(36) Lai tuvinātu šīs regulas mērķus veicināt kopīgu stāvokļa apzināšanos, uzlabot Savienības noturību un sagādāt iespēju efektīvi reaģēt uz ievērojamiem un plašiem kiberincidentiem, EU-CyCLONe, CSIRT tīklam vai Komisijai jāvar lūgt ENISA izskatīt un novērtēt briesmas, vājās vietas un seku mazināšanas darbības konkrēta ievērojama vai plaša kiberincidenta sakarā. Pēc incidenta izskatīšanas un novērtēšanas ENISA sadarbībā ar attiecīgajām ieinteresētajām personām, ieskaitot privātā sektora, dalībvalstu, Komisijas un citu attiecīgo ES iestāžu, struktūru un aģentūru pārstāvjus, jāsagatavo incidenta pārskata ziņojums. Attiecībā uz privāto sektoru ENISA veido kanālus informācijas apmaiņai ar specializētiem pakalpojumu sniedzējiem, arī pārvaldītu drošības risinājumu pagādātājiem un pārdevējiem, lai palīdzētu izpildīt ENISA uzdevumu visā Savienībā panākt vienādi augstu kiberdrošību. Pamatojoties uz sadarbību ar ieinteresētajām personām, ieskaitot privāto sektoru, pārskata ziņojumam par konkrētiem incidentiem jābūt mērķim pēc incidenta novērtēt tā cēloņus, ietekmi un seku mazinājumu. Īpaša uzmanība jāpievērš to pārvaldīto drošības pakalpojumu sniedzēju ieguldījumam un pieredzei, kuri atbilst šīs regulas noteiktajiem visaugstākās profesionālās godprātības, objektivitātes un nepieciešamo tehnisko zināšanu nosacījumiem. Ziņojums jāiesniedz EU-CyCLONe, CSIRT tīklam un Komisijai un jāizmanto to darbā. Ja incidents ir saistīts ar trešu valsti, Komisijai par to jāinformē	(36) Lai tuvinātu šīs regulas mērķus veicināt kopīgu stāvokļa apzināšanos, uzlabot Savienības noturību un sagādāt iespēju efektīvi reaģēt uz ievērojamiem un plašiem kiberincidentiem, EU-CyCLONe, CSIRT tīklam vai Komisijai jāvar lūgt ENISA izskatīt un novērtēt briesmas, vājās vietas un seku mazināšanas darbības konkrēta ievērojama vai plaša kiberincidenta sakarā. ***Ņemot vērā drošas savienojamības sistēmas izstrādi, pamatojoties uz Eiropas kvantu sakaru infrastruktūru (EuroQCI) un Eiropas Savienības valdības satelītsakariem (GOVSATCOM), jo īpaši Galileo GNSS ieviešanu aizsardzības lietotājiem, jebkurā turpmākajā iespējamajā izstrādē būtu jāņem vērā "hiperkara" iespējamība tuvākā nākotnē, jo šāds karš kvantu datošanas ātrumu un sarežģītumu apvieno ar ļoti autonomām militārām sistēmām.*** Pēc incidenta izskatīšanas un novērtēšanas ENISA sadarbībā ar attiecīgajām ieinteresētajām personām, ieskaitot privātā sektora, dalībvalstu, Komisijas un citu attiecīgo ES iestāžu, struktūru un aģentūru pārstāvjus, jāsagatavo incidenta pārskata ziņojums. Attiecībā uz privāto sektoru ENISA veido kanālus informācijas apmaiņai ar specializētiem pakalpojumu sniedzējiem, arī pārvaldītu drošības risinājumu pagādātājiem un pārdevējiem, lai palīdzētu izpildīt ENISA uzdevumu visā Savienībā panākt vienādi augstu kiberdrošību. Pamatojoties uz sadarbību ar ieinteresētajām personām, ieskaitot privāto sektoru, pārskata ziņojumam par konkrētiem incidentiem jābūt mērķim pēc

arī Augstais pārstāvis.	incidenta novērtēt tā cēloņus, ietekmi un seku mazinājumu. Īpaša uzmanība jāpievērš to pārvaldīto drošības pakalpojumu sniedzēju ieguldījumam un pieredzei, kuri atbilst šīs regulas noteiktajiem visaugstākās profesionālās godprātības, objektivitātes un nepieciešamo tehnisko zināšanu nosacījumiem. Ziņojums jāiesniedz EU-CyCLONe, CSIRT tīklam un Komisijai un jāizmanto to darbā. Ja incidents ir saistīts ar trešu valsti, Komisijai par to jāinformē arī Augstais pārstāvis***, EĀDD un jebkura KDAP misija incidenta skartajā valstī, izmantojot to galveno mītni***.

