EIROPAS SAVIENĪBA

EIROPAS PARLAMENTS **PADOME**

Briselē, 2024. gada 19. decembrī
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

EIROPAS PARLAMENTA UN PADOMES REGULA, KAS NOSAKA PASĀKUMUS, KURI STIPRINA SOLIDARITĀTI UN SPĒJAS SAVIENĪBĀ ATKLĀT KIBERDRAUDUS UN INCIDENTUS, TIEM SAGATAVOTIES UN UZ TIEM REAĢĒT UN AR KO GROZA REGULU (ES) 2021/694 (KIBERSOLIDARITĀTES AKTS)

EIROPAS PARLAMENTA UN PADOMES
REGULA (ES) 2024/...

(2024. gada 19. decembris),

kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberdraudus un incidentus, tiem sagatavoties un uz tiem reaģēt un ar ko groza Regulu (ES) 2021/694
(Kibersolidaritātes akts)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 173. panta 3. punktu un 322. panta 1. punkta a) apakšpunktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Revīzijas palātas atzinumu[1],

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[2],

ņemot vērā Reģionu komitejas atzinumu[3],

saskaņā ar parasto likumdošanas procedūru[4],

---

1 2023. gada 18. aprīļa atzinums (*Oficiālajā Vēstnesī* vēl nav publicēts).
2 OV C 349, 29.9.2023., 167. lpp.
3 OV C, C/2024/1049, 9.2.2024., ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Eiropas Parlamenta 2024. gada 24. aprīļa nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2024. gada 2. decembra lēmums.

tā kā:

(1) Informācijas un komunikācijas tehnoloģiju lietošana un atkarība no tām ir kļuvušas par fundamentāliem aspektiem visās saimnieciskās darbības nozarēs un sabiedrībā, ņemot vērā dalībvalstu publiskās pārvaldes iestāžu, uzņēmumu un iedzīvotāju arvien pieaugušo savstarpējo saistību un atkarību, vienlaikus radot iespējamu ievainojamību.

(2) Savienībā un pasaulē pieaug kiberdrošības incidentu apjoms, biežums un ietekme, tostarp uzbrukumi piegādes ķēdēm nolūkā veikt kiberspiegošanu, izspiedējprogrammu izmantošanu vai darbības traucēšanu. Tie ievērojami apdraud tīklu un informācijas sistēmu darbību. Ņemot vērā strauji mainīgo apdraudējuma ainu, draudoši liela mēroga kiberdrošības incidenti, kas izraisa būtisku pārrāvumu vai kaitējumu kritiskajai infrastruktūrai, prasa labāku Savienības kiberdrošības satvara gatavību. Minētais apdraudējums ir plašāks par Krievijas agresijas karu pret Ukrainu, un tas visdrīzāk saglabāsies, jo pašreizējā ģeopolitiskajā saspīlējumā ir iesaistījušies daudzi aktori. Šādi incidenti var kavēt sabiedrisko pakalpojumu sniegšanu, jo kiberuzbrukumi bieži tiek vērsti pret vietējiem, reģionāliem vai valsts mēroga sabiedriskajiem pakalpojumiem un infrastruktūru, un vietējās iestādes ir īpaši neaizsargātas, tostarp to ierobežoto resursu dēļ. Tie var arī kavēt saimniecisku darbību, tostarp sevišķi kritiskajās nozarēs vai citās kritiskajās nozarēs, radīt būtiskus finansiālus zaudējumus, mazināt lietotāju uzticēšanos, radīt būtisku kaitējumu Savienības ekonomikai un demokrātiskajām sistēmām, kā arī varētu pat radīt veselībai vai dzīvībai bīstamas sekas. Bez tam kiberdrošības incidenti ir neprognozējami, jo tie mēdz rasties un izplatīties strauji, tos neierobežo nekāda ģeogrāfiska platība un tie notiek vienlaicīgi vai vienā mirklī izplatās daudzās valstīs. Tāpēc ir vajadzīga publiskā sektora, privātā sektora, akadēmisko aprindu, pilsoniskās sabiedrības un mediju cieša sadarbība.

(3) Ir nepieciešams stiprināt rūpniecības un pakalpojumu nozaru konkurētspēju Savienībā visā digitālajā ekonomikā un ir jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā tirgus kiberdrošību, kā ieteikts trijos dažādos konferences par Eiropas nākotni priekšlikumos. Ir jāpalielina iedzīvotāju, uzņēmumu, tostarp mikrouzņēmumu, mazo un vidējo uzņēmumu un jaunuzņēmumu, un vienību, kuras darbina kritisko infrastruktūru, noturība pret pieaugošajiem kiberdraudiem, kam var būt postoša ietekme uz sabiedrību un tautsaimniecību. Tāpēc ir vajadzīgas investīcijas infrastruktūrā un pakalpojumos un spēju veidošanā, lai attīstītu kiberdrošības prasmes, kas palīdzēs ātrāk atklāt kiberdraudus un incidentus un ātrāk uz tiem reaģēt. Turklāt dalībvalstīm ir vajadzīga palīdzība, lai labāk sagatavotos būtiskiem un liela mēroga kiberdrošības incidentiem un reaģētu uz tiem, un palīdzība, lai uzsāktu atkopšanos no tiem. Ņemot vērā pašreizējās struktūras un cieši sadarbojoties ar tām, Savienībai būtu arī jāpalielina savas spējas minētajās jomās, jo īpaši attiecībā uz datu par kiberdraudiem un incidentiem vākšanu un analīzi.

(4) Savienība jau ir noteikusi vairākus pasākumus, lai samazinātu kritisko infrastruktūru un vienību ievainojamību un uzlabotu to noturība pret riskiem, jo īpaši Eiropas Parlamenta un Padomes Regulu (ES) 2019/881[5], Eiropas Parlamenta un Padomes Direktīvas 2013/40/ES[6] un (ES) 2022/2555[7] un Komisijas Ieteikumu (ES) 2017/1584[8]. Bez tam Padomes 2022. gada 8. decembra ieteikumā par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai dalībvalstis tiek aicinātas veikt steidzamus un efektīvus pasākumus un 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.

---

5 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.).

6 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.).

7 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.).

8 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.).

(5) Augošie kiberdrošības riski un vispārējā sarežģītā apdraudējuma vide, kurā nepārprotami draud strauja incidentu pāriešana no vienas dalībvalsts uz citām un no trešās valsts uz Savienību, prasa solidaritātes pastiprināšanu Savienības līmenī, lai labāk atklātu kiberdraudus un incidentus, tiem sagatavotos, uz tiem reaģētu un atkoptos pēc tiem, jo īpaši stiprinot pašreizējo struktūru spējas. Turklāt Padomes 2022. gada 23. maija secinājumos par Eiropas Savienības pozīcijas izstrādi kiberjautājumos dalībvalstis aicināja Komisiju iesniegt priekšlikumu par jaunu Ārkārtēja stāvokļa reaģēšanas fondu kiberdrošībai.

(6) Komisijas un Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos 2022. gada 10. novembrī pieņemtajā Kopīgajā paziņojumā Eiropas Parlamentam un Padomei par ES kiberaizsardzības politiku tika izziņota ES kiberdrošības solidaritātes iniciatīva, kuras mērķi ir stiprināt kopīgas ES kiberapdraudējumu atklāšanas, situāciju apzināšanās un reaģēšanas spējas, veicinot ES drošības operāciju centru (DOC) infrastruktūras izvēršanu, atbalstot ES līmeņa kiberrezervju pakāpenisku izveidi ar pakalpojumiem no uzticamiem privātiem pakalpojumu sniedzējiem un kritisko vienību testēšanu iespējamu ievainojamību atklāšanai, pamatojoties uz ES riska novērtējumiem.

(7) Ir jāstiprina kiberdraudu un incidentu atklāšana un situācijas apzināšanās visā Savienībā un solidaritāte, uzlabojot dalībvalstu un Savienības gatavību un spējas novērst būtiskus kiberdrošības incidentus un liela mēroga kiberdrošības incidentus un reaģēt uz tiem. Tādēļ Eiropas mērogā būtu jāizveido kibercentru tīkls (“Eiropas kiberdrošības trauksmes sistēma”), lai veidotu koordinētas spējas atklāt apdraudējumu un apzināties situāciju, tādējādi pastiprinot Savienības apdraudējumu atklāšanas un dalīšanās ar informāciju spējas; būtu jāizveido kiberdrošības ārkārtas mehānisms, lai pēc dalībvalstu pieprasījuma palīdzētu tām sagatavoties būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem, reaģēt uz tiem, mazināt to ietekmi un uzsākt atkopšanos no tiem, un lai palīdzētu citiem lietotājiem reaģēt uz būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem; un būtu jāizveido Eiropas kiberdrošības incidentu izskatīšanas mehānisms konkrētu būtisku kiberdrošības incidentu vai liela mēroga kiberdrošības incidentu izskatīšanai un novērtēšanai. Darbības, ko veic ievērojot šo regulu, būtu jāveic, pienācīgi ievērojot dalībvalstu kompetences, un tām būtu jāpapildina, nevis jādublē darbības, ko veic *CSIRT* tīkls, Eiropas Kiberkrīžu sadarbības organizāciju tīkls (*EU-CyCLONe*) vai Sadarbības grupa (TID sadarbības grupa), kas izveidoti, ievērojot Direktīvu (ES) 2022/2555. Minētās darbības neskar Līguma par Eiropas Savienības darbību (LESD) 107. un 108. pantu.

(8) Lai šos mērķus sasniegtu, dažās jomās ir jāgroza Eiropas Parlamenta un Padomes Regula (ES) 2021/694[9]. Jo īpaši ar šo regulu būtu jāgroza Regula (ES) 2021/694, lai pievienotu jaunus darbības mērķus, kas saistīti ar Eiropas kiberdrošības trauksmes sistēmu un kiberdrošības ārkārtas mehānismu saskaņā ar programmas "Digitālā Eiropa" ("*PDE*") konkrēto mērķi Nr. 3, kura mērķis ir garantēt digitālā vienotā tirgus noturību, veselumu un uzticamību, stiprinātu spējas uzraudzīt kiberuzbrukumus un kiberdraudus un reaģēt uz tiem, kā arī pastiprinātu pārrobežu sadarbību un koordināciju kiberdrošības jomā. Eiropas kiberdrošības trauksmes sistēmai varētu būt svarīga loma, atbalstot dalībvalstis kiberdraudu prognozēšanā un aizsardzībā pret tiem, un ES kiberdrošības rezervēm varētu būt svarīga loma, atbalstot dalībvalstis, Savienības iestādes, struktūras, birojus un aģentūras, kā arī *PDE* asociētās trešās valstis reaģēšanā uz būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem un lielam mērogam līdzvērtīgiem kiberdrošības incidentiem un to ietekmes mazināšanā. Minētā ietekme varētu ietvert ievērojamus materiālus vai nemateriālus zaudējumus un nopietnus sabiedriskās drošības un drošuma riskus. Ņemot vērā īpašās funkcijas, kādas varētu būt Eiropas kiberdrošības trauksmes sistēmai un ES kiberdrošības rezervēm, šai regulai būtu jāgroza Regula (ES) 2021/694 attiecībā uz tādu tiesību subjektu dalību, kuri ir iedibināti Savienībā, bet kurus kontrolē no trešām valstīm, gadījumos, ja pastāv reāls risks, ka Savienībā nav pieejami nepieciešamie un pietiekamie rīki, infrastruktūra un pakalpojumi vai tehnoloģijas, lietpratība un spējas, un ieguvumi no šādu subjektu iekļaušanas atsver drošības risku. Būtu jānosaka īpaši nosacījumi, ar kuriem var piešķirt finansiālu atbalstu darbībām, ar ko īsteno ES kiberdrošības trauksmes sistēmu un ES kiberdrošības rezerves, un būtu jānosaka paredzēto mērķu sasniegšanai nepieciešami pārvaldības un koordinācijas mehānismi. Citos Regulas (ES) 2021/694 grozījumos būtu jāiekļauj saskaņā ar jaunajiem darbības mērķiem ierosināto darbību apraksti, kā arī izmērāmi rādītāji minēto darbības mērķu īstenošanas uzraudzībai.

---

[9] Eiropas Parlamenta un Padomes Regula (ES) 2021/694 (2021. gada 29. aprīlis), ar ko izveido programmu "Digitālā Eiropa" un atceļ Lēmumu (ES) 2015/2240 (OV L 166, 11.5.2021., 1. lpp.).

(9) Lai stiprinātu Savienības spējas reaģēt uz kiberdraudiem un incidentiem, svarīgi ir īstenot sadarbību ar starptautiskām organizācijām, kā arī ar uzticamiem un līdzīgi domājošiem starptautiskajiem partneriem. Minētajā kontekstā ar uzticamiem un līdzīgi domājošiem starptautiskajiem partneriem būtu jāsaprot valstis, kurām ir kopīgi principi, kas ir iedvesmojuši Savienības izveidi, proti, demokrātija, tiesiskums, cilvēktiesību un pamatbrīvību universālums un nedalāmība, cilvēka cieņas neaizskaramība, vienlīdzība un solidaritāte, kā arī Apvienoto Nāciju Organizācijas Statūtu un starptautisko tiesību principu ievērošana un kuras neapdraud Savienības vai tās dalībvalstu būtiskās drošības intereses. Šāda sadarbība varētu būt noderīga arī attiecībā uz darbībām, kas veiktas ievērojot šo regulu, jo īpaši attiecībā uz Eiropas kiberdrošības trauksmes sistēmu un ES kiberdrošības rezervēm. Regulā (ES) 2021/694, ievērojot konkrētus pieejamības un drošības nosacījumus, būtu jāparedz, ka Eiropas kiberdrošības trauksmes sistēmas un ES kiberdrošības rezervju iepirkumu konkursos var piedalīties tiesību subjekti, kurus kontrolē no trešām valstīm, ja ir izpildīti drošības nosacījumi. Novērtējot drošības risku, ko rada iepirkuma procedūras paplašināšana šādā veidā, ir svarīgi ņemt vērā principus un vērtības, kas Savienībai ir kopīgas ar līdzīgi domājošiem starptautiskajiem partneriem, ja minētie principi un vērtības ir saistītas ar būtiskām Savienības drošības interesēm. Turklāt, ja šādas drošības prasības tiek apsvērtas saskaņā ar Regulu (ES) 2021/694, varētu ņemt vērā vairākus elementus, piemēram, subjekta korporatīvo struktūru un lēmumu pieņemšanas procesu, datu un klasificētas vai sensitīvas informācijas drošību un to, ka ir jānodrošina, ka darbības rezultātus nekontrolē vai neierobežo neatbilstīgas trešās valstis.

(10) Darbību finansēšana atbilstoši šai regulai būtu jānosaka Regulā (ES) 2021/694, kurai arī turpmāk būtu jābūt attiecīgajam pamataktam attiecībā uz darbībām, kuras ietvertas programmas *PDE* konkrētajā mērķī Nr. 3. Saskaņā ar Regulu (ES) 2021/694 attiecīgajās darba programmās katrai darbībai ir jāparedz īpaši dalības nosacījumi.

(11) Šai regulai piemēro horizontālos finanšu noteikumus, ko Eiropas Parlaments un Padome pieņēmuši, pamatojoties uz LESD 322. pantu. Minētie noteikumi ir izklāstīti Eiropas Parlamenta un Padomes Regulā (ES, *Euratom*) 2024/2509[10] un nosaka jo īpaši Savienības budžeta izveides un izpildes procedūru, kā arī paredz finanšu subjektu atbildības pārbaudes. Noteikumos, kas pieņemti, pamatojoties uz LESD 322. pantu, iekļauts arī vispārējs nosacītības režīms Savienības budžeta aizsardzībai, kā noteikts Eiropas Parlamenta un Padomes Regulā (ES, *Euratom*) 2020/2092[11].

---

[10] Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2024/2509 (2024. gada 23. septembris) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam (OV L 2024/2509, 26.9.2024, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2020/2092 (2020. gada 16. decembris) par vispārēju nosacītības režīmu Savienības budžeta aizsardzībai (OV L 433 I, 22.12.2020., 1. lpp., ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Lai gan novēršanas un gatavības pasākumi ir būtiski, lai uzlabotu Savienības noturību, risinot būtiskus kiberdrošības incidentus, liela mēroga kiberdrošības incidentus un lielam mērogam līdzvērtīgus kiberdrošības incidentus, šādu incidentu rašanās, laiks un apmērs pēc būtības nav prognozējami. Finanšu resursi, kas vajadzīgi, lai nodrošinātu pienācīgu reaģēšanu, katru gadu var ievērojami atšķirties, un tiem vajadzētu būt pieejamiem nekavējoties. Tāpēc budžeta paredzamības principa saskaņošana ar nepieciešamību ātri reaģēt uz jaunām vajadzībām nozīmē, ka jāpielāgo darba programmu finansiālā īstenošana. Līdz ar to ir lietderīgi atļaut pārnest neizlietotās apropriācijas, bet tikai uz nākamo gadu un tikai uz ES kiberdrošības rezervēm un darbībām, kuras atbalsta savstarpējo sadarbību, papildus apropriāciju pārnešanai, kas atļauta, ievērojot Regulas (ES, *Euratom*) 2024/2509 12. panta 4. punktu.