Grozījums Nr. 26

Regulas priekšlikums
37. apsvērums

Komisijas ierosinātais teksts	*Grozījums*
(37) Ņemot vērā kiberdrošības uzbrukumu neparedzamību un to, ka tie mēdz neaprobežoties ar noteiktu ģeogrāfisku apgabalu un draud pārmesties uz citiem apgabaliem, tad, stiprinot kaimiņvalstu noturību un spēju efektīvi reaģēt uz ievērojamiem un plašiem kiberdrošības incidentiem, tiek veicināta visas Savienības aizsardzība. Tāpēc ar programmu "Digitālā Eiropa" ***asociētās trešās valstis var saņemt atbalstu*** no ES kiberdrošības rezervēm, ***ja tāds*** ir ***paredzēts attiecīgajā asociācijas nolīgumā ar programmu "Digitālā Eiropa"***. Savienībai jāatbalsta finansējums asociētajām trešajām valstīm attiecīgo šīm valstīm paredzēto partnerību un finansēšanas instrumentu ietvaros. Atbalstam jāaptver dienesti, kas paredzēti reaģēšanai uz ievērojamiem vai plašiem kiberdrošības incidentiem un tūlītējai atkopšanai. Šīs regulas nosacījumi ES kiberdrošības rezervēm un uzticamiem pakalpojumu sniedzējiem jāpiemēro, arī atbalstot ar programmu "Digitālā Eiropa"	(37) Ņemot vērā kiberdrošības uzbrukumu neparedzamību un to, ka tie mēdz neaprobežoties ar noteiktu ģeogrāfisku apgabalu un draud pārmesties uz citiem apgabaliem, tad, stiprinot kaimiņvalstu***, jo īpaši Ukrainas un Moldovas,*** noturību un spēju efektīvi reaģēt uz ievērojamiem un plašiem kiberdrošības incidentiem, tiek veicināta visas Savienības aizsardzība. Tāpēc ar programmu "Digitālā Eiropa" ***asociētajām trešām valstīm būtu jāsaņem atbalsts*** no ES kiberdrošības rezervēm***. Atbalsts būtu jāpiemēro arī tām trešām valstīm***, ***kurās ir izvietota KDAP misija ar īpašām pilnvarām stiprināt noturību pret hibrīddraudiem, tostarp kiberdraudiem, vai kurās*** ir ***pieņemts EMM palīdzības pasākums, lai stiprinātu valsts kibernoturību***. Savienībai jāatbalsta finansējums asociētajām trešajām valstīm attiecīgo šīm valstīm paredzēto partnerību un finansēšanas instrumentu ietvaros. Atbalstam jāaptver dienesti, kas paredzēti reaģēšanai uz ievērojamiem vai plašiem

asociētās trešās valstis.	kiberdrošības incidentiem un tūlītējai atkopšanai. Šīs regulas nosacījumi ES kiberdrošības rezervēm un uzticamiem pakalpojumu sniedzējiem jāpiemēro, arī atbalstot ar programmu "Digitālā Eiropa" asociētās trešās valstis.

Grozījums Nr. 27

Regulas priekšlikums
1. pants – 1. punkts – c apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
c) Eiropas kiberincidentu izskatīšanas mehānisma izveide ievērojamu vai plašu incidentu izskatīšanai un novērtēšanai.	c) Eiropas kiberincidentu izskatīšanas mehānisma izveide ievērojamu vai plašu incidentu ***vai draudu*** izskatīšanai un novērtēšanai.

Grozījums Nr. 28

Regulas priekšlikums
1. pants – 2. punkts – a apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
a) stiprināt Savienības kiberapdraudējuma un kiberincidentu kopīgu atklāšanu un stāvokļa apzināšanos, tā ļaujot stiprināt Savienības rūpniecības un pakalpojumu nozaru konkurētspēju visā digitālajā ekonomikā un veicināt Savienības tehnoloģisko ***suverenitāti*** kiberdrošībā;	a) stiprināt Savienības kiberapdraudējuma un kiberincidentu kopīgu atklāšanu un stāvokļa apzināšanos, tā ļaujot stiprināt Savienības rūpniecības un pakalpojumu nozaru konkurētspēju visā digitālajā ekonomikā un veicināt Savienības tehnoloģisko ***noturību*** kiberdrošībā;

Grozījums Nr. 29

Regulas priekšlikums
1. pants – 2. punkts – b apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
b) visā Savienībā stiprināt to vienību gatavību, kuras darbojas kritiskās un ļoti kritiskās nozarēs, un stiprināt solidaritāti, attīstot spējas vienoti reaģēt ievērojama vai	b) visā Savienībā stiprināt to vienību gatavību, kuras darbojas kritiskās un ļoti kritiskās nozarēs, un stiprināt solidaritāti, attīstot spējas vienoti reaģēt ievērojama vai

plaša kiberincidenta gadījumā, arī darot pieejamu Savienības atbalstu ar programmu "Digitālā Eiropa" ("PDE") asociētajām trešajām valstīm ***reaģēšanai uz kiberincidentiem***;	plaša kiberincidenta gadījumā, arī darot pieejamu ***reaģēšanai uz kiberincidentiem paredzēto*** Savienības atbalstu ar programmu "Digitālā Eiropa" ("PDE") asociētajām trešajām valstīm ***vai tām trešām valstīm, kuras ir Savienības kandidātvalstis un kas nerīkojas pretrunā Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu. Dalībvalstīm savā kiberdrošības stratēģijā būtu jāiekļauj aktīva kiberaizsardzības programma, kurā būtu paredzētas regulāras, dalībvalstīm kopīgas apmācības un apmācības ar starptautisku organizāciju iesaisti. Šādai programmai būtu jānodrošina sinhronizēta reāllaika spēja atklāt, konstatēt, analizēt un mazināt apdraudējumus***;