(13) Lai efektīvāk novērstu un novērtētu kiberdraudus un incidentus, uz tiem reaģētu un atkoptos pēc tiem, ir nepieciešams attīstīt plašākas zināšanas par kritiskiem aktīviem un infrastruktūru Savienības teritorijā draudošām briesmām, tostarp par to ģeogrāfisko izplatību, savstarpējo saistību un iespējamām sekām kiberuzbrukumu gadījumā, kas skartu minēto infrastruktūru. Proaktīva pieeja kiberdraudu apzināšanai, mazināšanai un novēršanai ietver modernu atklāšanas spēju uzlabošanu. Eiropas kiberdrošības trauksmes sistēmai būtu jāsastāv no vairākiem sadarbīgiem pārrobežu kibercentriem, no kuriem katrs apvieno trīs vai vairākus valstu kibercentrus. Minētajai infrastruktūrai būtu jākalpo valstu un Savienības kiberdrošības interesēm un vajadzībām, izmantojot jaunākās tehnoloģijas nozīmīgu, attiecīgā gadījumā anonimizētu datu un informācijas progresīvai vākšanai, un analīzes rīkus, uzlabojot kiberapdraudējuma koordinētas atklāšanas un pārvaldības spējas un nodrošinot stāvokļa apzināšanos reāllaikā. Minētajai infrastruktūrai būtu jāpalīdz uzlabot pozīcija kiberjautājumos, palielinot datu un informācijas atklāšanu, apkopošanu un analīzi, nolūkā novērst kiberdraudus un incidentus un tādējādi papildināt un atbalstīt Savienības vienības un tīklus, kas ir atbildīgi par kiberkrīžu pārvarēšanu Savienībā, jo īpaši *EU-CyCLONe*.

(14) Dalība Eiropas kiberdrošības trauksmes sistēmā dalībvalstīm ir brīvprātīga. Katrai dalībvalstij valsts līmenī jānorīko viena vienība, kuras uzdevums ir attiecīgajā dalībvalstī koordinēt kiberdraudu atklāšanas darbības. Minētajiem valstu kibercentriem vajadzētu darboties kā uzziņas avotam un valsts līmeņa vārtejai dalībai Eiropas kiberdrošības trauksmes sistēmā un vajadzētu nodrošināt, ka informācija par kiberapdraudējumu no publiskām un privātām vienībām tiek efektīvi un racionalizēti nodota un vākta valsts līmenī. Valstu kibercentri varētu stiprināt publisko un privāto vienību sadarbību un dalīšanos ar informāciju un varētu arī atbalstīt nozīmīgo datu un informācijas apmaiņu ar attiecīgajām nozaru un starpnozaru kopienām, tostarp attiecīgajiem nozares informācijas apmaiņas un analīzes centriem (*ISAC*). Publisko un privāto vienību ciešai un koordinētai sadarbībai ir vissvarīgākā nozīme Savienības kibernoturības stiprināšanā. Šāda sadarbība ir īpaši vērtīga saistībā ar dalīšanos ar kiberdraudu izlūkdatiem, lai uzlabotu aktīvu kiberaizsardzību. Šādas sadarbības un dalīšanās ar informāciju ietvaros valstu kibercentri varētu pieprasīt un saņemt konkrētu informāciju. Šī regula neparedz minētajiem valstu kibercentriem ne pienākumu, ne pilnvaras prasīt šādu informācijas pieprasījumu izpildi. Attiecīgā gadījumā un saskaņā ar Savienības un valstu tiesību aktiem pieprasītā vai saņemtā informācija varētu ietvert telemetrijas, sensoru un reģistrēšanas datus no vienībām, piemēram, pārvaldītiem drošības pakalpojumu sniedzējiem, kas darbojas sevišķi kritiskajās nozarēs vai citās kritiskajās nozarēs minētajā dalībvalstī, lai veicinātu iespējamu kiberdraudu un incidentu ātru atklāšanu agrīnā posmā, tādējādi uzlabojot situācijas apzināšanos. Ja valsts kibercentrs nav kompetentā iestāde, ko attiecīgā dalībvalsts izraudzījusies vai izveidojusi, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu, ir būtiski, lai tas koordinētu savu darbību ar minēto kompetento iestādi attiecībā uz šādu datu pieprasījumiem un saņemšanu.

(15) Eiropas kiberdrošības trauksmes sistēmā būtu jāizveido vairāki pārrobežu kibercentri. Minētajos pārrobežu kibercentros būtu jāapvieno valstu kibercentri no vismaz trim dalībvalstīm, lai nodrošinātu, ka no pārrobežu apdraudējuma atklāšanas un dalīšanās ar informāciju un pārvaldības būtu pilnīgs ieguvums. Pārrobežu kibercentru vispārīgajam mērķim vajadzētu būt stiprināt spējas analizēt, novērst un atklāt kiberdraudus un atbalstīt kvalitatīvu izlūkdatu par kiberdraudiem sagatavošanu, jo īpaši uzticamā un drošā vidē daloties ar nozīmīgu un attiecīgā gadījumā anonimizētu informāciju, no dažādiem publiskiem vai privātiem avotiem, kā arī uzticamā un drošā vidē daloties ar modernākiem rīkiem un koplietojot tos un kopīgi attīstot atklāšanas, analīzes un novēršanas spējas. Pārrobežu kibercentriem būtu jānodrošina jaunas papildu spējas, izmantojot un savstarpēji papildinot esošos DOC un *CSIRT*, kā arī citus attiecīgus dalībniekus, tostarp *CSIRT* tīklu.

(16) Dalībvalstij, kuru pēc uzaicinājuma izteikt ieinteresētību izraudzījies Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centrs (*ECCC*), kas izveidots ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/887[12], lai tā izveidotu valsts kibercentru vai uzlabotu tā spējas, kopā ar *ECCC* būtu jāiegādājas attiecīgie rīki, infrastruktūra vai pakalpojumi. Šādai dalībvalstij vajadzētu būt tiesīgai saņemt dotāciju rīku vai infrastruktūras ekspluatācijai. Mitināšanas konsorcijam, kuru veido vismaz trīs dalībvalstis un kuru ir izraudzījies *ECCC* pēc uzaicinājuma izteikt ieinteresētību, lai izveidotu vai uzlabotu pārrobežu kibercentra spējas, kopā ar *ECCC* būtu jāiegādājas attiecīgie rīki, infrastruktūra vai pakalpojumi. Mitināšanas konsorcijam vajadzētu būt tiesīgam saņemt dotāciju rīku un infrastruktūras ekspluatācijai vai pakalpojumu sniegšanai. Iepirkuma procedūra attiecīgo rīku, infrastruktūras vai pakalpojumu iegādei būtu kopīgi jāveic *ECCC* un attiecīgajām dalībvalstu līgumslēdzējām iestādēm, kas atlasītas pēc šādiem uzaicinājumiem izteikt ieinteresētību. Šādam iepirkumam būtu jāatbilst Regulas (ES, *Euratom*) 2024/2509 168. panta 2. punktam un *ECCC* finanšu noteikumiem. Tāpēc privātām struktūrām nevajadzētu būt tiesīgām piedalīties uzaicinājumos izteikt ieinteresētību par rīku, infrastruktūras vai pakalpojumu kopīgu iegādi ar *ECCC* vai saņemt dotācijas šo rīku un infrastruktūru ekspluatācijai vai pakalpojumu sniegšanai. Tomēr dalībvalstīm vajadzētu būt iespējai iesaistīt privātas vienības savu valstu kibercentru un pārrobežu kibercentru izveidē, uzlabošanā un darbībā citos veidos, ko tās uzskata par piemērotiem, saskaņā ar Savienības un valstu tiesību aktiem. Privātas vienības arī varētu būt tiesīgas saņemt Savienības finansējumu, ievērojot Regulu (ES) 2021/887, lai sniegtu atbalstu valstu kibercentriem.

---

[12] Eiropas Parlamenta un Padomes Regula (ES) 2021/887 (2021. gada 20. maijs), ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu (OV L 202, 8.6.2021., 1. lpp., ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) Lai uzlabotu kiberdraudu atklāšanu un situācijas apzināšanos Savienībā, dalībvalstij, kas pēc uzaicinājuma izteikt ieinteresētību ir izraudzīta izveidot valsts kibercentru vai uzlabot tā spējas, būtu jāapņemas pieteikties dalībai pārrobežu kibercentrā. Ja dalībvalsts nav pārrobežu kibercentra dalībniece divu gadu laikā no dienas, kad ir iegādāti rīki, infrastruktūra vai pakalpojumi vai dienas, kad tā saņem dotācijas finansējumu, atkarībā no tā, kas ir ātrāk, tai nevajadzētu būt tiesīgai piedalīties turpmākās Savienības atbalsta darbībās Eiropas kiberdrošības trauksmes sistēmas ietvaros, lai uzlabot savas valsts kibercentra spējas. Šādos gadījumos dalībvalstu vienības joprojām varētu piedalīties uzaicinājumos iesniegt priekšlikumus citās *PDE* jomās vai citās Savienības finansēšanas programmās, tostarp uzaicinājumos par kiberatklāšanas un dalīšanās ar informāciju spējām, ar noteikumu, ka minētās vienības atbilst minētajās programmās noteiktajiem atbilstības kritērijiem.

(18) Saskaņā ar Direktīvu (ES) 2022/2555 *CSIRT* apmainās ar informāciju *CSIRT* tīklā. Eiropas kiberdrošības trauksmes sistēmai būtu jāizveido jauna spēja, kas papildina *CSIRT* tīklu, palīdzot veidot Savienības situācijas apzināšanos un tādējādi ļaujot stiprināt *CSIRT* tīkla spējas. Pārrobežu kibercentriem būtu jākoordinē *CSIRT* tīkls un cieši jāsadarbojas ar to. Tiem būtu jārīkojas, apkopojot datus un daloties ar nozīmīgu un attiecīgā gadījumā anonimizētu informāciju par kiberdraudiem no publiskām un privātām vienībām, šādu datu un informācijas vērtību paaugstinot ar ekspertīzēm, kopīgi iegādātu infrastruktūru un modernākajiem rīkiem un veicinot Savienības tehnoloģisko suverenitāti, tās atvērto stratēģisko autonomiju, konkurētspēju un noturību, kā arī Savienības spēju attīstību.

(19) Pārrobežu kibercentriem būtu jādarbojas kā centrālajiem punktiem, kuros iespējams plaši apkopot attiecīgus datus un kiberdraudu izlūkdatus, un jānodrošina iespēja izplatīt informāciju par apdraudējumu lielā un daudzveidīgā dalībnieku kopā, piemēram, datorapdraudējuma reaģēšanas vienībām (*CERT*), *CSIRT*, *ISAC* un kritiskās infrastruktūras operatoriem. Mitināšanas konsorcija dalībniekiem konsorcija nolīgumā būtu jānorāda attiecīgā informācija, ar ko jādalās starp attiecīgā pārrobežu kibercentra dalībniekiem. Informācija, ar ko apmainās starp pārrobežu kibercentra dalībniekiem, varētu ietvert, piemēram, datus no tīkliem un sensoriem, apdraudējuma izlūkdatu plūsmas, aizskāruma rādītājus un kontekstualizētu informāciju par incidentiem, kiberdraudiem, gandrīz notikušiem incidentiem, ievainojamībām, paņēmieniem un procedūrām, apdraudētāju taktiku, apdraudējuma dalībniekiem specifisku informāciju, kiberdrošības brīdinājumus un ieteikumus par kiberdrošības rīku konfigurāciju kiberuzbrukumu atklāšanai. Turklāt pārrobežu kibercentriem būtu arī savstarpēji jānoslēdz sadarbības nolīgumi. Šādiem sadarbības nolīgumiem jo īpaši būtu jāprecizē dalīšanās ar informāciju principi un sadarbspēja. To klauzulās par sadarbspēju, jo īpaši dalīšanās ar informācijas formātos un protokolos, būtu jāvadās pēc sadarbspējas pamatnostādnēm, kuras izdevusi ar Regulu (ES) 2019/881 izveidotā Eiropas Savienības Kiberdrošības aģentūra (*ENISA*), un tāpēc tās būtu jāizmanto par sākumpunktu. Minētās pamatnostādnes būtu jāizdod ātri, lai nodrošinātu, ka pārrobežu kibercentri tās var ņemt vērā agrīnā posmā. Tajās būtu jāņem vērā starptautiskie standarti un paraugprakse, kā arī visu izveidoto pārrobežu kibercentru darbība.

(20) Pārrobežu kibercentriem un *CSIRT* tīklam būtu cieši jāsadarbojas, lai nodrošinātu darbību sinerģiju un papildināmību. Minētajā nolūkā tiem būtu jāvienojas par sadarbības un dalīšanās ar nozīmīgu informāciju procesuālo kārtību. Tas varētu ietvert dalīšanos ar nozīmīgu informāciju par kiberdraudiem un būtiskiem kiberdrošības incidentiem un to, ka ar *CSIRT* tīklu dalās ar pieredzi attiecībā uz modernākajiem rīkiem, jo īpaši mākslīgo intelektu un datu analīzes tehnoloģiju, ko izmanto pārrobežu kibercentros.

(21) Kopīga situācijas apzināšanās attiecīgo iestāžu vidū ir nepieciešams priekšnoteikums visas Savienības gatavībai un koordinācijai būtiskos kiberdrošības incidentos un liela mēroga kiberdrošības incidentos. Lai atbalstītu liela mēroga kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru nozīmīgas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām, Direktīva (ES) 2022/2555 izveidoja *EU-CyCLONe*. Direktīva (ES) 2022/2555 izveidoja arī *CSIRT* tīklu, lai veicinātu ātru un efektīvu operatīvo sadarbību starp visām dalībvalstīm. Lai nodrošinātu situācijas apzināšanos un stiprinātu solidaritāti, apstākļos, kad pārrobežu kibercentri iegūst informāciju, kas saistīta ar iespējamu vai notiekošu liela mēroga kiberdrošības incidentu, tiem būtu jāsniedz attiecīga informācija *CSIRT* tīklam un agrīns brīdinājums *EU-CyCLONe*. Atkarībā no situācijas informācija, kas jānodod jo īpaši varētu ietvert tehnisku informāciju, informāciju par uzbrucēja vai potenciālā uzbrucēja būtību un motīviem un augstāka līmeņa netehnisku informāciju par iespējamu vai notiekošu liela mēroga kiberdrošības incidentu. Minētajā sakarā būtu pienācīgi jāievēro princips "nepieciešamība zināt" un tas, ka nodotā informācija var būt sensitīva. Direktīvā (ES) 2022/2555 ir arī atkārti uzsvērti Komisijas pienākumi Savienības civilās aizsardzības mehānismā (UCPM), kas izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES[13], un tās pienākums sniegt analītiskus ziņojumus ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem (*IPCR* mehānismi), ievērojot Padomes īstenošanas lēmumu (ES) 2018/1993[14].

---

13 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., ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par ES integrētajiem krīzes situāciju politiskās reaģēšanas mehānismiem (OV L 320, 17.12.2018., 28. lpp., ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Ja pārrobežu kibercentri dalās ar *EU-CyCLONe* un *CSIRT* tīklu ar nozīmīgu informāciju un agrīniem brīdinājumiem, kas saistīti ar iespējamu vai notiekošu liela mēroga kiberdrošības incidentu, ir ļoti svarīgi, lai dalīšanās ar minēto informāciju notiktu minētajos tīklos ar dalībvalstu iestādēm, kā arī ar Komisiju. Minētajā sakarā Direktīva (ES) 2022/2555 paredz, ka *EU-CyCLONe* mērķis ir atbalstīt liela mēroga kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošināt regulāru dalīšanos ar nozīmīgu informāciju starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām. *EU-CyCLONe* uzdevumi ietver kopīgu situācijas apzināšanos attiecībā uz šādiem incidentiem un krīzēm. Ir ārkārtīgi svarīgi, lai *EU-CyCLONe* saskaņā ar minēto mērķi un tās uzdevumiem nodrošinātu, ka šāda informācija nekavējoties tiek sniegta attiecīgo dalībvalstu pārstāvjiem un Komisijai. Minētajā nolūkā ir ļoti svarīgi, lai *EU-CyCLONe* reglamentā tiktu iekļauti attiecīgi noteikumi.

(22) Vienībām, kuras piedalās Eiropas kiberdrošības trauksmes sistēmā, būtu jānodrošina augsta līmeņa spēja savā starpā sadarboties, tostarp attiecīgā gadījumā attiecībā uz datu formātu, taksonomiju, datu apstrādi un datu analīzes rīkiem. Tām būtu arī jānodrošina droši sakaru kanāli, lietojumprogrammu slāņa minimālais drošības līmenis, situācijas apzināšanās infopanelis un rādītāji. Pieņemot vienotu taksonomiju un izstrādājot stāvokļa ziņojuma veidni konstatēto kiberdraudu cēloņu un risku aprakstīšanai, būtu jāņem vērā paveiktais darbs saistībā ar Direktīvas (ES) 2022/2555 īstenošanu.

(23) Lai uzticamā un drošā vidē nodrošinātu plašu nozīmīgu datu un informācijas apmaiņu par kiberdraudiem no dažādiem avotiem, vienībām, kuras piedalās Eiropas kiberdrošības trauksmes sistēmā, vajadzētu būt apgādātām ar modernākajiem un ļoti drošiem rīkiem, iekārtām un infrastruktūru, un tām būtu jānodrošina augsti kvalificēts personāls. Tam būtu jāļauj uzlabot kolektīvās atklāšanas spējas un laikus brīdināt iestādes un attiecīgās vienības, it īpaši – izmantojot jaunākās mākslīgā intelekta un datu analīzes tehnoloģijas.