Grozījums Nr. 30

Regulas priekšlikums
1. pants – 2.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	2.a samazināt sistēmiskos kiberdrošības riskus, ko rada atkarība no kritiski svarīga aprīkojuma no valstīm, kas rīkotos pretrunā Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu;

Grozījums Nr. 31

Regulas priekšlikums
2. pants – 2.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	"kiberaizsardzības kopiena" ir dalībvalstu aizsardzības iestādes, ko atbalsta ES iestādes, struktūras un aģentūras, kā izklāstīts Kopīgajā paziņojumā "ES

kiberaizsardzības politika" [1];

[1] Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika", JOIN/2022/49 final.

Grozījums Nr. 32

Regulas priekšlikums
3. pants – 2. punkts – 1. daļa – ba apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	ba) palīdz modernizēt visas kiberaizsardzības sistēmas, līdz ar MI sistēmu ieviešanu uzlabojot kiberaizsardzības spēju kvalitāti, un paātrina informācijas apmaiņu starp valstu DOC un pārrobežu DOC;

Grozījums Nr. 33

Regulas priekšlikums
3. pants – 2. punkts – 1. daļa – da apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(da) pārskata un izvērtē kritiskās kiberdrošības tehnoloģijas un aprīkojumu, ko DOC izmanto reaģēšanai uz kiberdrošības incidentiem, lai atklātu sistēmiskus riskus, kuri saistīti ar valstu ietekmi uz augsta riska piegādātājiem, kas kaitētu Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu;

Grozījums Nr. 34

Regulas priekšlikums
4. pants – 1. punkts – 2. daļa

Komisijas ierosinātais teksts	*Grozījums*
Tam ir spēja būt par uzziņas avotu un vārteju citām publiskām un privātām organizācijām valsts līmenī, lai vāktu un analizētu informāciju par kiberdrošības apdraudējumu un incidentiem un sekmētu pārrobežu DOC izveidi. Tas ir bruņots ar pašām modernākajām tehnoloģijām, kuras spēj atklāt, agreģēt un analizēt datus par kiberdrošības apdraudējumu un incidentiem.	Tam ir spēja būt par uzziņas avotu un vārteju citām publiskām un privātām organizācijām ***un nepieciešamības gadījumā militārajam sektoram*** valsts līmenī, lai vāktu un analizētu informāciju par kiberdrošības apdraudējumu un incidentiem un sekmētu pārrobežu DOC izveidi. Tas ir bruņots ar pašām modernākajām tehnoloģijām, kuras spēj atklāt, agreģēt un analizēt datus par kiberdrošības apdraudējumu un incidentiem.

Grozījums Nr. 35

Regulas priekšlikums
4. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Pēc uzaicinājuma izteikt ieinteresētību Eiropas Kiberdrošības kompetences centrs (ECCC) atlasa valstu DOC dalībai ar ECCC kopīgā rīku un infrastruktūru iepirkumā. ECCC var atlasītajiem valstu DOC piešķirt dotācijas šo rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 50 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet dalībvalsts sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras ECCC un valsts DOC noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.	2. Pēc uzaicinājuma izteikt ieinteresētību Eiropas Kiberdrošības kompetences centrs (ECCC) atlasa valstu DOC dalībai ar ECCC kopīgā rīku un infrastruktūru iepirkumā. ECCC var atlasītajiem valstu DOC piešķirt dotācijas šo rīku un infrastruktūru darbības finansēšanai ***ar stingru nosacījumu, ka šādus rīkus un infrastruktūru nodrošina uzticami pakalpojumu sniedzēji saskaņā ar 16. pantu.*** Savienības finansiālās iemaksas sedz līdz 50 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet dalībvalsts sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras ECCC un valsts DOC noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.

Grozījums Nr. 36

Regulas priekšlikums
5. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Pēc uzaicinājuma izteikt ieinteresētību ECCC atlasa mitināšanas konsorciju dalībai ar ECCC kopīgā rīku un infrastruktūru iepirkumā. ECCC var mitināšanas konsorcijam piešķirt dotāciju rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 75 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet mitināšanas konsorcijs sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras ECCC un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.	2. Pēc uzaicinājuma izteikt ieinteresētību ECCC atlasa mitināšanas konsorciju dalībai ar ECCC kopīgā rīku un infrastruktūru iepirkumā. ECCC var mitināšanas konsorcijam piešķirt dotāciju rīkus un infrastruktūru darbības finansēšanai ***ar stingru nosacījumu, ka šādus rīkus un infrastruktūru nodrošina uzticami pakalpojumu sniedzēji saskaņā ar 16. pantu***. Savienības finansiālās iemaksas sedz līdz 75 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet mitināšanas konsorcijs sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras ECCC un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.

Grozījums Nr. 37

Regulas priekšlikums
5. pants – 2.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	2.a Jebkura infrastruktūra vai pakalpojumu sniedzējs, kura izcelsme ir augsta riska trešā valstī, tiek automātiski izslēgti.

Grozījums Nr. 38

Regulas priekšlikums
6. pants – 1. punkts – ba apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	ba) tieši atbalsta iesaistīto dalībvalstu militāro un aizsardzības spēju stiprināšanu vai novērš tiešus un tūlītējus draudus to drošībai. Tā kā aizsardzības nozarē pastāvošo ievainojamību

	izmantošana var radīt būtiskus traucējumus un kaitējumu, aizsardzības nozares kiberdrošībai ir vajadzīgi īpaši pasākumi, lai nodrošinātu piegādes ķēžu drošību, jo īpaši tādu piegādes ķēdēs iesaistītu zemāka līmeņa vienību drošību, kurām nav nepieciešama piekļuve klasificētai informācijai, bet kuras varētu radīt nopietnus riskus visai nozarei. Īpaša uzmanība būtu jāpievērš jebkāda pārkāpuma iespējamai ietekmei un jebkādas iespējamas manipulācijas ar tīkla datiem apdraudējumam, kurš varētu padarīt kritiski svarīgus aizsardzības līdzekļus nelietojamus vai pat apturēt operētājsistēmu darbību, padarot tās neaizsargātas pret pārņemšanu.

Grozījums Nr. 39

Regulas priekšlikums
6. pants – 1. punkts – ba apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	(bb) atbalsta iesaistīto dalībvalstu aizsardzības spēju stiprināšanu vai novērš tiešus un tūlītējus draudus to drošībai, nodrošinot piegādes ķēžu drošību, jo īpaši tādu piegādes ķēdēs iesaistītu zemāka līmeņa struktūru drošību, kurām nav nepieciešama piekļuve klasificētai informācijai, bet kuras varētu nopietni apdraudēt visu nozari.

Grozījums Nr. 40

Regulas priekšlikums
7. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Ja pārrobežu DOC iegūst informāciju par potenciālu vai notiekošu plaša mēroga kiberincidentu, tie bez liekas kavēšanās sniedz attiecīgu informāciju EU-CyCLONe, CSIRT tīklam un Komisijai,	1. Ja pārrobežu DOC iegūst informāciju par potenciālu vai notiekošu plaša mēroga kiberincidentu, tie bez liekas kavēšanās sniedz attiecīgu informāciju EU-CyCLONe, CSIRT tīklam un Komisijai,

ņemot vērā to attiecīgās krīzes pārvarēšanas funkcijas saskaņā ar Direktīvu (ES) 2022/2555.	***tostarp Augstajam pārstāvim un EĀDD, ja informācija attiecas uz trešo valsti,*** ņemot vērā to attiecīgās krīzes pārvarēšanas funkcijas saskaņā ar Direktīvu (ES) 2022/2555.

Grozījums Nr. 41

Regulas priekšlikums
8. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Dalībvalstis, kuras piedalās Eiropas kibervairogā, Eiropas kibervairoga infrastruktūrai nodrošina augstu datu drošību un fizisko drošību un gādā, lai infrastruktūra tiek pienācīgi pārvaldīta un kontrolēta, to sargājot no apdraudējuma un nodrošinot tās un sistēmu drošību, ***ieskaitot*** to datu drošību, ar kuriem infrastruktūrā notiek apmaiņa.	1. Dalībvalstis, kuras piedalās Eiropas kibervairogā, Eiropas kibervairoga infrastruktūrai nodrošina augstu datu drošību un fizisko drošību un gādā, lai infrastruktūra tiek pienācīgi pārvaldīta un kontrolēta, to sargājot no apdraudējuma un nodrošinot tās un sistēmu drošību, ***mazinot risku un veicinot ES tehnoloģisko izcilību kritiski svarīgās nozarēs, tostarp pasākumus, lai ierobežotu vai izslēgtu augsta riska piegādātājus, kā arī aizsargātu*** to datu drošību, ar kuriem infrastruktūrā notiek apmaiņa.