(24) Vācot, analizējot un daloties ar nozīmīgiem datiem un informāciju un ar to apmainoties, Eiropas kiberdrošības trauksmes sistēmai būtu jāstiprina Savienības tehnoloģiskā suverenitāte un atvērtā stratēģiskā autonomija kiberdrošības, konkurētspējas un noturības jomā. Kvalitatīvu kūrētu datu apkopošana varētu arī veicināt progresīvu mākslīgā intelekta un datu analīzes tehnoloģiju attīstību. Augstas kvalitātes datu efektīvā apkopošanā būtiska nozīme joprojām ir cilvēka veiktai pārraudzībai un, minētajā nolūkā, kvalificētam darbaspēkam.

(25) Lai gan Eiropas kiberdrošības trauksmes sistēma ir civils projekts, kiberaizsardzības kopienai varētu būt labums no spēcīgākām civilpersonu spējām atklāt apdraudējumu un apzināties situāciju, kuras izstrādātas kritiskās infrastruktūras aizsardzībai.

(26) Informācijas koplietošanai Eiropas kiberdrošības trauksmes sistēmas dalībnieku starpā būtu jāatbilst spēkā esošajām juridiskajām prasībām un jo īpaši Savienības un valstu datu aizsardzības tiesību aktiem, kā arī Savienības konkurences noteikumiem, kas reglamentē informācijas apmaiņu. Tādā mērā, kādā nepieciešama personas datu apstrāde, informācijas saņēmējam būtu jāīsteno tehniski un organizatoriski pasākumi, kas sargā datu subjektu tiesības un brīvības, un dati jāiznīcina, tiklīdz tie vairs nav nepieciešami norādītajam mērķim, un jāinformē vienība, kas datus dara pieejamus, ka dati ir iznīcināti.

(27) Konfidencialitātes un informācijas drošības saglabāšana ir ārkārtīgi svarīga visiem trim šīs regulas pīlāriem – lai veicinātu dalīšanos ar informāciju vai apmaiņu ar to Eiropas kiberdrošības trauksmes sistēmas kontekstā, lai saglabātu to vienību intereses, kuras piesakās uz atbalstu saskaņā ar kiberdrošības ārkārtas mehānismu, vai lai nodrošinātu, ka ziņojumi saskaņā ar Eiropas kiberdrošības incidentu izskatīšanas mehānismu var sniegt noderīgu pieredzi, negatīvi neietekmējot incidentu skartās vienības. Dalībvalstu un vienību dalība minētajos mehānismos ir atkarīga no uzticības attiecībām starp to komponentiem. Ja informācija ir konfidenciāla, ievērojot Savienības vai valstu noteikumus, dalīšanās vai apmaiņa ar to saskaņā ar šo regulu būtu jāierobežo līdz tādai, kas ir būtiska un samērīga ar dalīšanās vai apmaiņas mērķi. Minētajā informācijas nodošanā vai apmaiņā būtu arī jāievēro minētās informācijas konfidencialitāte, tostarp jāaizsargā attiecīgo vienību drošība un komerciālās intereses. Informācijas nodošana vai apmaiņa, ievērojot šo regulu, varētu notikt, izmantojot vienošanās par informācijas neizpaušanu vai norādījumus par informācijas izplatīšanu, piemēram, gaismas signālu protokolu (GSP). GSP ir jāsaprot kā līdzeklis, ar ko sniedz informāciju par jebkādiem ierobežojumiem attiecībā uz tālāku informācijas izplatīšanu. To izmanto gandrīz visās *CSIRT* un dažos *ISAC*. Papildus minētajām vispārīgajām prasībām attiecībā uz Eiropas kiberdrošības trauksmes sistēmu mitināšanas konsorciju nolīgumos būtu jāparedz īpaši noteikumi par informācijas nodošanas nosacījumiem attiecīgajā pārrobežu kiberdrošības centrā. Minētajos nolīgumos jo īpaši varētu prasīt, lai informācijas nodošana notiktu tikai saskaņā ar Savienības un valstu tiesību aktiem.

(28) Attiecībā uz ES kiberdrošības rezervju izmantošanu ir jāparedz īpaši konfidencialitātes noteikumi. Atbalsts tiks pieprasīts, novērtēts un sniegts krīzes apstākļos un attiecībā uz vienībām, kas darbojas sensitīvās nozarēs. Lai ES kiberdrošības rezerves darbotos efektīvi, ir svarīgi, lai lietotāji un vienības varētu bez kavēšanās dalīties ar visu informāciju, kas ir vajadzīga, lai katra vienība varētu piedalīties pieprasījumu novērtēšanā un atbalsta izmantošanā, un nodrošināt piekļuvi šādai informācijai. Attiecīgi šai regulai būtu jāparedz, ka visa šāda informācija ir jāizmanto vai ar to jādalās tikai tad, ja tas nepieciešams ES kiberdrošības rezervju darbībai, un ka informācija, kas ir konfidenciāla vai klasificēta saskaņā ar Savienības un valstu tiesību aktiem, ir jāizmanto un ar to jādalās tikai saskaņā ar minētajiem tiesību aktiem. Turklāt lietotājiem vajadzētu būt iespējai attiecīgā gadījumā izmantot dalīšanās ar informāciju protokolus, piemēram, GSP, lai sīkāk precizētu ierobežojumus. Lai gan lietotājiem šajā ziņā ir rīcības brīvība, ir svarīgi, lai šādu ierobežojumu piemērošanā tiktu ņemtas vērā iespējamās sekas, jo īpaši attiecībā uz pieprasīto pakalpojumu novēlotu novērtēšanu vai sniegšanu. Lai nodrošinātu ES kiberdrošības rezervju efektīvu darbību, ir svarīgi paredzēt, lai līgumslēdzēja iestāde pirms pieprasījuma iesniegšanas izskaidrotu lietotājam minētās sekas. Minētie aizsardzības pasākumi attiecas tikai uz ES kiberdrošības rezervju pakalpojumu pieprasīšanu un sniegšanu un neietekmē informācijas apmaiņu citos kontekstos, piemēram, ES kiberdrošības rezervju iepirkuma procesos.

(29) Ņemot vērā to, ka dalībvalstis skar aizvien lielāks kiberincidentu risks un skaits, ir jāizveido krīzes atbalsta instruments, proti, kiberdrošības ārkārtas mehānisms, lai uzlabotu Savienības noturību pret būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem un lielam mērogam līdzvērtīgiem kiberdrošības incidentiem un dalībvalstu darbības papildinātu ar ārkārtas finansiālu atbalstu būtiskāko dienestu gatavībai, reaģēšanai uz incidentiem un sākotnējas atkopšanās pasākumiem. Tā kā pilnīga atkopšanās pēc incidenta ir visaptverošs process, kura mērķis ir atjaunot incidenta skartās vienības darbību tādā stāvoklī, kāds bija pirms incidenta, un tas varētu būt ilgs process, kas saistīts ar ievērojamām izmaksām, tādēļ atbalsts no ES kiberdrošības rezervēm būtu jāattiecina tikai uz atkopšanās procesa sākumposmu, kā rezultātā tiktu atjaunotas sistēmu pamatfunkcijas. Kiberdrošības ārkārtas mehānismam būtu jānodrošina ātra un efektīva palīdzība noteiktos apstākļos un ar skaidriem nosacījumiem un jādod iespēja rūpīgi uzraudzīt un izvērtēt, kā resursi izmantoti. Lai gan pienākums incidentus un krīzes novērst, tām sagatavoties un uz tām reaģēt pirmām kārtām ir dalībvalstīm, kiberdrošības ārkārtas mehānisms veicina solidaritāti starp dalībvalstīm saskaņā ar Līguma par Eiropas Savienību (LES) 3. panta 3. punktu.

(30) Kiberdrošības ārkārtas mehānismam būtu jāparedz tāds atbalsts dalībvalstīm, kas papildina pašu dalībvalstu pasākumus un resursus, kā arī citas pastāvošās atbalsta iespējas, kad jāreaģē uz būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem un sākotnēji jāatkopjas pēc tiem, piemēram, pakalpojumus, ko sniedz *ENISA* saskaņā ar tās pilnvarām, koordinētu reaģēšanu un *CSIRT* tīkla palīdzību, *EU-CyCLONe* sniegto seku mazināšanas atbalstu, kā arī dalībvalstu savstarpējo palīdzību, tostarp – LES 42. panta 7. punkta kontekstā – pastāvīgās strukturētās sadarbības (*PESC*) kiberdrošības ātrās reaģēšanas vienību, kas izveidotas, ievērojot Padomes Lēmumu (KĀDP) 2017/2315,[15] atbalstu. Tam būtu jāapmierina vajadzība nodrošināt, ka ir pieejami specializēti līdzekļi, lai atbalstītu gatavību šādiem incidentiem, reaģēšanu uz tiem un atkopšanos pēc tiem visā Savienībā un *PDE* asociētajās trešās valstīs.

[15] Padomes Lēmums (KĀDP) 2017/2315 (2017. gada 11. decembris), ar ko izveido pastāvīgo strukturēto sadarbību (*PESCO*) un nosaka iesaistīto dalībvalstu sarakstu (OV L 331, 14.12.2017, 57. lpp., ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Šī regula neskar procedūras un regulējumu, kuru mērķis ir koordinēt Savienības līmeņa reaģēšanu krīzēs, jo īpaši Direktīvu (ES) 2022/2555, Savienības civilās aizsardzības mehānismu, kas izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES[16], *IPCR* mehānismus un Komisijas Ieteikumu (ES) 2017/1584[17]. Kiberdrošības ārkārtas mehānisma atbalsts var papildināt palīdzību, ko sniedz kopīgajā ārpolitikā un drošības politikā un kopīgajā drošības un aizsardzības politikā, tostarp izmantojot kiberdrošības ātrās reaģēšanas vienības, ņemot vērā Kiberdrošības ārkārtas mehānisma civilo raksturu. Atbalsts, ko sniedz saskaņā ar kiberdrošības ārkārtas mehānismu, var papildināt darbības, kuras tiek īstenotas LES 42. panta 7. punkta sakarā, tostarp palīdzību, ko viena dalībvalsts sniedz citai dalībvalstij, vai veidot daļu no Savienības un dalībvalstu kopīgās reakcijas vai LESD 222. pantā minētajos apstākļos. Attiecīgā gadījumā šīs regulas īstenošana būtu jākoordinē arī ar kiberdiplomātijas rīkkopas pasākumu īstenošanu.

---

16 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.).

17 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.).

(32) Saskaņā ar šo regulu sniegtajai palīdzībai būtu jāatbalsta un jāpapildina dalībvalstu līmenī veiktās darbības. Tālab būtu jānodrošina cieša sadarbība un apspriešanās starp Komisiju, *ENISA*, dalībvalstīm, un attiecīgā gadījumā *ECCC*. Pieprasot kiberdrošības ārkārtas mehānisma atbalstu, dalībvalstīm būtu jāsniedz attiecīga informācija, kas pamato atbalsta nepieciešamību.

(33) Direktīva (ES) 2022/2555 prasa dalībvalstīm izraudzīties vai izveidot vienu vai vairākas kiberkrīzes pārvaldības iestādes un nodrošināt, ka tām ir pietiekami resursi savu uzdevumu efektīvai un lietderīgai pildīšanai. Tā arī prasa dalībvalstīm apzināt spējas, līdzekļus un procedūras, ko var izmantot krīzes gadījumā, kā arī pieņemt valsts plānu reaģēšanai uz liela mēroga kiberdrošības incidentu un krīzi, kurā ir izklāstīti liela mēroga kiberdrošības incidentu un krīžu pārvaldības mērķi un kārtība. Dalībvalstīm arī jāizveido viena vai vairākas *CSIRT*, kurām uzticēti incidentu risināšanas pienākumi saskaņā ar skaidri definētu procesu un aptverot vismaz nozares, apakšnozares un vienību veidus, kas ir minētās direktīvas darbības jomā, un jānodrošina, ka tām ir pietiekami resursi savu uzdevumu faktiskai izpildei. Šī regula neskar Komisijas funkciju nodrošināt, ka dalībvalstis pilda Direktīvā (ES) 2022/2555 noteiktos pienākumus. Kiberdrošības ārkārtas mehānismam būtu jāpalīdz veikt darbības, kuru mērķis ir pastiprināt gatavību, kā arī darbības reaģēšanai uz incidentu, lai mazinātu būtisku kiberdrošības incidentu un liela mēroga kiberdrošības incidentu ietekmi, atbalstītu sākotnēju atkopšanos pēc tiem vai atjaunotu to pakalpojumu būtiskākās funkcijas, kurus sniedz vienības, kas darbojas sevišķi kritiskajās nozarēs vai vienības, kuras darbojas citās kritiskajās nozarēs.

(34) Lai gatavības darbību ietvaros veicinātu konsekventu pieeju un stiprinātu drošību visā Savienībā un tās iekšējā tirgū, būtu jāsniedz atbalsts, tostarp izmantojot mācības un apmācību, koordinētai tādu vienību kiberdrošības testēšanai un novērtēšanai, kuras darbojas sevišķi kritiskajās nozarēs, kas apzinātas, ievērojot Direktīvu (ES) 2022/2555. Minētajā nolūkā Komisijai pēc apspriešanās ar *ENISA*, TID sadarbības grupu un *EU-CyCLONe* regulāri būtu jānosaka attiecīgās nozares vai apakšnozares, kurām vajadzētu būt tiesīgām saņemt finansiālu atbalstu koordinētai gatavības testēšanai Savienības līmenī. Nozares vai apakšnozares būtu jāizraugās no Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajām sevišķi kritiskajām nozarēm. Koordinētās gatavības testēšanas pamatā vajadzētu būt kopīgiem riska scenārijiem un metodikai.

Nozaru atlasē un riska scenāriju izstrādē būtu jāņem vērā attiecīgie Savienības mēroga riska novērtējumi un riska scenāriji, tostarp vajadzība izvairīties no dublēšanās, piemēram, riska izvērtēšana un riska scenāriji, kurus izmantot aicināts Padomes secinājumos par Eiropas Savienības pozīcijas kiberjautājumos izstrādi, ko veic Komisija, Savienības Augstais pārstāvis ārlietās un drošības politikas jautājumos ("Augstais pārstāvis") un TID sadarbības grupa, sadarbībā 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, kas izveidota ar Eiropas Parlamenta un Padomes Regulu (ES) 2018/1971[18], Savienības līmeņa koordinēti kritiski svarīgu piegādes ķēžu drošības riska novērtējumi, kas veicami, ievērojot Direktīvas (ES) 2022/2555 22. pantu, un digitālās darbības noturības testēšana, kā paredzēts Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554[19]. Nozaru atlasē būtu jāņem vērā arī Padomes ieteikums par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai.

---

[18] Eiropas Parlamenta un Padomes Regula (ES) 2018/1971 (2018. gada 11. decembris), ar ko izveido Eiropas Elektronisko sakaru regulatoru iestādi (*BEREC*) un *BEREC* atbalsta aģentūru (*BEREC* birojs), groza Regulu (ES) 2015/2120 un atceļ Regulu (EK) Nr. 1211/2009 (OV L 321, 17.12.2018., 1. lpp.).

[19] 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 (OV L 333, 27.12.2022., 1. lpp.).

(35) Turklāt kiberdrošības ārkārtas mehānismam būtu jāsniedz atbalsts citām gatavības darbībām un jāatbalsta gatavība citās nozarēs, uz kurām neattiecas koordinēta gatavības testēšana vienībām, kuras darbojas sevišķi kritiskajās nozarēs, vai vienībām, kas darbojas citās kritiskajās nozarēs. Minētās darbības varētu ietvert dažādus valstu gatavības pasākumu veidus.

(36) Ja dalībvalstis saņem dotācijas gatavības darbību atbalstam, vienības, kas darbojas sevišķi kritiskajās nozarēs, var brīvprātīgi piedalīties minētajās darbībās. Laba prakse ir tāda, ka pēc šādām darbībām iesaistītās vienības izstrādā sanācijas plānu, lai īstenotu visus izrietošos ieteikumus par konkrētiem pasākumiem maksimāla labuma gūšanai no gatavības darbības. Lai gan ir svarīgi, lai dalībvalstis kā daļu no darbībām pieprasītu iesaistītajām vienībām izstrādāt un īstenot šādus sanācijas plānus, šī regula neparedz dalībvalstīm ne pienākumu, ne pilnvaras nodrošināt šādu pieprasījumu izpildi. Šādi pieprasījumi neskar prasības vienībām un kompetento iestāžu uzraudzības pilnvaras saskaņā ar Direktīvu (ES) 2022/2555.

(37) Kiberdrošības ārkārtas mehānismam arī būtu jāsniedz atbalsts reaģēšanas uz incidentiem darbībām, lai mazinātu būtisku kiberdrošības incidentu, liela mēroga kiberdrošības incidentu un lielam mērogam līdzvērtīgu kiberdrošības incidentu ietekmi, atbalstītu sākotnēju atkopšanos vai atjaunotu būtiskāko dienestu darbību. Attiecīgā gadījumā tam būtu jāpapildina UCPM, lai nodrošinātu visaptverošu pieeju reaģēšanai uz incidentu ietekmi uz iedzīvotājiem.

(38) Kiberdrošības ārkārtas mehānismam būtu jāatbalsta tehniskā palīdzība, ko viena dalībvalsts sniedz citai dalībvalstij, kuru skāris būtisks kiberdrošības incidents vai liela mēroga kiberdrošības incidents, tostarp palīdzība, ko sniedz *CSIRT*, kā minēts Direktīvas (ES) 2022/2555 11. panta 3. punkta f) apakšpunktā. Būtu jāļauj dalībvalstīm, kuras sniedz šādu palīdzību, iesniegt pieprasījumus segt izmaksas, kas saistītas ar ekspertu vienību nosūtīšanu savstarpējai palīdzībai. Attiecināmajās izmaksās varētu iekļaut kiberdrošības ekspertu ceļa, uzturēšanās un dienas naudas izdevumus.

(39) Ņemot vērā privāto uzņēmumu būtisko lomu liela mēroga kiberdrošības incidentu un lielam mērogam līdzvērtīgu kiberdrošības incidentu atklāšanā, gatavībā tiem un reaģēšanā uz tiem, ir svarīgi atzīt, cik vērtīga ir brīvprātīga *pro bono* sadarbība ar šādiem uzņēmumiem, kad tie piedāvā pakalpojumus bez atlīdzības liela mēroga kiberdrošības incidentu un lielam mērogam līdzvērtīgu kiberdrošības incidentu un krīžu gadījumos. *ENISA* sadarbībā ar *EU-CyCLONe* varētu uzraudzīt šādu *pro bono* iniciatīvu attīstību un veicināt to atbilstību kritērijiem, kas saskaņā ar šo regulu piemērojami uzticamiem pārvaldītu drošības pakalpojumu sniedzējiem, tostarp attiecībā uz privātu uzņēmumu uzticamību, to pieredzi, kā arī spēju drošā veidā rīkoties ar sensitīvu informāciju.

(40) Kiberdrošības ārkārtas mehānisma ietvaros, lai atbalstītu reaģēšanas darbības un sāktu atkopšanās darbības gadījumos, kad notiek būtiski kiberdrošības incidenti, liela mēroga kiberdrošības incidenti vai lielam mērogam līdzvērtīgi kiberdrošības incidenti, kas skar dalībvalstis, Savienības iestādes, struktūras, birojus vai aģentūras vai *PDE* asociētās trešās valstis, būtu pakāpeniski jāveido ES kiberdrošības rezerves, kas sastāv no uzticamu pārvaldītu drošības pakalpojumu sniedzēju pakalpojumiem. ES kiberdrošības rezervēm būtu jānodrošina pakalpojumu pieejamība un gatavība. Tāpēc tajās būtu jāiekļauj pakalpojumi, kas ir iepriekš nolīgti, tostarp, piemēram, spējas, kas ir pastāvīgā gatavībā un izmantojamas īsā laikā. Pakalpojumiem no ES kiberdrošības rezervēm būtu jāpalīdz valstu iestādēm papildus darbībām valsts līmenī sniegt palīdzību skartajām vienībām, kuras darbojas sevišķi kritiskajās vai vienībām, kuras darbojas citās kritiskajās nozarēs. Ar līdzīgiem nosacījumiem pakalpojumiem no ES kiberdrošības rezervēm vajadzētu būt izmantojamiem arī Savienības iestāžu, struktūru, biroju un aģentūru atbalstam. ES kiberdrošības rezerves varētu arī palīdzēt stiprināt rūpniecības un pakalpojumu konkurētspēju Savienībā visā digitālajā ekonomikā, kas ietver arī mikrouzņēmumus un mazos un vidējos uzņēmumus, kā arī jaunuzņēmumus, un to darīt, cita starpā stimulējot investīcijas pētniecībā un inovācijā. Iepērkot ES kiberdrošības rezervēm paredzētos pakalpojumus, ir svarīgi ņemt vērā *ENISA* Eiropas kiberdrošības prasmju satvaru. Pieprasot atbalstu no ES kiberdrošības rezervēm, lietotājiem savā pieteikumā būtu jāiekļauj atbilstoša informācija par skarto vienību un iespējamo ietekmi, informācija par pieprasīto pakalpojumu no rezervēm un atbalstu, kas skartajai vienībai sniegts valsts līmenī, ko būtu jāņem vērā, novērtējot pieteikuma iesniedzēja pieprasījumu. Lai nodrošinātu papildināmību ar citiem skartajai vienībai pieejamā atbalsta veidiem, pieprasījumā būtu jāiekļauj arī informācija, ja tāda ir pieejama, par spēkā esošu līgumisku vienošanos attiecībā uz reaģēšanas uz incidentiem un sākotnējas atkopšanās pakalpojumiem, kā arī par apdrošināšanas līgumiem, kas potenciāli aptver šāda veida incidentu.

(41) Lai nodrošinātu Savienības finansējuma efektīvu izmantošanu, iepriekš nolīgtie pakalpojumi saskaņā ar ES kiberdrošības rezervēm būtu atbilstoši attiecīgajam līgumam jāpārveido par gatavības pakalpojumiem, kas saistīti ar incidentu novēršanu un reaģēšanu uz tiem, ja minētie iepriekš nolīgtie pakalpojumi netiek izmantoti reaģēšanai uz incidentiem laikā, uz kādu tie ir iepriekš nolīgti. Minētajiem pakalpojumiem vajadzētu būt savstarpēji papildinošiem un nebūtu jādublē *ECCC* pārvaldītās gatavības darbības.

(42) Pieprasījumi saņemt atbalstu no ES kiberdrošības rezervēm, ko dalībvalstu kiberkrīžu pārvaldības iestādes un *CSIRT* vai *CERT*-EU iesniedz Savienības iestāžu, struktūru, biroju un aģentūru vārdā, būtu jāizvērtē līgumslēdzējai iestādei. Minētā līgumslēdzēja iestāde ir *ENISA*, ja tai ir uzticēta ES kiberdrošības rezervju darbības nodrošināšana un pārvaldība. Atbalsta pieprasījumi no *PDE* asociētajām trešām valstīm būtu jāizvērtē Komisijai. Lai atvieglotu atbalsta pieprasījumu iesniegšanu un novērtēšanu, *ENISA* varētu izveidot drošu platformu.

(43) Ja tiek saņemti vairāki paralēli pieprasījumi, tie būtu jāsakārto prioritārā secībā saskaņā ar šajā regulā noteiktajiem kritērijiem. Ņemot vērā šīs regulas vispārīgos mērķus, minētajiem kritērijiem būtu jāietver incidenta apmērs un smagums, skartās vienības veids, incidenta iespējamā ietekme uz skartajām dalībvalstīm un lietotājiem, incidenta iespējamais pārrobežu raksturs un izplatīšanās risks, kā arī pasākumi, ko lietotājs jau ir veicis, lai sekmētu reaģēšanu un sākotnēju atkopšanos. Ņemot vērā minētos mērķus un to, ka dalībvalstu lietotāju pieprasījumi ir paredzēti vienīgi tam, lai visā Savienībā atbalstītu vienības, kuras darbojas sevišķi kritiskajās nozarēs vai vienības, kuras darbojas citās kritiskajās nozarēs, ir lietderīgi piešķirt augstāku prioritāti dalībvalstu lietotāju pieprasījumiem, ja minēto kritēriju rezultātā divi vai vairāki pieprasījumi tiek novērtēti kā līdzvērtīgi. Tas neskar nekādus pienākumus, kas dalībvalstīm var būt saskaņā ar attiecīgajiem mitināšanas nolīgumiem, proti, veikt pasākumus, lai aizsargātu Savienības iestādes, struktūras, birojus un aģentūras un palīdzētu tām.

(44) Komisijai vajadzētu būt vispārējai atbildībai par ES kiberdrošības rezervju īstenošanu. Ņemot vērā plašo pieredzi, ko *ENISA* guvusi kiberdrošības atbalsta darbībā, *ENISA* ir vispiemērotākā aģentūra ES kiberdrošības rezervju īstenošanai. Tāpēc Komisijai ES kiberdrošības rezervju darbības nodrošināšana un pārvaldība būtu jāuztic *ENISA* vai nu daļēji, vai, ja Komisija to uzskata par lietderīgu, pilnībā. Pilnvarojums būtu jāīsteno saskaņā ar piemērojamajiem noteikumiem, kas paredzēti Regulā (ES, *Euratom*) 2024/2509, un jo īpaši uz to būtu jāattiecina attiecīgie iemaksu nolīguma parakstīšanas nosacījumi. Jebkuri ES kiberdrošības rezervju darbības un administrēšanas aspekti, kas nav uzticēti *ENISA*, būtu tieši jāpārvalda Komisijai, tostarp pirms iemaksu nolīguma parakstīšanas.

(45) Dalībvalstīm vajadzētu būt svarīgai lomai ES kiberdrošības rezervju izveidē, ieviešanā un pēcieviešanā. Tā kā Regula (ES) 2021/694 ir attiecīgais pamatakts darbībām, ar kurām īsteno ES kiberdrošības rezerves, darbības saskaņā ar ES kiberdrošības rezervēm būtu jāparedz attiecīgajās darba programmās, kas minētas Regulas (ES) 2021/694 24. pantā. Ievērojot minētā panta 6. punktu, minētās darba programmas Komisijai jāpieņem ar īstenošanas aktiem saskaņā ar pārbaudes procedūru. Turklāt Komisijai saskaņoti ar TID sadarbības grupu būtu jānosaka ES kiberdrošības rezervju prioritātes un attīstība.

(46) Līgumiem, kas noslēgti saistībā ar ES kiberdrošības rezervēm, nebūtu jāietekmē uzņēmumu savstarpējās attiecības un pastāvošās saistības starp skarto vienību vai lietotājiem un pakalpojumu sniedzēju.

(47) Lai izvēlētos privātos pakalpojumu sniedzējus pakalpojumu sniegšanai saistībā ar ES kiberdrošības rezervēm, ir nepieciešams noteikt minimālo kritēriju un prasību kopumu, kas būtu jāiekļauj uzaicinājumā iesniegt piedāvājumus, lai atlasītu minētos pakalpojumu sniedzējus, tādējādi nodrošinot, ka tiek apmierinātas dalībvalstu iestāžu, vienību, kuras darbojas sevišķi kritiskajās nozarēs, un vienību, kuras darbojas citās kritiskajās nozarēs, vajadzības. Lai risinātu dalībvalstu īpašās vajadzības, līgumslēdzējai iestādei, iepērkot pakalpojumus saistībā ar ES kiberdrošības rezervēm, attiecīgā gadījumā būtu jāizstrādā atlases kritēriji un prasības papildus tiem, kas noteikti šajā regulā. Ir svarīgi veicināt tādu mazāku pakalpojumu sniedzēju līdzdalību, kuri darbojas reģionālā un vietējā līmenī.

(48) Izvēloties pakalpojumu sniedzējus iekļaušanai ES kiberdrošības rezervēs, līgumslēdzējai iestādei būtu jācenšas nodrošināt, ka ES kiberdrošības rezerves kopumā ietver pakalpojumu sniedzējus, kas spēj apmierināt lietotāju valodas prasības. Šajā nolūkā līgumslēdzējai iestādei pirms konkursa specifikāciju sagatavošanas būtu jānoskaidro, vai potenciālajiem ES kiberdrošības rezervju lietotājiem ir īpašas valodas prasības, lai ES kiberdrošības rezervju atbalsta pakalpojumus varētu sniegt kādā no Savienības institūciju vai dalībvalstu oficiālajām valodām, ko lietotājs vai skartā vienība varētu saprast. Ja ES kiberdrošības rezervju atbalsta pakalpojumu sniegšanai lietotājam ir vajadzīga vairāk nekā viena valoda un minētie pakalpojumi konkrētajam lietotājam ir iegādāti minētajās valodās, lietotājam ES kiberdrošības rezervju atbalsta pieprasījumā vajadzētu būt iespējai norādīt, kurā no šīm valodām pakalpojumi būtu jāsniedz saistībā ar konkrēto incidentu, kas ir pieprasījuma pamatā.

(49) Atbalstot ES kiberdrošības rezervju izveidi, ir svarīgi, lai Komisija pieprasītu *ENISA* sagatavot kandidātu kiberdrošības sertifikācijas shēmu pārvaldītiem drošības pakalpojumiem, ievērojot Regulu (ES) 2019/881, jomās, uz kurām attiecas kiberdrošības ārkārtas mehānisms.

(50) Lai atbalstītu šīs regulas mērķus veicināt kopīgu stāvokļa apzināšanos, uzlabot Savienības noturību un sekmēt spēju efektīvi reaģēt uz būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem, Komisijai vai *EU-CyCLONe* vajadzētu būt iespējai lūgt *ENISA* ar *CSIRT* tīkla atbalstu un attiecīgo dalībvalstu piekrišanu izskatīt un novērtēt kiberdraudus, zināmas ļaunprātīgi izmantojamas ievainojamības un seku mazināšanas darbības konkrēta būtiska kiberdrošības incidenta vai liela mēroga kiberdrošības incidenta sakarā. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* sadarbībā ar attiecīgo dalībvalsti, attiecīgajām ieinteresētajām personām, tostarp privātā sektora, Komisijas un citu attiecīgo Savienības iestāžu, struktūru, biroju un aģentūru pārstāvjiem, būtu jāsagatavo incidenta pārskata ziņojums. Pamatojoties uz sadarbību ar ieinteresētajām personām, ieskaitot privāto sektoru, pārskata ziņojumam par konkrētiem incidentiem vajadzētu būt vērstam uz to, lai pēc incidenta novērtētu tā cēloņus, ietekmi un seku mazinājumu. Īpaša uzmanība būtu jāpievērš ieguldījumam un pieredzei, ar ko dalās pārvaldīto drošības pakalpojumu sniedzēji, kuri atbilst visaugstākās profesionālās godprātības, objektivitātes un nepieciešamo tehnisko zināšanu nosacījumiem, kā noteikts šajā regulā. Ziņojums būtu jāiesniedz *EU-CyCLONe*, *CSIRT* tīklam un Komisijai, un būtu jāizmanto to darbā un *ENISA* darbā. Ja incidents ir saistīts ar *PDE* asociētu trešo valsti, Komisijai ziņojums būtu jāiesniedz arī Augstajam pārstāvim.

(51) Ņemot vērā kiberdrošības uzbrukumu neparedzamību un to, ka tie mēdz neaprobežoties ar noteiktu ģeogrāfisku apgabalu un tiem ir augsts izplatīšanās risks, kaimiņvalstu noturības stiprināšana un to spēja efektīvi reaģēt uz būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem veicina visas Savienības, jo īpaši tās iekšējā tirgus un rūpniecības, aizsardzību kopumā. Šādas darbības varētu vēl vairāk veicināt Savienības kiberdiplomātiju. Tāpēc *PDE* asociētajām trešām valstīm vajadzētu būt iespējai pieprasīt atbalstu no ES kiberdrošības rezervēm visā to teritorijā vai tās daļā, ja tas ir paredzēts nolīgumā, ar kuru nosaka šīs trešās valsts asociāciju ar *PDE*. Savienībai būtu jāatbalsta finansējums *PDE* asociētajām trešām valstīm atbilstīgi attiecīgajām šīm valstīm paredzētajām partnerībām un finansēšanas instrumentiem. Atbalstam būtu jāaptver pakalpojumi, kas paredzēti reaģēšanai uz būtiskiem kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem un sākotnējas atkopšanās pasākumiem.

(52) Šīs regulas nosacījumi ES kiberdrošības rezervēm un uzticamiem pārvaldītas drošības pakalpojumu sniedzējiem būtu jāpiemēro, sniedzot atbalstu *PDE* asociētajām trešām valstīm. *PDE* asociētajām trešām valstīm vajadzētu būt iespējai pieprasīt atbalstu no ES kiberdrošības rezervēm, ja vienības, kuras ir skartas un kurām tās pieprasa atbalstu no ES kiberdrošības rezervēm, ir vienības, kas darbojas sevišķi kritiskajās nozarēs vai vienības, kas darbojas citās kritiskajās nozarēs, un ja atklātie incidenti rada būtiskus darbības traucējumus vai tiem varētu būt plašāka ietekme Savienībā. *PDE* asociētajām trešām valstīm vajadzētu būt tiesīgām saņemt atbalstu tikai tad, ja nolīgums, kas nosaka to asociēšanu ar *PDE*, īpaši paredz šādu atbalstu. Turklāt šādām trešām valstīm vajadzētu palikt atbalsttiesīgām tikai tik ilgi, kamēr tiek izpildīti trīs kritēriji. Pirmkārt, trešai valstij būtu pilnībā jāievēro attiecīgie minētā nolīguma noteikumi. Otrkārt, ņemot vērā ES kiberdrošības rezervju papildinošo raksturu, trešai valstij būtu vajadzējis pašai veikt atbilstošus pasākumus, lai sagatavotos būtiskiem kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem. Treškārt, atbalsta sniegšanai no ES kiberdrošības rezervēm vajadzētu atbilst Savienības politikai attiecībā uz minēto valsti un vispārējām attiecībām ar to, kā arī citiem Savienības politikas virzieniem drošības jomā. Saistībā ar novērtējumu par atbilstību šim trešajam kritērijam Komisijai būtu jāapspriežas ar Augsto pārstāvi par to, lai šāda atbalsta piešķiršana tiktu saskaņota ar kopējo ārpolitikas un drošības politiku.