Grozījums Nr. 42

Regulas priekšlikums
8. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Dalībvalstis, kuras piedalās Eiropas kibervairogā, nodrošina, ka informācijas kopīgošana Eiropas kibervairogā ar vienībām, kuras nav dalībvalstu publiskās struktūras, negatīvi neietekmē Savienības drošības intereses.	2. Dalībvalstis, kuras piedalās Eiropas kibervairogā, nodrošina, ka informācijas kopīgošana Eiropas kibervairogā ar vienībām, kuras nav dalībvalstu publiskās struktūras, negatīvi neietekmē Savienības drošības intereses ***un ka jebkāda informācijas apmaiņa ar augsta riska pakalpojumu sniedzējiem ir ierobežota un neskar Savienības drošību un stratēģiskās intereses***.

Grozījums Nr. 43

Regulas priekšlikums
8. pants – 3. punkts

Komisijas ierosinātais teksts	*Grozījums*
3. Komisija var pieņemt īstenošanas aktus, nosakot tehniskās prasības dalībvalstīm 1. un 2. punktā noteikto pienākumu izpildei. Minētos īstenošanas aktus pieņem saskaņā ar šīs regulas 21. panta 2. punktā minēto pārbaudes procedūru. Šajā darbībā Komisija ar Augstā pārstāvja atbalstu ievēro attiecīgā aizsardzības līmeņa drošības standartus, lai veicinātu sadarbību ar militārām iestādēm.	3. Komisija var pieņemt īstenošanas aktus, nosakot tehniskās prasības dalībvalstīm 1. un 2. punktā noteikto pienākumu izpildei. Minētos īstenošanas aktus pieņem saskaņā ar šīs regulas 21. panta 2. punktā minēto pārbaudes procedūru. Šajā darbībā Komisija ar Augstā pārstāvja atbalstu ievēro attiecīgā aizsardzības līmeņa drošības standartus, lai veicinātu sadarbību ar militārām iestādēm***, pienācīgi izmantojot visas civilās un militārās kopienas rīcībā esošās aizsardzības iespējas plašākai ES drošībai un aizsardzībai, un informē Eiropas Parlamentu***.

Grozījums Nr. 44

Regulas priekšlikums
9. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Kiberavārijas mehānisma īstenošanas darbības atbalsta ar finansēm no programmas "Digitālā Eiropa" un īsteno saskaņā ar Regulu (ES) 2021/694, sevišķi tās konkrēto mērķi Nr. 3.	2. Kiberavārijas mehānisma īstenošanas darbības atbalsta ar finansēm no programmas "Digitālā Eiropa" un īsteno saskaņā ar Regulu (ES) 2021/694, sevišķi tās konkrēto mērķi Nr. 3***, un ar Eiropas Miera mehānismu (EMM), ja palīdzības pasākumi tiek īstenoti attiecībā uz trešām valstīm, jo īpaši attiecībā uz Ukrainu un Moldovu***.

Grozījums Nr. 45

Regulas priekšlikums
10. pants – 1. punkts – a apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*

a) gatavības darbības, ieskaitot koordinētas gatavības pārbaudes visā Savienībā vienībām, kuras darbojas ļoti ***kritiskās nozarēs***;	a) gatavības darbības, ieskaitot koordinētas gatavības pārbaudes visā Savienībā vienībām, kuras darbojas ļoti ***kritiskos sektoros, piemēram, publiskajā infrastruktūrā, vēlēšanu infrastruktūrā, transportā, veselības aprūpē, finansēs, telekomunikācijā, pārtikas piegādē un nodrošinājumā visā Savienībā***;

Grozījums Nr. 46

Regulas priekšlikums
10. pants – 1. punkts – c apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
c) savstarpējas palīdzības darbības, kas ietver palīdzības sniegšanu no vienas dalībvalsts valsts iestādēm citai dalībvalstij, sevišķi tā, kā noteikts Direktīvas (ES) 2022/2555 11. panta 3. punkta f) apakšpunktā.	c) savstarpējas palīdzības darbības, kas ietver palīdzības sniegšanu no vienas dalībvalsts valsts iestādēm citai dalībvalstij, sevišķi tā, kā noteikts Direktīvas (ES) 2022/2555 11. panta 3. punkta f) apakšpunktā ***un saistībā ar LES 42. panta 7. punktu un LESD 222. pantu;***

Grozījums Nr. 47

Regulas priekšlikums
10. pants – 1. punkts – ca apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	ca) tāda kritiski svarīga aprīkojuma aizstāšana vai pakāpeniska atteikšanās no tā, ko piegādā augsta riska piegādātāji, kas būtu pretrunā Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu.

Grozījums Nr. 48

Regulas priekšlikums
11. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. TID sadarbības grupa sadarbībā ar Komisiju, ENISA ***un*** Augsto pārstāvi izstrādā kopīgus riska scenārijus un metodiku koordinētajiem pārbaudes pasākumiem.	2. TID sadarbības grupa sadarbībā ar Komisiju, ENISA***,*** Augsto pārstāvi***, EĀDD un— attiecīgā gadījumā — EAA*** izstrādā kopīgus riska scenārijus un metodiku koordinētajiem pārbaudes pasākumiem.