(53) Atbalsta sniegšana *PDE* asociētajām trešām valstīm var ietekmēt attiecības ar trešām valstīm un Savienības drošības politiku, tostarp kopējās ārpolitikas un drošības politikas un kopējās drošības un aizsardzības politikas kontekstā. Tādēļ ir lietderīgi Padomei piešķirt īstenošanas pilnvaras atļaut un precizēt laikposmu, kurā šādu atbalstu var sniegt. Padomei būtu jārīkojas, pamatojoties uz Komisijas priekšlikumu un pienācīgi ņemot vērā Komisijas novērtējumu par minētajiem trim kritērijiem. Tas pats būtu jāattiecina uz atjaunošanu un priekšlikumiem grozīt vai atcelt šādus aktus. Ja Padome izņēmuma kārtā uzskata, ka attiecībā uz trešo kritēriju apstākļi ir būtiski mainījušies, Padomei vajadzētu būt iespējai rīkoties pēc savas iniciatīvas grozīt vai atcelt īstenošanas aktu, negaidot Komisijas priekšlikumu. Šādu būtisku izmaiņu gadījumā, visticamāk, būs jārīkojas steidzami un tām būs īpaši svarīga ietekme uz attiecībām ar trešām valstīm, tādēļ tām nebūs nepieciešams iepriekšējs un detalizēts Komisijas novērtējums. Turklāt Komisijai attiecībā uz pieprasījumiem par atbalsta sniegšana *PDE* asociētajām trešām valstīm un par šādām trešām valstīm piešķirtā atbalsta īstenošanu būtu jāsadarbojas ar Augsto pārstāvi. Komisijai būtu arī jāņem vērā *ENISA* sniegtie viedokļi par šādiem pieprasījumiem un atbalstu. Komisijai būtu jāinformē Padome par pieprasījumu novērtējuma rezultātiem, tostarp par attiecīgiem šajā sakarībā paustiem apsvērumiem, un par sniegtajiem pakalpojumiem.

(54) Komisijas 2023. gada 18. aprīļa paziņojumā par Kiberprasmju akadēmiju atzīts kvalificētu speciālistu trūkums. Šādas prasmes ir vajadzīgas šīs regulas mērķu sasniegšanai. Savienībā ir steidzami vajadzīgi profesionāļi ar tādām prasmēm un kompetencēm, kas vajadzīgas, lai novērstu, atklātu un aizkavētu kiberuzbrukumus un aizsargātu Savienību, tostarp tās kritiski vissvarīgāko infrastruktūru, pret šādiem uzbrukumiem un nodrošinātu tās noturību. Minētajā nolūkā ir svarīgi veicināt sadarbību starp ieinteresētajām personām, tostarp privāto sektoru, akadēmiskajām aprindām un publisko sektoru. Vienlīdz svarīgi ir radīt sinerģiju visās Savienības teritorijās attiecībā uz investīcijām izglītībā un apmācībā, lai veicinātu aizsardzības pasākumu izveidi nolūkā novērst intelektuālā darbaspēka emigrāciju vai prasmju trūkuma palielināšanos dažos reģionos vairāk nekā citos. Ir steidzami jānovērš kiberdrošības prasmju trūkums, īpašu uzmanību pievēršot kiberdrošības darbaspēka dzimumu nevienlīdzības mazināšanai, lai veicinātu sieviešu klātbūtni un līdzdalību digitālās pārvaldības izveidē.

(55) Lai veicinātu inovāciju digitālajā vienotajā tirgū, ir svarīgi stiprināt pētniecību un inovāciju kiberdrošības jomā, lai sekmētu dalībvalstu noturības uzlabošanu un Savienības atvērto stratēģisko autonomiju, kas abi ir šīs regulas mērķi. Sinerģija ir būtiska, lai stiprinātu sadarbību un koordināciju starp dažādām ieinteresētajām personām, tostarp privāto sektoru, pilsonisko sabiedrību un akadēmiskajām aprindām.

(56) Šai regulai būtu jāņem vērā apņemšanās, kas izklāstīta Eiropas Parlamenta, Padomes un Komisijas 2022. gada 26. janvāra kopīgajā deklarācijā "Eiropas Deklarācija par digitālajām tiesībām un principiem digitālajai desmitgadei" aizsargāt Savienības demokrātiju, cilvēku, uzņēmumu un publisko iestāžu intereses pret kiberdrošības riskiem un kibernoziedzību, tostarp datu aizsardzības pārkāpumiem un identitātes zādzību vai manipulācijām.

(57) Lai papildinātu dažus nebūtiskus šīs regulas elementus, būtu jādeleģē Komisijai pilnvaras saskaņā ar LESD 290. pantu precizēt to reaģēšanas pakalpojumu veidus un skaitu, kas vajadzīgi ES kiberdrošības rezervēm. Ir īpaši būtiski, lai Komisija, veicot sagatavošanas darbus, rīkotu atbilstīgas apspriešanās, tostarp ekspertu līmenī, un lai minētās apspriešanās tiktu rīkotas saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu[20]. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienādu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem, un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana.

[20] OV L 123, 12.5.2016., 1. lpp, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(58) Lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, būtu jāpiešķir īstenošanas pilnvaras Komisijai, lai papildus noteiktu detalizētu kārtību ES kiberdrošības rezervju atbalsta pakalpojumu piešķiršanai. Minētās pilnvaras būtu jāizmanto saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011[21].

(59) Neskarot Līgumos paredzētos noteikumus par Savienības gada budžetu, Komisijai, kad tā novērtējot *ENISA* budžeta un personāla vajadzības, būtu jāņem vērā pienākumi, kas izriet no šīs regulas.

(60) Komisijai būtu regulāri jāizvērtē šajā regulā paredzētie pasākumi. Pirmais šāds izvērtējums būtu jāveic pirmajos divos gados pēc šīs regulas spēkā stāšanās dienas un pēc tam vismaz reizi četros gados, ņemot vērā daudzgadu finanšu shēmas, kas pieņemta ievērojot LESD 312. pantu, pārskatīšanas grafiku. Komisijai būtu jāiesniedz Eiropas Parlamentam un Padomei progresa ziņojums. Lai novērtētu dažādos nepieciešamos elementus, tostarp Eiropas kiberdrošības trauksmes sistēmā nodotās informācijas apjomu, Komisijai būtu jābalstās tikai uz informāciju, kas ir viegli pieejama vai sniegta brīvprātīgi. Ņemot vērā ģeopolitiskās norises un mērķi nodrošināt šajā regulā noteikto pasākumu nepārtrauktību un turpmāku attīstību pēc 2027. gada, ir svarīgi, lai Komisija novērtētu vajadzību daudzgadu finanšu shēmā 2028.–2034. gadam paredzēt atbilstīgus budžeta līdzekļus.

---

[21] Eiropas Parlamenta un Padomes Regula (ES) Nr. 182/2011 (2011. gada 16. februāris), ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13. lpp., ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) Ņemot vērā to, ka šīs regulas mērķus, proti, stiprināt rūpniecības un pakalpojumu konkurētspēju Savienībā visā digitālajā ekonomikā un veicināt Savienības tehnoloģisko suverenitāti un atvērtu stratēģisko autonomiju kiberdrošības jomā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet darbības mēroga vai iedarbības dēļ tos var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar LES 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minēto mērķu sasniegšanai,

IR PIEŅĒMUŠI ŠO REGULU.

I nodaļa
Vispārīgi noteikumi

1. pants

Priekšmets un mērķi

1. Šī regula nosaka pasākumus, kuru mērķis ir stiprināt spējas Savienībā atklāt kiberdrošības apdraudējumus un incidentus, tiem sagatavoties un uz tiem reaģēt, izveidojot:

a) Eiropas mēroga kibercentru tīklu (Eiropas kiberdrošības trauksmes sistēmas), lai veidotu un uzlabotu koordinētas atklāšanas un kopīgas situācijas apzināšanās spējas;

b) kiberdrošības ārkārtas mehānismu, lai palīdzētu dalībvalstīm sagatavoties būtiskiem un liela mēroga kiberdrošības incidentiem, uz tiem reaģēt, mazināt to ietekmi un sākt atkopšanos pēc tiem un palīdzētu citiem lietotājiem reaģēt uz būtiskiem kiberdrošības incidentiem un lielam mērogam līdzvērtīgiem kiberdrošības incidentiem;

c) Eiropas kiberdrošības incidentu izskatīšanas mehānismu, lai izskatītu un novērtētu būtiskus kiberdrošības incidentus vai liela mēroga kiberdrošības incidentus.

2. Šīs regulas mērķis ir sasniegt vispārīgos mērķus – stiprināt rūpniecības un pakalpojumu, tostarp mikrouzņēmumu un mazo un vidējo uzņēmumu, kā arī jaunuzņēmumu, konkurētspēju Savienībā visā digitālajā ekonomikā un veicināt Savienības tehnoloģisko suverenitāti un atvērtu stratēģisko autonomiju kiberdrošības jomā, tostarp veicinot inovāciju digitālajā vienotajā tirgū. Tā tiecas sasniegt minētos mērķus, stiprinot solidaritāti Savienības līmenī, papildinot kiberdrošības ekosistēmu, uzlabojot dalībvalstu kibernoturību un attīstot darbaspēka prasmes, zinātību, spējas un kompetences kiberdrošības jomā.

3. Panta 2. punktā minēto vispārīgo mērķu sasniegšanu tuvina ar šādu konkrētu mērķu starpniecību:

a) stiprināt kiberdraudu un incidentu kopīgas koordinētas atklāšanas spējas Savienības līmenī un kopīgu situācijas apzināšanos;

b) visā Savienībā stiprināt to vienību gatavību, kuras darbojas sevišķi kritiskajās nozarēs, vai tās vienības, kuras darbojas citās kritiskajās nozarēs, un stiprināt solidaritāti, attīstot koordinētas gatavības testēšanas spējas un spējas labāk reaģēt un atkopties būtisku kiberdrošības incidentu, liela mēroga kiberdrošības incidentu vai lielam mērogam līdzvērtīgu kiberdrošības incidentu gadījumā, tostarp paredzot iespēju darīt pieejamu Savienības atbalstu *PDE* asociētajām trešām valstīm reaģēšanai uz kiberdrošības incidentiem;

c) uzlabot Savienības noturību un veicināt iedarbīgu reaģēšanu, pārskatot un novērtējot būtiskus kiberdrošības incidentus vai liela mēroga kiberdrošības incidentus, mācoties no tiem un attiecīgā gadījumā sagatavojot ieteikumus.

4. Darbības saskaņā ar šo regulu veic, pienācīgi ievērojot dalībvalstu kompetences, un tās papildina darbības, ko veic *CSIRT* tīkls, *EU-CyCLONe* un TID sadarbības grupa.

5. Šī regula neskar dalībvalstu būtiskākās valstu funkcijas, tostarp valstu teritoriālās integritātes nodrošināšanu, likumības un kārtības uzturēšanu un valstu drošības aizsardzību. Jo īpaši valsts drošība paliek vienīgi katras dalībvalsts atbildībā.

6. Dalīšanās vai apmaiņa ar tādu informāciju atbilstīgi šai regulai, kas ir konfidenciāla, ievērojot Savienības vai valstu noteikumus, ietver tikai tādu informāciju, kura ir būtiska un ir samērīga ar dalīšanās vai apmaiņas nolūku. Dalīšanās vai apmaiņa ar šādu konfidencialitāti saglabā minētās informācijas konfidencialitāti un aizsargā attiecīgo vienību drošību un komerciālās intereses. Tas nenozīmē tādas informācijas sniegšanu, kuras izpaušana būtu pretrunā būtiskām dalībvalstu drošības, sabiedrības drošības vai aizsardzības interesēm.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "pārrobežu kibercentrs" ir daudzvalstu platforma, kas izveidota ar rakstisku konsorcija nolīgumu un koordinētā tīkla struktūrā apvieno valstu kibercentrus no vismaz trim dalībvalstīm, un ir izstrādāta, lai sekmētu kiberdraudu uzraudzību, atklāšanu un analīzi nolūkā novērst incidentus un sniegt atbalstu kiberdraudu izlūkdatu sagatavošanā, jo īpaši apmainoties ar nozīmīgiem un attiecīgā gadījumā anonimizētiem datiem un informāciju, kā arī daloties ar modernākiem rīkiem un uzticamā vidē kopīgi attīstot kiberatklāšanas, analīzes, novēršanas un aizsardzības spējas;

2) "mitināšanas konsorcijs" ir konsorcijs, ko veido iesaistītās dalībvalstis, kuras ir piekritušas izveidot rīkus, infrastruktūru vai pakalpojumus pārrobežu kibercentra vajadzībām un veicināt to iegādi un darbību;

3) "*CSIRT*" ir *CSIRT*, kas izveidota, ievērojot Direktīvas (ES) 2022/2555 10. pantu;

4) "vienība" ir vienība, kā definēts Direktīvas (ES) 2022/2555 6. panta 38) punktā;

5) “vienības, kas darbojas sevišķi kritiskajās nozarēs”, ir Direktīvas (ES) 2022/2555 I pielikumā uzskaitīto vienību veidi;

6) “vienības, kas darbojas citās kritiskajās nozarēs”, ir Direktīvas (ES) 2022/2555 II pielikumā uzskaitīto vienību veidi;

7) “risks” ir risks, kā definēts Direktīvas (ES) 2022/2555 6. panta 9) punktā;

8) “kiberdraudi” ir kiberdraudi, kā definēts Regulas (ES) 2019/881 2. panta 8) punktā;

9) “incidents” ir incidents, kā definēts Direktīvas (ES) 2022/2555 6. panta 6) punktā;

10) “būtisks kiberdrošības incidents” ir kiberdrošības incidents, kas atbilst Direktīvas (ES) 2022/2555 23. panta 3. punktā noteiktajiem kritērijiem;

11) “liels incidents” ir liels incidents, kā definēts Eiropas Parlamenta un Padomes Regulas (ES, *Euratom*) 2023/2841[22] 3. panta 8. punktā;

12) “liela mēroga kiberdrošības incidents” ir liela mēroga kiberdrošības incidents, kā definēts Direktīvas (ES) 2022/2555 6. panta 7. punktā;

[22] Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2023/2841 (2023. gada 13. decembris), kas paredz pasākumus nolūkā panākt vienādu augstu kiberdrošības līmeni Savienības iestādēs, struktūrās, birojos un aģentūrās (OJ L, 2023/2841, 18.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13) “lielam mērogam līdzvērtīgs kiberdrošības incidents” Savienības iestāžu, struktūru, biroju un aģentūru gadījumā ir liels incidents, un – *PDE* asociēto trešo valstu gadījumā – incidents, kas izraisa traucējumu līmeni, kurš pārsniedz attiecīgās *PDE* asociētās trešās valsts spēju uz to reaģēt;

14) “*PDE* asociētā trešā valsts” ir trešā valsts, kas ir puse nolīgumā ar Savienību, kurš ļauj tai piedalīties programmā “Digitālā Eiropa”, ievērojot Regulas (ES) 2021/694 10. pantu;

15) “līgumslēdzēja iestāde” ir Komisija vai – ciktāl ES kiberdrošības rezervju darbības nodrošināšana un pārvaldība ir uzticēta *ENISA*, ievērojot 14. panta 5. punktu, – *ENISA*;

16) “pārvaldītu drošības pakalpojumu sniedzējs” ir pārvaldītu drošības pakalpojumu sniedzējs, kā definēts Direktīvas (ES) 2022/2555 6. panta 40) punktā;

17) “uzticami pārvaldītu drošības pakalpojumu sniedzēji” ir pārvaldītu drošības pakalpojumu sniedzēji, kas atlasīti iekļaušanai ES kiberdrošības rezervēs saskaņā ar 17. pantu.

II nodaļa

Eiropas kiberdrošības trauksmes sistēma

3. pants

Eiropas kiberdrošības trauksmes sistēmas izveide

1. Lai sekmētu Savienības progresīvas spējas atklāt, analizēt un apstrādāt datus saistībā ar kiberdraudiem un incidentu novēršanu Savienībā, izveido Eiropas kiberdrošības trauksmes sistēmu – Eiropas mēroga infrastruktūras tīklu, kas sastāv no valstu kibercentriem un pārrobežu kibercentriem, kuri pievienojas brīvprātīgi.

2. Eiropas kiberdrošības trauksmes sistēma:

   a) veicina labāku aizsardzību un reaģēšanu uz kiberdraudiem, atbalstot un sadarbojoties ar attiecīgajām vienībām, jo īpaši *CSIRT*, *CSIRT* tīklu, *EU-CyCLONe* un kompetentajām iestādēm, kas izraudzītas vai izveidotas, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu, un stiprinot to spējas;

   b) pārrobežu kibercentros apkopo dažādu avotu datus un informāciju par kiberdraudiem un incidentiem un ar pārrobežu kibercentru starpniecību nodod analizēto vai apkopoto informāciju, attiecīgā gadījumā ar *CSIRT* tīklu;

c) vāc un atbalsta kvalitatīvas un tūlīt izmantojamas informācijas un kiberdraudu izlūkdatu sagatavošanu, izmantojot modernākos rīkus un progresīvas tehnoloģijas, un dalās ar minēto informāciju un kiberdraudu izlūkdatiem;

d) palīdz uzlabot kiberdraudu koordinētu atklāšanu un kopīgu situācijas apzināšanos visā Savienībā un izsludināt kiberdrošības brīdinājumus, tostarp attiecīgā gadījumā sniedzot konkrētus ieteikumus vienībām;

e) sniedz pakalpojumus un darbības kiberdrošības kopienai Savienībā, veicinot arī progresīvu rīku un tehnoloģiju, piemēram, mākslīgā intelekta un datu analīzes rīku, izstrādi.

3. Eiropas kiberdrošības trauksmes sistēmas īstenošanas darbības atbalsta ar programmas "Digitālā Eiropa" (*PDE*) finansējumu un īsteno saskaņā ar Regulu (ES) 2021/694, jo īpaši tās konkrēto mērķi Nr. 3.

4. pants

Valstu kibercentri

1. Ja dalībvalsts nolemj piedalīties Eiropas kiberdrošības trauksmes sistēmā, tā šīs regulas nolūkiem norīko vai attiecīgā gadījumā izveido valsts kibercentru.

2. Valsts kibercentrs ir viena vienota vienība, kas darbojas dalībvalsts pakļautībā. Tas var būt *CSIRT* vai attiecīgā gadījumā valsts kiberkrīžu pārvaldības iestāde, vai cita kompetentā iestāde, kas norīkota vai izveidota, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu, vai arī cita vienība. Valsts kibercentrs:

a) spēj darboties kā atsauces punkts un vārteja citām publiskām un privātām organizācijām valsts līmenī informācijas par kiberdraudiem un incidentiem vākšanai un analizēšanai un pārrobežu kibercentra, kā minēts 5. pantā, darbības sekmēšanai; un

b) spēj atklāt, apkopot un analizēt datus un informāciju, kas attiecas uz kiberdraudiem un incidentiem, piemēram, kiberdraudu izlūkdatus, jo īpaši izmantojot modernākās tehnoloģijas, nolūkā novērst incidentus.

3. Atbilstīgi šā panta 2. punktā minētajām funkcijām valstu kibercentri var sadarboties ar privātā sektora vienībām, lai apmainītos ar attiecīgiem datiem un informāciju nolūkā atklāt un novērst kiberdraudus un incidentus, tostarp ar būtisko un svarīgo vienību nozaru un starpnozaru kopienām, kā minēts Direktīvas (ES) 2022/2555 3. pantā. Attiecīgā gadījumā un saskaņā ar Savienības un valstu tiesību aktiem valstu kibercentru pieprasītā vai saņemtā informācija var ietvert telemetrijas, sensoru un reģistrēšanas datus.

4. Dalībvalsts, kas atlasīta, ievērojot 9. panta 1. punktu, apņemas pieteikt tās valsts kibercentru dalībai pārrobežu kibercentrā.

5. pants

Pārrobežu kibercentri

1. Ja vismaz trīs dalībvalstis ir apņēmušās nodrošināt, ka to valstu kibercentri sadarbojas, lai koordinētu to kiberatklāšanas un apdraudējuma uzraudzības darbības, minētās dalībvalstis šīs regulas nolūkā var izveidot mitināšanas konsorciju.

2. Mitināšanas konsorcijs ir konsorcijs, ko veido vismaz trīs iesaistītās dalībvalstis, kuras ir piekritušas izveidot pārrobežu kibercentru un veicināt tā rīku, infrastruktūras vai pakalpojumu iegādi un darbību saskaņā ar 4. punktu.

3. Ja mitināšanas konsorciju atlasa saskaņā ar 9. panta 3. punktu, tā dalībnieki noslēdz rakstisku konsorcija nolīgumu:

   a) kurā izklāstīta iekšējā kārtība 9. panta 3. punktā minētā mitināšanas un izmantošanas nolīguma īstenošanai;

   b) ar ko izveido mitināšanas konsorcija pārrobežu kibercentru; un

   c) kas ietver īpašus noteikumus, kuri prasīti, ievērojot 6. panta 1. un 2. punktu.

4. Pārrobežu kibercentrs ir daudzvalstu platforma, kas izveidota ar rakstisku konsorcija nolīgumu, kā minēts 3. punktā. Tas koordinētā tīkla struktūrā apvieno mitināšanas konsorcija dalībvalstu valsts kibercentrus. Tas ir izveidots, lai palīdzētu uzraudzīt, atklāt un analizēt kiberdraudus, novērst incidentus un atbalstīt kiberdraudu izlūkdatu sagatavošanu, jo īpaši veicot apmaiņu ar nozīmīgiem un attiecīgā gadījumā anonimizētiem datiem un informāciju, kā arī uzticamā vidē daloties ar modernākajiem rīkiem un kopīgi attīstot kiberatklāšanas, analīzes, profilakses un aizsardzības spējas.

5. Juridiskos jautājumos pārrobežu kibercentru pārstāv attiecīgā mitināšanas konsorcija dalībnieks, kas darbojas kā koordinators, vai mitināšanas konsorcijs, ja tas ir juridiska persona. Atbildību par pārrobežu kibercentra atbilstību šai regulai un mitināšanas un izmantošanas nolīgumam nosaka 3. punktā minētajā rakstiskajā konsorcija nolīgumā.

6. Dalībvalsts var pievienoties esošam mitināšanas konsorcijam ar mitināšanas konsorcija dalībnieku piekrišanu. Attiecīgi groza 3. punktā minēto rakstisko konsorcija nolīgumu un mitināšanas un izmantošanas nolīgumu. Tas neietekmē Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra (“*ECCC*”) īpašumtiesības uz rīkiem, infrastruktūru vai pakalpojumiem, kas jau ir kopīgi iepirkti ar minēto mitināšanas konsorciju.

6. pants

Sadarbība un dalīšanās ar informāciju

pārrobežu kibercentru iekšienē un starp tiem

1. Mitināšanas konsorcija dalībnieki nodrošina, ka to valsts kibercentri saskaņā ar 5. panta 3. punktā minēto rakstisko konsorcija nolīgumu pārrobežu kibercentrā savstarpēji dalās ar nozīmīgu un attiecīgā gadījumā anonimizētu informāciju, piemēram, informāciju par kiberdraudiem, gandrīz notikušiem incidentiem, ievainojamībām, metodēm un procedūrām, aizskāruma rādītājiem, apdraudētāju taktiku, specifiskām ziņām par apdraudētājiem, kiberdrošības brīdinājumiem un ieteikumiem par kiberdrošības rīku konfigurāciju kiberuzbrukumu atklāšanai, ja dalīšanās ar šādu informāciju:

   a) veicina un uzlabo kiberdraudu atklāšanu un stiprina *CSIRT* tīkla spējas novērst incidentus un reaģēt uz tiem vai mazināt to ietekmi;

   b) uzlabo kiberdrošības līmeni, piemēram, paplašinot informētību par kiberdraudiem, ierobežojot vai iegrožojot šādu apdraudējumu spēju izplatīties, atbalstot virkni aizsardzības spēju, ievainojamības novēršanu un atklāšanu, apdraudējumu atklāšanas, profilakses un novēršanas metodes, mazināšanas stratēģijas, reaģēšanas un atkopšanās posmus vai veicinot publiskā un privātā sektora vienību sadarbību kiberapdraudējuma izpētē.

2. Rakstiskajā konsorcija nolīgumā, kas minēts 5. panta 3. punktā, nosaka:

a) apņemšanos mitināšanas konsorcija dalībnieku starpā dalīties ar 1. punktā minēto informāciju un nosacījumus, ar kuriem ar minēto informāciju jādalās;

b) pārvaldības sistēmu, kas precizē un stimulē to, ka visi dalībnieki dalās ar nozīmīgu un attiecīgā gadījumā anonimizētu informāciju, kā minēts 1. punktā;

c) mērķrādītājus ieguldījumam tādu progresīvu rīku un tehnoloģiju kā mākslīgais intelekts un datu analīze izstrādē.

Rakstiskajā konsorcija nolīgumā var precizēt, ka dalīšanās ar 1. punktā minēto informāciju notiek saskaņā ar Savienības un valstu tiesību aktiem.

3. Pārrobežu kibercentri cits ar citu noslēdz sadarbības nolīgumus, kuros nosaka sadarbspējas un dalīšanās ar informāciju starp pārrobežu kibercentriem principus. Pārrobežu kibercentri informē Komisiju par noslēgtajiem sadarbības nolīgumiem.

4. Šā panta 1. punktā minēto dalīšanos ar informāciju starp pārrobežu kibercentriem nodrošina augsta līmeņa sadarbspēja. Lai sekmētu šādu sadarbspēju, *ENISA*, cieši apspriežoties ar Komisiju, bez nepamatotas kavēšanās un jebkurā gadījumā līdz ... [12 mēneši pēc šīs regulas spēkā stāšanās dienas] izdod sadarbspējas pamatnostādnes, kurās jo īpaši nosaka dalīšanās ar informāciju formātus un protokolus, ņemot vērā starptautiskos standartus un paraugpraksi, kā arī visu izveidoto pārrobežu kibercentru darbību. Pārrobežu kibercentru sadarbības nolīgumu sadarbspējas prasību pamatā ir *ENISA* izdotās pamatnostādnes.

7. pants

Sadarbība un dalīšanās informācijā ar Savienības līmeņa tīkliem

1. Pārrobežu kibercentri un *CSIRT* tīkls cieši sadarbojas, jo īpaši nolūkā dalīties ar informāciju. Minētajā nolūkā tie vienojas par procesuālo kārtību sadarbībai un attiecīgās informācijas nodošanai, kā arī, neskarot 2. punktu, par to, ar kāda veida informāciju dalīties.

2. Ja pārrobežu kibercentri iegūst informāciju par potenciālu vai notiekošu liela mēroga kiberdrošības incidentu, tie kopīgas situācijas apzināšanās nolūkā bez nepamatotas kavēšanās nodrošina, ka dalībvalstu iestādēm un Komisijai ar *EU-CyCLONe* un *CSIRT* tīkla starpniecību tiek sniegta attiecīgā informācija, kā arī agrīni brīdinājumi.

8. pants

Drošība

1. Dalībvalstis, kuras piedalās Eiropas kiberdrošības trauksmes sistēmā, nodrošina augsta līmeņa kiberdrošību, tostarp konfidencialitāti un datu drošību, kā arī fizisko drošību Eiropas kiberdrošības trauksmes sistēmas tīklā un nodrošina, lai tīkls tiktu pienācīgi pārvaldīts un kontrolēts, sargājot to no apdraudējumiem un nodrošinot tīkla un sistēmu drošību, tostarp to datu un informācijas drošību, ar kuriem tīklā notiek dalīšanās.

2. Dalībvalstis, kas piedalās Eiropas kiberdrošības trauksmes sistēmā, nodrošina, ka 6. panta 1. punktā minēto dalīšanos ar informāciju Eiropas kiberdrošības trauksmes sistēmā ar jebkuru vienību, kas nav dalībvalsts publiska iestāde vai struktūra, negatīvi neietekmē Savienības vai dalībvalstu drošības intereses.

9. pants

Eiropas kiberdrošības trauksmes sistēmas finansējums

1. Pēc uzaicinājuma paust ieinteresētību *ECCC* atlasa dalībvalstis, kas plāno piedalīties Eiropas kiberdrošības trauksmes sistēmā, lai tās ar *ECCC* piedalītos rīku, infrastruktūras un pakalpojumu kopīgā iepirkumā nolūkā izveidot valstu kibercentrus, kas izraudzīti vai izveidoti, kā minēts 4. panta 1. punktā, vai uzlabot esošo centru spējas. *ECCC* var atlasītajām dalībvalstīm piešķirt dotācijas šādu rīku, infrastruktūras vai pakalpojumu darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 50 % rīku, infrastruktūras vai pakalpojumu iegādes izmaksu un līdz 50 % darbības izmaksu. Atlasītās dalībvalsts sedz atlikušās izmaksas. Pirms rīku, infrastruktūras vai pakalpojumu iegādes procedūras uzsākšanas *ECCC* un atlasītās dalībvalstis noslēdz mitināšanas un izmantošanas nolīgumu, kas reglamentē rīku, infrastruktūras vai pakalpojumu izmantošanu.

2. Ja dalībvalsts valsts kibercentrs nav pārrobežu kibercentra dalībnieks 2 gadu laikā no dienas, kad ir iegādāti rīki, infrastruktūra vai pakalpojumi, vai kad tas saņēmis dotāciju finansējumu, atkarībā no tā, kas ir agrāk, dalībvalsts nav tiesīga saņemt Savienības papildu atbalstu atbilstīgi šai nodaļai, kamēr tā nav pievienojusies pārrobežu kibercentram.

3. Pēc uzaicinājuma paust ieinteresētību *ECCC* izraugās mitināšanas konsorciju dalībai ar *ECCC* kopīgā rīku, infrastruktūras vai pakalpojumu iepirkumā. *ECCC* var mitināšanas konsorcijam piešķirt dotāciju rīku, infrastruktūras vai pakalpojumu darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 75 % rīku, infrastruktūras vai pakalpojumu iegādes izmaksu un līdz 50 % darbības izmaksu. Mitināšanas konsorcijs sedz atlikušās izmaksas. Pirms rīku, infrastruktūras vai pakalpojumu iegādes procedūras uzsākšanas *ECCC* un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas nolīgumu, kas reglamentē rīku, infrastruktūras vai pakalpojumu izmantošanu.

4. *ECCC* vismaz reizi divos gados sagatavo to rīku, infrastruktūras vai pakalpojumu kartējumu, kas vajadzīgi un ir pietiekamas kvalitātes, lai izveidotu vai uzlabotu valstu kibercentru un pārrobežu kibercentru spējas un pieejamību, tostarp juridiskām personām, kuras iedibinātas vai tiek uzskatītas par iedibinātām dalībvalstīs un kuras kontrolē dalībvalstis vai dalībvalstu valstspiederīgie. Sagatavojot kartējumu, *ECCC* apspriežas ar *CSIRT* tīklu, visiem esošajiem pārrobežu kibercentriem, *ENISA* un Komisiju.

III nodaļa
Kiberdrošības ārkārtas mehānisms

10. pants

Kiberdrošības ārkārtas mehānisma izveide

1. Lai palīdzētu uzlabot Savienības noturību pret kiberdraudiem un solidaritātes garā sagatavotos būtisku kiberdrošības incidentu, liela mēroga kiberdrošības incidentu un lielam mērogam līdzvērtīgu kiberdrošības incidentu īslaicīgai ietekmei un to mazinātu, tiek izveidots kiberdrošības ārkārtas mehānisms.

2. Dalībvalstu gadījumā darbības, kas paredzētas kiberdrošības ārkārtas mehānismā, nodrošina pēc pieprasījuma, un tās papildina dalībvalstu centienus un darbības, kuru mērķis ir sagatavoties kiberdrošības incidentiem, reaģēt uz tiem un atkopties pēc tiem.

3. Darbības, ar kurām īsteno Eiropas kiberdrošības ārkārtas mehānismu, atbalsta no programmas *PDE* finansējuma un īsteno saskaņā ar Regulu (ES) 2021/694, jo īpaši tās konkrēto mērķi Nr. 3.

4. Darbības kiberdrošības ārkārtas mehānismā galvenokārt īsteno, izmantojot *ECCC* saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/887. Tomēr darbības, ar kurām īsteno ES kiberdrošības rezerves, kā minēts šīs regulas 11. panta b) apakšpunktā, īsteno Komisija un *ENISA*.

11. pants

Darbību veidi

Kiberdrošības ārkārtas mehānisms atbalsta šādus darbību veidus:

a) gatavības darbības, proti:

i) koordinētu gatavības testēšanu vienībām, kas darbojas sevišķi kritiskajās nozarēs visā Savienībā, kā precizēts 12. pantā;

ii) citas gatavības darbības vienībām, kas darbojas sevišķi kritiskajās nozarēs, vai vienībām, kas darbojas citās kritiskajās nozarēs, kā precizēts 13. pantā;

b) darbības, kas atbalsta reaģēšanu uz būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem un lielam mērogam līdzvērtīgiem kiberdrošības incidentiem un atkopšanās pēc tiem uzsākšanu un kas jāveic uzticamiem pārvaldītu drošības pakalpojumu sniedzējiem, kuri piedalās ES kiberdrošības rezervēs, kas izveidotas atbilstīgi 14. pantam;

c) darbības, kas atbalsta savstarpēju palīdzību, kā minēts 18. pantā.

12. pants

Koordinēta vienību gatavības testēšana

1. Kiberdrošības ārkārtas mehānisms atbalsta brīvprātīgu un koordinētu tādu vienību gatavības testēšanu, kuras darbojas sevišķi kritiskajās nozarēs.

2. Koordinētās gatavības testēšana var ietvert gatavības darbības, piemēram, ielaušanās testēšanu, un apdraudējuma novērtēšanu.

3. Atbalstu gatavības darbībām atbilstīgi šim pantam dalībvalstīm sniedz galvenokārt dotāciju veidā un saskaņā ar nosacījumiem, kas paredzēti attiecīgajās darba programmās, kā minēts Regulas (ES) 2021/694 24. pantā.

4. Lai visā Savienībā atbalstītu šīs regulas 11. panta a) apakšpunkta i) punktā minēto vienību koordinētu gatavības testēšanu, Komisija pēc apspriešanās ar TID sadarbības grupu, *EU-CyCLONe* un *ENISA* nosaka attiecīgās nozares vai apakšnozares no Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajām sevišķi kritiskajām nozarēm, kurām var izsludināt uzaicinājumus iesniegt priekšlikumus dotāciju piešķiršanai. Dalībvalstu piedalīšanās minētajos uzaicinājumos iesniegt priekšlikumus ir brīvprātīga.