Grozījums Nr. 49

Regulas priekšlikums
12. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. ES kiberdrošības rezerves veido reaģēšanas uz incidentiem pakalpojumi no uzticamiem pakalpojumu sniedzējiem, kas atlasīti pēc 16. pantā noteiktajiem kritērijiem. Rezervēs ietilpst pakalpojumi, par kuriem iepriekš uzņemtas saistības. Pakalpojumi ir izvietojami visās dalībvalstīs.	2. ES kiberdrošības rezerves veido reaģēšanas uz incidentiem pakalpojumi no uzticamiem pakalpojumu sniedzējiem, kas atlasīti pēc 16. pantā noteiktajiem kritērijiem. Rezervēs ietilpst pakalpojumi, par kuriem iepriekš uzņemtas saistības. Pakalpojumi ir izvietojami visās dalībvalstīs ***un trešās valstīs, kas atbilst piemērojamajām šīs regulas prasībām***.

Grozījums Nr. 50

Regulas priekšlikums
12. pants – 3. punkts – b apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
b) Savienības iestādes, struktūras un aģentūras.	b) Savienības iestādes, struktūras un aģentūras***, tostarp KDAP misijas***.

Grozījums Nr. 51

Regulas priekšlikums
12. pants – 4. punkts

Komisijas ierosinātais teksts	*Grozījums*
4. Šā panta 3. punkta a) apakšpunktā minētie lietotāji izmanto ES kiberdrošības rezervju pakalpojumus, lai reaģētu vai	4. Šā panta 3. punkta a) apakšpunktā minētie lietotāji izmanto ES kiberdrošības rezervju pakalpojumus, lai reaģētu vai

atbalstītu reaģēšanu uz ievērojamiem vai plašiem incidentiem, kas ietekmē vienības, kuras darbojas ***kritiskās*** vai ļoti ***kritiskās nozarēs***, un tūlītēju atkopšanos no tiem.	atbalstītu reaģēšanu uz ievērojamiem vai plašiem incidentiem, kas ietekmē vienības, kuras darbojas ***kritiskos*** vai ļoti ***kritiskos sektoros, piemēram, publiskajā infrastruktūrā, vēlēšanu infrastruktūrā, transportā, veselības aprūpē, finansēs, telekomunikācijā, pārtikas piegādē un nodrošinājumā***, un tūlītēju atkopšanos no tiem.

Grozījums Nr. 52

Regulas priekšlikums
12. pants – 5. punkts

Komisijas ierosinātais teksts	*Grozījums*
5. Komisijai ir vispārēja atbildība par ES kiberdrošības rezerves īstenošanu. Komisija nosaka ES kiberdrošības rezervju prioritātes un attīstību saskaņā ar 3. punktā minēto lietotāju prasībām un uzrauga to īstenošanu, kā arī nodrošina savstarpēju papildināmību, konsekvenci, sinerģiju un sakaru ar citām atbalsta darbībām saskaņā ar šo regulu, kā arī citām Savienības darbībām un programmām.	5. Komisijai ir vispārēja atbildība par ES kiberdrošības rezerves īstenošanu. Komisija nosaka ES kiberdrošības rezervju prioritātes un attīstību saskaņā ar 3. punktā minēto lietotāju prasībām un uzrauga to īstenošanu, kā arī nodrošina savstarpēju papildināmību, konsekvenci, sinerģiju un sakaru ar citām atbalsta darbībām saskaņā ar šo regulu, kā arī citām Savienības darbībām un programmām***, un mērķiem, jo īpaši stratēģisko mērķi, kas paredz samazināt atkarību no augsta riska piegādātājiem, kas būtu pretrunā Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu***.

Grozījums Nr. 53

Regulas priekšlikums
12. pants – 7. punkts

Komisijas ierosinātais teksts	*Grozījums*
7. Lai atbalstītu Komisiju ES kiberdrošības rezervju izveidē, ENISA pēc apspriešanās ar dalībvalstīm un Komisiju sagatavo vajadzīgo pakalpojumu kartējumu. Pēc apspriešanās ar Komisiju ENISA sagatavo līdzīgu kartējumu, lai	7. Lai atbalstītu Komisiju ES kiberdrošības rezervju izveidē, ENISA pēc apspriešanās ar dalībvalstīm un Komisiju sagatavo vajadzīgo pakalpojumu kartējumu. Pēc apspriešanās ar Komisiju ENISA ***ar EĀDD atbalstu*** sagatavo līdzīgu

apzinātu to trešo valstu vajadzības, kuras ir tiesīgas uz atbalstu no ES kiberdrošības rezervēm saskaņā ar 17. pantu. Attiecīgā gadījumā Komisija apspriežas ar Augsto pārstāvi.	kartējumu, lai apzinātu to trešo valstu vajadzības, kuras ir tiesīgas uz atbalstu no ES kiberdrošības rezervēm saskaņā ar 17. pantu. Attiecīgā gadījumā Komisija apspriežas ar Augsto pārstāvi.

Grozījums Nr. 54

Regulas priekšlikums
14. pants – 2. punkts – aa apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	aa) incidenta ietekmi uz Savienības drošību un aizsardzību;

Grozījums Nr. 55

Regulas priekšlikums
15. pants – 3. punkts

Komisijas ierosinātais teksts	*Grozījums*
3. Apspriežoties ar Augsto pārstāvi, kiberavārijas mehānisma atbalsts var papildināt palīdzību, ko sniedz kopīgajā ārpolitikā un drošības politikā un kopīgajā drošības un aizsardzības politikā, arī ***caur*** kiberdrošības ātrās reaģēšanas ***vienībām***. Tas var arī papildināt vai veicināt palīdzību, ko dalībvalsts sniedz citai dalībvalstij uz Līguma par Eiropas Savienību 42. panta 7. punkta pamata.	3. Apspriežoties ar Augsto pārstāvi, kiberavārijas mehānisma atbalsts var papildināt palīdzību, ko sniedz kopīgajā ārpolitikā un drošības politikā un kopīgajā drošības un aizsardzības politikā, arī ***ar*** kiberdrošības ātrās reaģēšanas ***vienību (CRRT) starpniecību, lai uzlabotu atbalsta sniegšanu ES dalībvalstīm, KDAP misijām un operācijām, kā arī trešām valstīm, kas kiberaizsardzības spēju veidošanas centienos rīkojas saskaņoti ar ES kopējo ārpolitiku un drošības politiku un kopējo drošības un aizsardzības politiku, jo īpaši Ukrainai un Moldovai***. Tas var arī papildināt vai veicināt palīdzību, ko dalībvalsts sniedz citai dalībvalstij uz Līguma par Eiropas Savienību 42. panta 7. punkta pamata.

Grozījums Nr. 56

Regulas priekšlikums

16. pants – 2. punkts – ba apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	aa) pakalpojumu sniedzējs pierāda, ka tā lēmumi un pārvaldības struktūras ir brīvas no valstu valdību nepamatotas ietekmes, kas būtu pretrunā Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu;

Grozījums Nr. 57

Regulas priekšlikums
16. pants – 2. punkts – f apakšpunkts

Komisijas ierosinātais teksts	*Grozījums*
f) pakalpojumu sniedzējs ir aprīkots ar pieprasītajam pakalpojumam nepieciešamo aparatūru un programmatūras tehnisko aprīkojumu;	f) pakalpojumu sniedzējs ir aprīkots ar pieprasītajam pakalpojumam nepieciešamo aparatūru un programmatūras tehnisko aprīkojumu ***un atbilst Regulas XX/XXXX (Kibernoturības akts) X pantā noteiktajām prasībām***;

Grozījums Nr. 58

Regulas priekšlikums
16. pants – 2. punkts – ja (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	ja) neviens pakalpojumu sniedzējs no augsta riska trešās valsts nav pieņemams.

Grozījums Nr. 59

Regulas priekšlikums
16. pants – 2. punkts – jb apakšpunkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	jb) pakalpojumu sniedzējs, ja iespējams, cieši sadarbojas ar

attiecīgajiem MVU;

Grozījums Nr. 60

Regulas priekšlikums
17. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. ***Trešas*** valstis var pieprasīt ES kiberdrošības rezervju atbalstu, ja to paredz asociācijas nolīgumi, kas noslēgti par to dalību programmā "Digitālā Eiropa".	1. ***Trešās*** valstis var pieprasīt ES kiberdrošības rezervju atbalstu, ja***:***
	a) to paredz asociācijas nolīgumi, kas noslēgti par to dalību programmā "Digitālā Eiropa";
	b) trešās valstis, kurās ir izvietota KDAP misija ar īpašām pilnvarām stiprināt noturību pret hibrīddraudiem, tostarp kiberdraudiem, vai kurās ir pieņemts EMM palīdzības pasākums, lai stiprinātu valsts kibernoturību.

Grozījums Nr. 61

Regulas priekšlikums
17. pants – 2. punkts

Komisijas ierosinātais teksts	*Grozījums*
2. Atbalsts no ES kiberdrošības rezervēm ir saskaņā ar šo regulu un atbilst 1. punktā minēto asociācijas nolīgumu īpašajiem nosacījumiem.	2. Atbalsts no ES kiberdrošības rezervēm ir saskaņā ar šo regulu un atbilst 1. punktā minēto asociācijas nolīgumu īpašajiem nosacījumiem***, izņemot attiecībā uz trešām valstīm, uz kurām attiecas 1. punkta b) apakšpunktā paredzētie noteikumi***.