5. Apzinot nozares vai apakšnozares, kas minētas 4. punktā, Komisija ņem vērā koordinētus riska novērtējumus un noturības testēšanu Savienības līmenī, kā arī to rezultātus.

6. TID sadarbības grupa sadarbībā ar Komisiju, Savienības Augsto pārstāvi ārlietās un drošības politikas jautājumos (“Augstais pārstāvis”) un *ENISA*, kā arī *EU-CyCLONe* atbilstoši tā pilnvarām izstrādā kopīgus riska scenārijus un metodiku koordinētai gatavības testēšanai, kas minēta 11. panta a) apakšpunkta i) punktā, un attiecīgā gadījumā citām gatavības darbībām, kas minētas minētā panta a) apakšpunkta ii) punktā.

7. Ja vienība, kas darbojas sevišķi kritiskā nozarē, brīvprātīgi piedalās koordinētā gatavības testēšanā un minētās testēšanas rezultātā tiek izstrādāti ieteikumi veikt konkrētus pasākumus, kurus iesaistītā vienība varētu integrēt sanācijas plānā, par koordinētās gatavības testēšanu atbildīgā dalībvalsts iestāde attiecīgā gadījumā izvērtē iesaistīto vienību veikto pasākumu pēcpārbaudi nolūkā stiprināt gatavību.

13. pants

Citas gatavības darbības

1. Kiberdrošības ārkārtas mehānisms atbalsta arī gatavības darbības, uz kurām neattiecas 12. pants. Šādas darbības ietver gatavības darbības vienībām nozarēs, kas nav identificētas koordinētajai gatavības testēšanai, ievērojot 12. pantu. Šādas darbības var atbalstīt ievainojamības uzraudzību, riska uzraudzību, mācības un apmācību.

2. Atbalstu gatavības darbībām atbilstīgi šim pantam dalībvalstīm sniedz pēc pieprasījuma un galvenokārt dotāciju veidā un saskaņā ar nosacījumiem, kas paredzēti attiecīgajās darba programmās, kā minēts Regulas (ES) 2021/694 24. pantā.

14. pants

ES kiberdrošības rezervju izveide

1. Lai pēc pieprasījuma palīdzētu 3. punktā minētajiem lietotājiem reaģēt vai atbalstītu reaģēšanu uz būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem, kā arī atkopšanās uzsākšanu pēc šādiem incidentiem, tiek izveidotas ES kiberdrošības rezerves.

2. ES kiberdrošības rezerves veido reaģēšanas pakalpojumi, ko sniedz uzticami pārvaldītu drošības pakalpojumu sniedzēji, kas atlasīti saskaņā ar 17. panta 2. punktā noteiktajiem kritērijiem. ES kiberdrošības rezerves var ietvert pakalpojumus, par kuriem iepriekš uzņemtas saistības. Uzticama pārvaldītu drošības pakalpojumu sniedzēja pakalpojumi, par kuriem iepriekš uzņemtas saistības, gadījumos, kad minētie pakalpojumi, par kuriem iepriekš uzņemtas saistības, nav izmantoti reaģēšanai uz incidentiem laikposmā, attiecībā uz kuru par minētajiem pakalpojumiem ir iepriekš uzņemtas saistības, ir pārveidojami par gatavības pakalpojumiem saistībā ar incidentu novēršanu un reaģēšanu uz tiem. ES kiberdrošības rezerves pēc pieprasījuma ir izmantojamas visās dalībvalstīs, Savienības iestādēs, struktūrās, birojos un aģentūrās un *PDE* asociētajās trešās valstīs, kā minēts 19. panta 1. punktā.

3. ES kiberdrošības rezervju sniegto pakalpojumu lietotāji ir:

a) dalībvalstu kiberkrīžu pārvaldības iestādes un *CSIRT*, kā minēts attiecīgi Direktīvas (ES) 2022/2555 9. panta 1. un 2. punktā un 10. pantā;

b) *CERT*-EU saskaņā ar Regulas (ES, *Euratom*) 2023/2841 13. pantu;

c) kompetentās iestādes, piemēram, *PDE* asociēto trešo valstu datordrošības incidentu reaģēšanas vienības un kiberkrīžu pārvaldības iestādes saskaņā ar 19. panta 8. punktu.

4. Komisijai ir vispārēja atbildība par ES kiberdrošības rezervju īstenošanu. Komisija sadarbībā ar TID koordinācijas grupu un atbilstīgi 3. punktā minēto lietotāju prasībām nosaka ES kiberdrošības rezervju prioritātes un attīstību un uzrauga to īstenošanu, kā arī nodrošina savstarpēju papildināmību, konsekvenci, sinerģiju un saikni ar citām atbalsta darbībām saskaņā ar šo regulu, kā arī citām Savienības darbībām un programmām. Minētās prioritātes pārskata un, ja vajadzīgs, pielāgo reizi divos gados. Komisija informē Eiropas Parlamentu un Padomi par minētajām prioritātēm un to pielāgojumiem.

5. Neskarot Komisijas vispārējo atbildību par šā panta 4. punktā minēto ES kiberdrošības rezervju īstenošanu un ievērojot iemaksu nolīgumu, kā definēts Regulas (ES, *Euratom*) 2024/2509 2. panta 18. punktā, Komisija ES kiberdrošības rezervju darbības nodrošināšanu un pārvaldību pilnībā vai daļēji uztic *ENISA*. Aspektus, kas nav uzticēti *ENISA*, turpina tieši pārvaldīt Komisija.

6. *ENISA* vismaz reizi divos gados sagatavo to pakalpojumu kartējumu, kas vajadzīgi šā panta 3. punkta a) un b) apakšpunktā minētajiem lietotājiem. Kartējumā iekļauj arī šādu pakalpojumu pieejamību, tostarp no tiesību subjektiem, kas iedibināti vai ko uzskata par iedibinātiem dalībvalstīs un ko kontrolē dalībvalstis vai dalībvalstu valstspiederīgie. Kartējot minēto pieejamību, *ENISA* novērtē Savienības kiberdrošības darbaspēka prasmes un spējas saistībā ar ES kiberdrošības rezervju mērķiem. Sagatavojot kartēšanu, *ENISA* apspriežas ar TID sadarbības grupu, *EU-CyCLONe*, Komisiju un attiecīgā gadījumā Iestāžu kiberdrošības padomi, kas izveidota, ievērojot Regulas (ES, *Euratom*) 2023/2841 10. pantu (IICB). Kartējot pakalpojumu pieejamību, *ENISA* apspriežas arī ar attiecīgajām kiberdrošības nozares ieinteresētajām personām, tostarp pārvaldītiem drošības pakalpojumu sniedzējiem. *ENISA* pēc tam, kad tā ir informējusi Padomi un apspriedusies ar *EU-CyCLONe* un Komisiju, kā arī attiecīgā gadījumā Augsto pārstāvi, sagatavo līdzīgu kartējumu, lai identificētu šā panta 3. punkta c) apakšpunktā minēto lietotāju vajadzības.

7. Komisija tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 23. pantu, lai papildinātu šo regulu, precizējot ES kiberdrošības rezervēm nepieciešamo reaģēšanas pakalpojumu veidus un skaitu. Sagatavojot minētos deleģētos aktus, Komisija ņem vērā šā panta 6. punktā minēto kartēšanu un var apmainīties ieteikumiem un sadarboties ar TID sadarbības grupu un *ENISA*.

15. pants

ES kiberdrošības rezervju atbalsta pieprasījumi

1. Šīs regulas 14. panta 3. punktā minētie lietotāji var pieprasīt pakalpojumus no ES kiberdrošības rezervēm, lai atbalstītu reaģēšanu uz būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem un uzsāktu atkopšanos no tiem.

2. Lai saņemtu atbalstu no ES kiberdrošības rezervēm, 14. panta 3. punktā minētie lietotāji veic visus atbilstošos pasākumus, kas mazina tā incidenta sekas, par kuru tiek pieprasīts atbalsts, tostarp attiecīgā gadījumā tiešas tehniskās palīdzības un citu resursu sniegšanu, lai palīdzētu reaģēt uz incidentu, un atkopšanās pasākumus.

3. Atbalsta pieprasījumus līgumslēdzējai iestādei nosūta šādā veidā:

   a) šīs regulas 14. panta 3. punkta a) apakšpunktā minēto lietotāju gadījumā -izmantojot vienoto kontaktpunktu, kas norīkots vai izveidots, ievērojot Direktīvas (ES) 2022/2555 8. panta 3. punktu.

b) šīs regulas 14. panta 3. punkta b) apakšpunktā minēto lietotāju gadījumā - pieprasījumus nosūta minētais lietotājs;

c) šīs regulas 14. panta 3. punkta c) apakšpunktā - izmantojot šīs regulas 19. panta 9. punktā minēto vienoto kontaktpunktu.

4. Šīs regulas 14. panta 3. punkta a) apakšpunktā minēto lietotāju pieprasījumu gadījumā dalībvalstis informē *CSIRT* tīklu un attiecīgā gadījumā *EU-CyCLONe* par savu lietotāju saskaņā ar šo pantu iesniegtajiem pieprasījumiem reaģēt uz incidentu un atbalstīt sākotnējo atkopšanos.

5. Pieprasījumā reaģēt uz incidentu un atbalstīt sākotnējo atkopšanos ietver:

a) atbilstošu informāciju par skarto vienību un incidenta iespējamo ietekmi uz:

i) šīs regulas 14. panta 3. punkta a) apakšpunktā minēto lietotāju gadījumā - skartās dalībvalstis un lietotājus, tostarp risku, ka tas varētu izplatīties uz citu dalībvalsti;

ii) šīs regulas 14. panta 3. punkta b) apakšpunktā minēto lietotāju gadījumā - skartajām Savienības iestādēm, struktūrām, birojiem un aģentūrām;

iii) šīs regulas 14. panta 3. punkta c) apakšpunktā minēto lietotāju gadījumā - skartajām *PDE* asociētajām valstīm;

b) informāciju par pieprasīto pakalpojumu, kopā ar pieprasītā atbalsta plānoto izmantošanu, tostarp norādi par aplēstajām vajadzībām;

c) atbilstošu informāciju par pasākumiem, kas veikti, lai mazinātu incidentu, par kuru tiek pieprasīts atbalsts, kā minēts 2. punktā;

d) attiecīgā gadījumā pieejamo informāciju par citu veidu atbalstu, kas pieejams skartajai vienībai.

6. *ENISA* sadarbībā ar Komisiju un *EU-CyCLONe* izstrādā veidni, lai vienkāršotu ES kiberdrošības rezervju atbalsta pieprasījumu iesniegšanu.

7. Komisija ar īstenošanas aktiem var sīkāk precizēt detalizētu procesuālo kārtību tam, kā ES kiberdrošības rezervju atbalsta pakalpojumi tiek pieprasīti un kā uz minētajiem pieprasījumiem tiek atbildēts, ievērojot šo pantu, 16. panta 1. punktu un 19. panta 10. punktu, tostarp šādu pieprasījumu iesniegšanai un atbilžu sniegšanai, un 16. panta 9. punktā minēto ziņojumu veidnes. Minētos īstenošanas aktus pieņem saskaņā ar pārbaudes procedūru, kas minēta 24. panta 2. punktā.

16. pants

ES kiberdrošības rezervju atbalsta īstenošana

1. Šīs regulas 14. panta 3. punkta a) un b) apakšpunktā minēto lietotāju pieprasījumu gadījumā ES kiberdrošības rezervju atbalsta pieprasījumus izvērtē līgumslēdzēja iestāde. Atbildi 14. panta 3. punkta a) un b) apakšpunktā minētajiem lietotājiem nosūta nekavējoties un jebkurā gadījumā ne vēlāk kā 48 stundu laikā pēc pieprasījuma iesniegšanas, lai nodrošinātu atbalsta efektivitāti. Līgumslēdzēja iestāde informē Padomi un Komisiju par procesa rezultātiem.

2. Attiecībā uz informāciju, kuru nodod, pieprasot un sniedzot ES kiberdrošības rezervju pakalpojumus, visas šīs regulas piemērošanā iesaistītās personas:

   a) ierobežo minētās informācijas izmantošanu un dalīšanos ar to tādā apmērā, kāds nepieciešams tām šajā regulā noteikto pienākumu vai funkciju izpildei;

   b) jebkuru informāciju, kas ir konfidenciāla vai klasificēta saskaņā ar Savienības un valstu tiesību aktiem, izmanto un ar to dalās tikai saskaņā ar minētajiem tiesību aktiem; un

   c) nodrošina efektīvu, lietderīgu un drošu dalīšanos ar informāciju, attiecīgā gadījumā izmantojot un ievērojot attiecīgos informācijas dalīšanās protokolus, tostarp gaismas signālu protokolu.

3. Izvērtējot atsevišķus pieprasījumus saskaņā ar 16. panta 1. punktu un 19. panta 10. punktu, attiecīgi līgumslēdzēja iestāde vai Komisija vispirms novērtē, vai ir izpildīti 15. panta 1. un 2. punktā minētie kritēriji. Ja tie ir izpildīti, tās novērtē, kāds atbalsta ilgums un veids būtu piemērots, ņemot vērā 1. panta 3. punkta b) apakšpunktā minēto mērķi un attiecīgā gadījumā šādus kritērijus:

a) incidenta apmērs un smagums;

b) skartās vienības veids, augstāku prioritāti piešķirot incidentiem, kuri skar būtiskās vienības, kā minēts Direktīvas (ES) 2022/2555 3. panta 1. punktā;

c) iespējamā ietekme uz skartajām dalībvalstīm, Savienības iestādēm, struktūrām, birojiem vai aģentūrām, vai *PDE* asociētajām trešām valstīm;

d) incidenta iespējamā pārrobežu ietekme un risks, ka tas var izplatīties citās dalībvalstīs, Savienības iestādēs, struktūrās, birojos vai aģentūrās, vai *PDE* asociētajās trešās valstīs;

e) pasākumi, ko lietotājs veicis, lai palīdzētu reaģēt, un sākotnējas atkopšanās pasākumi, kā minēts 15. panta 2. punktā.

4. Ja 14. panta 3. punktā minētie lietotāji iesniedz pieprasījumus vienlaicīgi, to prioritāti nosaka, attiecīgā gadījumā ņemot vērā šā panta 3. punktā minētos kritērijus, neskarot lojālas sadarbības principu starp dalībvalstīm un Savienības iestādēm, struktūrām, birojiem un aģentūrām. Ja divi vai vairāki pieprasījumi tiek novērtēti kā vienādi atbilstīgi minētajiem kritērijiem, augstāku prioritāti piešķir dalībvalstu lietotāju pieprasījumiem. Ja ES kiberdrošības rezervju darbības nodrošināšana un pārvaldība ir pilnībā vai daļēji uzticēta *ENISA*, ievērojot 14. panta 5. punktu, *ENISA* un Komisija cieši sadarbojas, lai piešķirtu prioritāti pieprasījumiem saskaņā ar šo punktu.

5. ES kiberdrošības rezervju pakalpojumus sniedz saskaņā ar īpašiem nolīgumiem starp uzticamu pārvaldītu drošības pakalpojumu sniedzēju un lietotāju, kuram tiek sniegts atbalsts no ES kiberdrošības rezervēm. Minētos pakalpojumus var sniegt saskaņā ar īpašiem nolīgumiem starp uzticamo pārvaldītu drošības pakalpojumu sniedzēju, lietotāju un skarto vienību. Visi šajā punktā minētie nolīgumi cita starpā ietver atbildības nosacījumus.

6. Šā panta 5. punktā minēto nolīgumu pamatā ir veidnes, ko *ENISA* sagatavojusi pēc apspriešanās ar dalībvalstīm un attiecīgā gadījumā citiem ES kiberdrošības rezervju lietotājiem.

7. Komisija, *ENISA* un ES kiberdrošības rezervju lietotāji neuzņemas līgumisku atbildību par kaitējumu, ko trešām personām nodarījuši pakalpojumi, kuri sniegti ES kiberdrošības rezervju īstenošanā.

8. Lietotāji var izmantot ES kiberdrošības rezervju pakalpojumus, ko sniedz saistībā ar 15. panta 1. punktā minētu pieprasījumu, tikai nolūkā atbalstīt reaģēšanu uz būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem un lai uzsāktu atkopšanos pēc tiem. Tie var izmantot šos pakalpojumus tikai attiecībā uz:

   a) vienībām, kas darbojas sevišķi kritiskajās nozarēs, vai vienībām, kas darbojas citās kritiskajās nozarēs, – attiecībā uz 14. panta 3. punkta a) apakšpunktā minētajiem lietotājiem, un līdzvērtīgām vienībām – attiecībā uz 14. panta 3. punkta c) apakšpunktā minētajiem lietotājiem, un

   b) Savienības iestādēm, struktūrām, birojiem un aģentūrām – attiecībā uz 14. panta 3. punkta b) apakšpunktā minēto lietotāju.

9. Lietotāji, kas saņēmuši atbalstu, divu mēnešu laikā pēc atbalsta darbības beigām par sniegto pakalpojumu, sasniegtajiem rezultātiem un gūtajām atziņām iesniedz kopsavilkuma ziņojumu:

   a) Komisijai, *ENISA*, *CSIRT* tīklam un *EU-CyCLONe* - šīs regulas 14. panta 3. punkta a) apakšpunktā minēto lietotāju gadījumā;

   b) Komisijai, *ENISA* un Iestāžu kiberdrošības padomei - šīs regulas 14. panta 3. punkta b) apakšpunktā minētā lietotāja gadījumā;

c) Komisijai šīs regulas 14. panta 3. punkta c) apakšpunktā minēto lietotāju gadījumā.