Grozījums Nr. 62

Regulas priekšlikums
18. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
1. Pēc Komisijas, EU-CyCLONe vai CSIRT tīkla pieprasījuma ENISA izskata un novērtē apdraudējumu, vājās vietas un apdraudējuma mazināšanas darbības, kas attiecas uz konkrētu ievērojamu vai plašu kiberincidentu. Pēc incidenta izskatīšanas un novērtēšanas ENISA iesniedz incidenta pārskata ziņojumu CSIRT tīklam, EU-CyCLONe un Komisijai, lai palīdzētu tiem veikt to uzdevumus, sevišķi Direktīvas (ES) 2022/2555 15. un 16. pantā noteiktos uzdevumus. Attiecīgā gadījumā Komisija ziņojumu iesniedz Augstajam pārstāvim.	1. Pēc Komisijas, EU-CyCLONe vai CSIRT tīkla pieprasījuma ENISA izskata un novērtē apdraudējumu, vājās vietas un apdraudējuma mazināšanas darbības, kas attiecas uz konkrētu ievērojamu vai plašu kiberincidentu. Pēc incidenta izskatīšanas un novērtēšanas ENISA iesniedz incidenta pārskata ziņojumu CSIRT tīklam, EU-CyCLONe un Komisijai, lai palīdzētu tiem veikt to uzdevumus, sevišķi Direktīvas (ES) 2022/2555 15. un 16. pantā noteiktos uzdevumus. Attiecīgā gadījumā***, jo īpaši, ja incidents ir saistīts ar kādu trešo valsti,*** Komisija ziņojumu iesniedz Augstajam pārstāvim ***un EĀDD***.

Grozījums Nr. 63

Regulas priekšlikums
18. pants – 3.a punkts (jauns)

Komisijas ierosinātais teksts	*Grozījums*
	3.a Ziņojumu dara zināmu Eiropas Parlamentam saskaņā ar Savienības vai valsts tiesību aktiem par sensitīvas klasificētas informācijas aizsardzību.

Grozījums Nr. 64

Regulas priekšlikums
19. pants – 1. daļa – 1. punkts – a apakšpunkts – 1. punkts
Regula (ES) 2021/694
6. pants – 1. punkts

Komisijas ierosinātais teksts	*Grozījums*
aa) atbalstīt ES kibervairoga izstrādi, ieskaitot tādu valsts un pārrobežu DOC platformu izstrādi, ierīkošanu un darbību, kuras veicina stāvokļa apzināšanos Savienībā ***un uzlabo*** Savienības kiberapdraudējuma izlūkošanas ***spējas***;	aa) atbalstīt ES kibervairoga izstrādi, ieskaitot tādu valsts un pārrobežu DOC platformu izstrādi, ierīkošanu un darbību, kuras veicina stāvokļa apzināšanos Savienībā***,*** Savienības kiberapdraudējuma izlūkošanas ***spēju palielināšanu un to, lai mazinātu Savienības atkarību no augsta***

	riska kritiskās kiberdrošības aprīkojuma vai komponentu piegādātājiem, kas būtu pretrunā Savienības un tās dalībvalstu drošības un aizsardzības interesēm, kā noteikts KĀDP satvarā saskaņā ar LES V sadaļu;

Grozījums Nr. 65

Regulas priekšlikums
20. pants – 1. daļa

Komisijas ierosinātais teksts	*Grozījums*
[Četrus gadus pēc šīs regulas piemērošanas ***sākuma]Komisija*** iesniedz Eiropas Parlamentam un Padomei šīs regulas ***izvērtējumu*** un ***pārskatu***.	***[Trīs*** gadus pēc šīs regulas piemērošanas ***dienas un pēc tam reizi divos gados] Komisija*** iesniedz Eiropas Parlamentam un Padomei ***ziņojumu par*** šīs regulas ***izvērtēšanu*** un ***pārskatīšanu***.

ATZINUMU SNIEDZOŠĀS KOMITEJAS PROCEDŪRA

Virsraksts	Pasākumu noteikšana solidaritātes un spēju stiprināšanai Savienībā nolūkā atklāt kiberapdraudējumu un kiberdrošības incidentus, tiem sagatavoties un uz tiem reaģēt
Atsauces	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Atbildīgā komiteja Datums, kad paziņoja plenārsēdē	ITRE 1.6.2023
Atzinumu sniedza Datums, kad paziņoja plenārsēdē	AFET 1.6.2023
Atzinuma sagatavotājs(-a) Iecelšanas datums	Dragoş Tudorache 16.6.2023
Izskatīšana komitejā	18.9.2023
Pieņemšanas datums	24.10.2023
Galīgais balsojums	+: 39 –: 4 0: 0
Komitejas locekļi, kas bija klāt galīgajā balsošanā	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Aizstājēji, kas bija klāt galīgajā balsošanā	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

ATZINUMU SNIEDZOŠĀS KOMITEJAS
GALĪGAIS BALSOJUMS PĒC SARAKSTA

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Izmantoto apzīmējumu skaidrojums:
+ : par
- : pret
0 : atturas