Komisija, ievērojot šā punkta pirmās daļas c) apakšpunktu, nosūta no 14. panta 3. punktā minētajiem lietotājiem saņemto ziņojumu kopsavilkumu Padomei un Augstajam pārstāvim.

10. Ja ES kiberdrošības rezervju darbības nodrošināšana un pārvaldība ir pilnībā vai daļēji uzticēta *ENISA*, ievērojot šīs regulas 14. panta 5. punktu, *ENISA* par to regulāri ziņo Komisijai un apspriežas ar to minētajā sakarā. Minētajā sakarībā *ENISA* nekavējoties nosūta Komisijai visus pieprasījumus, ko tā saņem no šīs regulas 14. panta 3. punkta c) apakšpunktā minētajiem lietotājiem, un, ja tas nepieciešams prioritāšu noteikšanai saskaņā ar šo pantu, visus pieprasījumus, ko tā saņēmusi no šīs regulas 14. panta 3. punkta a) vai b) apakšpunktā minētajiem lietotājiem. Šajā punktā noteiktie pienākumi neskar Regulas (ES) 2019/881 14. pantu.

11. Attiecībā uz 14. panta 3. punkta a) un b) apakšpunktā minētajiem lietotājiem līgumslēdzēja iestāde regulāri un vismaz divas reizes gadā ziņo TID sadarbības grupai par atbalsta izmantošanu un rezultātiem.

12. Attiecībā uz 14. panta 3. punkta c) apakšpunktā minētajiem lietotājiem Komisija regulāri un vismaz divas reizes gadā ziņo Padomei un informē Augsto pārstāvi par atbalsta izmantošanu un rezultātiem.

17. pants

Uzticami pārvaldīti drošības pakalpojumu sniedzēji

1. Iepirkuma procedūrās ES kiberdrošības rezervju izveidei līgumslēdzēja iestāde rīkojas saskaņā ar Regulā (ES, *Euratom*) 2024/2509 noteiktajiem principiem un saskaņā ar šādiem principiem:

   a) nodrošināt, ka kopējās ES kiberdrošības rezervēs iekļautie pakalpojumi garantē, ka ES kiberdrošības rezervēs ir pakalpojumi, kurus var ieviest visās dalībvalstīs, jo īpaši ņemot vērā valsts prasības attiecībā uz šādu pakalpojumu sniegšanu, tostarp par valodām, sertifikāciju vai akreditāciju;

   b) nodrošināt Savienības un tās dalībvalstu būtisko drošības interešu aizsardzību;

   c) nodrošināt, ka ES kiberdrošības rezerves rada Savienības pievienoto vērtību, sekmējot Regulas (ES) 2021/694 3. panta mērķu sasniegšanu un cita starpā veicinot kiberdrošības prasmju attīstību Savienībā.

2. Iepērkot pakalpojumus ES kiberdrošības rezervēm, līgumslēdzēja iestāde iepirkuma procedūras dokumentos iekļauj šādus atlases kritērijus un prasības:

a) pakalpojumu sniedzējs pierāda, ka tā personālam ir pati augstākā profesionālā godprātība, neatkarība, atbildība un tehniskā kompetence, kas vajadzīga darbībai savā specifiskajā jomā, un nodrošina lietpratības pastāvību un nepārtrauktību, kā arī vajadzīgos tehniskos resursus;

b) pakalpojumu sniedzējs un jebkuri attiecīgie meitasuzņēmumi un apakšuzņēmēji ievēro piemērojamos noteikumus par klasificētas informācijas aizsardzību un ievieš atbilstīgus pasākumus, tostarp attiecīgā gadījumā savstarpējus nolīgumus, lai aizsargātu konfidenciālu informāciju, kas saistīta ar pakalpojumu, un jo īpaši pierādījumus, konstatējumus un ziņojumus;

c) pakalpojumu sniedzējs sniedz pietiekamus pierādījumus, ka tā pārvaldes struktūra ir pārredzama, nevar apdraudēt tā objektivitāti un pakalpojumu kvalitāti vai radīt interešu konfliktu;

d) pakalpojumu sniedzējam ir attiecīga drošības pielaide – vismaz personālam, kas paredzēts pakalpojumu ieviešanai, – ja to prasa dalībvalsts;

e) pakalpojumu sniedzējam ir attiecīgs drošības līmenis tā IT sistēmām;

f) pakalpojumu sniedzējs ir aprīkots ar pieprasītā pakalpojuma atbalstīšanai nepieciešamo aparatūru un programmatūru, kas nesatur zināmas ļaunprātīgi izmantojamas ievainojamības, ietver jaunākos drošības atjauninājumus un jebkurā gadījumā atbilst visiem piemērojamajiem Eiropas Parlamenta un Padomes Regulas (ES) 2024/...[23+] noteikumiem;

g) pakalpojumu sniedzējs spēj pierādīt, ka tam ir pieredze līdzīgu pakalpojumu sniegšanā attiecīgām valsts iestādēm, vienībām, kas darbojas sevišķi kritiskajās nozarēs, vai vienībām, kas darbojas citās kritiskajās nozarēs;

h) pakalpojumu sniedzējs dalībvalstīs, kurās tas var sniegt pakalpojumu, spēj to sniegt īsā laikā;

i) pakalpojumu sniedzējs dalībvalstīs, kurās tas var sniegt pakalpojumu, spēj to sniegt vienā vai vairākās Savienības iestāžu vai dalībvalsts oficiālajās valodās, kā to, iespējams, prasa dalībvalstis vai 14. panta 3. punkta b) un c) apakšpunktā minētie lietotāji;

j) kad ir ieviesta Eiropas kiberdrošības sertifikācijas shēma pārvaldītiem drošības pakalpojumiem, ievērojot Regulu (ES) 2019/881, pakalpojumu sniedzējs tiek sertificēts saskaņā ar minēto shēmu divu gadu laikā pēc minētās shēmas piemērošanas dienas;

---

23 Eiropas Parlamenta un Padomes Regula (ES) 2024/... (… gada …) par ... (OV L ..., ELI: ...).

+ OV: lūgums tekstā ievietot dokumentā PE-CONS 100/23 (2022/0272(COD)) ietvertās regulas numuru un zemsvītras piezīmē ievietot minētās regulas numuru, datumu, nosaukumu, OV atsauci un ELI atsauci.

k) pakalpojumu sniedzējs piedāvājumā iekļauj pārveides nosacījumus jebkuram neizmantotam reaģēšanas uz incidentiem pakalpojumam, ko varētu pārveidot par gatavības pakalpojumiem, kuri ir cieši saistīti ar reaģēšanu uz incidentiem, piemēram, mācībām vai apmācību.

3. Nolūkā iepirkt pakalpojumus ES kiberdrošības rezervēm līgumslēdzēja iestāde, cieši sadarbojoties ar dalībvalstīm, attiecīgā gadījumā var izstrādāt kritērijus un prasības papildus 2. punktā minētajiem.

18. pants

Darbības savstarpējas palīdzības atbalstam

1. Kiberdrošības ārkārtas mehānisms atbalsta tehnisko palīdzību, ko kāda dalībvalsts sniedz citai dalībvalstij, kuru skāris būtisks kiberdrošības incidents vai liela mēroga kiberdrošības incidents, tostarp gadījumos, kas minēti Direktīvas (ES) 2022/2555 11. panta 3. punkta f) apakšpunktā.

2. Atbalstu šā panta 1. punktā minētajai savstarpējai tehniskajai palīdzībai sniedz dotāciju veidā, ievērojot nosacījumus, kas paredzēti attiecīgajās darba programmās, kā minēts Regulas (ES) 2021/694 24. 24. pantā.

19. pants

Atbalsts PDE asociētajām trešām valstīm

1. *PDE* asociētā trešā valsts var pieprasīt ES kiberdrošības rezervju atbalstu, ja nolīgums, ar ko nosaka tās asociāciju ar *PDE*, paredz dalību ES kiberdrošības rezervēs. Minētajā nolīgumā iekļauj noteikumus, kas paredz, ka *PDE* asociētajai trešai valstij ir jāpilda šā panta 2. un 9. punktā noteiktie pienākumi. Lai trešā valsts varētu piedalīties ES kiberdrošības rezervēs, trešās valsts daļējā asociācija ar *PDE* var iekļaut asociāciju, kas paredz tikai Regulas (ES) 2021/694 6. panta 1. punkta g) apakšpunktā minēto darbības mērķi.

2. Trīs mēnešu laikā pēc 1. punktā minētā nolīguma noslēgšanas un jebkurā gadījumā pirms atbalsta saņemšanas no ES kiberdrošības rezervēm *PDE* asociētās trešā valsts sniedz Komisijai informāciju par savu kibernoturību un riska pārvaldības spējām, tostarp vismaz informāciju par valsts mēroga pasākumiem, kas veikti, lai sagatavotos būtiskiem kiberdrošības incidentiem, liela mēroga kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem, kā arī informāciju par atbildīgajām valsts vienībām, tostarp *CSIRT* vai līdzvērtīgām vienībām, to spējām un tām piešķirtajiem resursiem. *PDE* asociētā trešā valsts regulāri un vismaz reizi gadā sniedz minētās informācijas atjauninājumus. Komisija sniedz minēto informāciju Augstajam pārstāvim un *ENISA* nolūkā veicināt 11. punkta piemērošanu.

3. Komisija regulāri un vismaz reizi gadā attiecībā uz katru no 1. punktā minētajām *PDE* asociētajām trešām valstīm novērtē šādus kritērijus:

a) vai minētā valsts ievēro 1. punktā minētā nolīguma noteikumus, ciktāl minētie noteikumi attiecas uz dalību ES kiberdrošības rezervēs;

b) vai minētā valsts ir veikusi atbilstīgus pasākumus, lai sagatavotos būtiskiem kiberdrošības incidentiem vai lielam mērogam līdzvērtīgiem kiberdrošības incidentiem, pamatojoties uz 2. punktā minēto informāciju; un

c) vai atbalsta sniegšana atbilst Savienības politikai attiecībā uz minēto valsti un vispārējām attiecībām ar to un vai tā atbilst citiem Savienības politikas virzieniem drošības jomā.

Komisija, veicot pirmajā daļā minēto novērtējumu, apspriežas ar Augsto pārstāvi attiecībā uz minētās daļas c) apakšpunktā minēto kritēriju.

Ja Komisija secina, ka *PDE* asociētā trešā valsts atbilst visiem pirmajā daļā minētajiem nosacījumiem, Komisija iesniedz priekšlikumu Padomei pieņemt īstenošanas aktu saskaņā ar 4. punktu, ar ko atļauj sniegt minētajai valstij atbalstu no ES kiberdrošības rezervēm.

4. Padome var pieņemt 3. punktā minētos īstenošanas aktus. Minētos īstenošanas aktus piemēro ilgākais vienu gadu. Tos var atjaunot. Tie var ietvert tādu ierobežojumu attiecībā uz to dienu skaitu, par kurām var sniegt atbalstu, atbildot uz vienu pieprasījumu, kas ilgst ne mazāk kā 75 dienas.

Šā panta nolūkos Padome rīkojas ātri un šajā punktā minētos īstenošanas aktus parasti pieņem astoņu nedēļu laikā pēc tam, kad pieņemts attiecīgais Komisijas priekšlikums, ievērojot 3. punkta trešo daļu.

5. Padome pēc Komisijas priekšlikuma jebkurā laikā var grozīt vai atcelt īstenošanas aktu, kas pieņemts, ievērojot 4. punktu.

Ja Padome uzskata, ka attiecībā uz 3. punkta pirmās daļas c) apakšpunktā minēto kritēriju ir notikušas būtiskas izmaiņas, Padome pēc vienas vai vairāku dalībvalstu pienācīgi motivētas iniciatīvas var grozīt vai atcelt īstenošanas aktu, kas pieņemts, ievērojot 4. punktu.

6. Īstenojot savas īstenošanas pilnvaras atbilstīgi šim pantam, Padome piemēro 3. punkta pirmajā daļā minētos kritērijus un paskaidro, kā tā ir novērtējusi minētos kritērijus. Jo īpaši tad, ja Padome rīkojas pēc savas iniciatīvas, ievērojot 5. punkta otro daļu, tā paskaidro minētajā daļā minētās būtiskās izmaiņas.

7. Atbalsts no ES kiberdrošības rezervēm *PDE* asociētai trešai valstij atbilst 1. punktā minētā nolīguma īpašajiem nosacījumiem.

8. Lietotāji no *PDE* asociētajām trešām valstīm, kam ir tiesības saņemt pakalpojumus no ES kiberdrošības rezervēm, ietver kompetentās iestādes, piemēram, datordrošības incidentu reaģēšanas vienības vai līdzvērtīgas vienības un kiberkrīzes pārvaldības iestādes.

9. Katra *PDE* asociētā trešā valsts, kas tiesīga prasīt atbalstu no ES kiberdrošības rezervēm, norīko iestādi, kura darbojas kā vienots kontaktpunkts šīs regulas nolūkiem.

10. Pieprasījumus saņemt atbalstu no ES kiberdrošības rezervēm atbilstīgi šim punktam izvērtē Komisija. Līgumslēdzēja iestāde var sniegt atbalstu trešai valstij tikai tad, ja ir spēkā ievērojot šā panta 4. pantu pieņemts Padomes īstenošanas akts, ar ko atļauj šādu atbalstu attiecībā uz minēto valsti, un tikai tik ilgi, kamēr tas ir spēkā. Atbildi bez nepamatotas kavēšanās nosūta 14. panta 3. punkta c) apakšpunktā minētajiem lietotājiem.

11. Pēc atbalsta pieprasījuma saņemšanas atbilstīgi šim pantam Komisija nekavējoties informē Padomi. Komisija pastāvīgi informē Padomi par pieprasījuma novērtējumu. Komisija arī sadarbojas ar Augsto pārstāvi attiecībā uz saņemtajiem pieprasījumiem un no ES kiberdrošības rezervēm *PDE* asociētajām trešām valstīm piešķirtā atbalsta īstenošanu. Turklāt Komisija ņem vērā arī *ENISA* sniegto viedokli par minētajiem pieprasījumiem.

20. pants

Koordinācija ar Savienības krīžu pārvaldības mehānismiem

1. Ja būtiska kiberdrošības incidenta, liela mēroga kiberdrošības incidenta vai lielam mērogam līdzvērtīga kiberdrošības incidenta cēlonis vai sekas ir katastrofa, kā definēts Lēmuma Nr. 1313/2013/ES 4. panta 1. punktā, šajā regulā paredzētais atbalsts reaģēšanai uz šādu incidentu papildina minētajā lēmumā paredzētās darbības, to neskarot.

2. Liela mēroga kiberdrošības incidenta vai lielam mērogam līdzvērtīga kiberdrošības incidenta gadījumā, kad tiek aktivizēti Īstenošanas lēmumā (ES) 2018/1993 paredzētie ES integrētie krīzes situāciju politiskās reaģēšanas mehānismi (*IPCR* mehānismi), šajā regulā paredzēto atbalstu reaģēšanai uz šādu incidentu sniedz saskaņā ar attiecīgajām *IPCR* mehānismos noteiktajām procedūrām.

IV nodaļa

Eiropas kiberdrošības incidentu izskatīšanas mehānisms

21. pants

Eiropas Kiberdrošības incidentu izskatīšanas mehānisms

1. Pēc Komisijas vai *EU-CyCLONe* pieprasījuma *ENISA* ar *CSIRT* tīkla atbalstu un attiecīgo dalībvalstu piekrišanu izskata un novērtē kiberdraudus, zināmas ļaunprātīgi izmantojamas ievainojamības un apdraudējuma mazināšanas darbības attiecībā uz konkrētu būtisku kiberdrošības incidentu vai liela mēroga kiberdrošības incidentu. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* nolūkā izdarīt secinājumus, lai izvairītos no incidentiem nākotnē un mazinātu to sekas, iesniedz incidenta pārskata ziņojumu *EU-CyCLONe*, *CSIRT* tīklam, attiecīgajām dalībvalstīm un Komisijai, lai palīdzētu tiem veikt to uzdevumus, jo īpaši Direktīvas (ES) 2022/2555 15. un 16. pantā noteiktos uzdevumus. Ja incidents ietekmē *PDE* asociēto trešo valsti, *ENISA* iesniedz ziņojumu Padomei. Šādos gadījumos Komisija iesniedz ziņojumu Augstajam pārstāvim.

2. Lai sagatavotu šā panta 1. punktā minēto incidenta pārskata ziņojumu, *ENISA* sadarbojas ar visām attiecīgajām ieinteresētajām personām, tostarp dalībvalstu pārstāvjiem, Komisiju, citām attiecīgajām Savienības iestādēm, birojiem un aģentūrām, nozares pārstāvjiem, tostarp pārvaldīto drošības pakalpojumu sniedzējiem un kiberdrošības pakalpojumu lietotājiem, un saņem to atsauksmes. Attiecīgā gadījumā *ENISA* sadarbībā ar *CSIRT* un attiecīgā gadījumā sadarbībā ar kompetentajām iestādēm, kas izraudzītas vai izveidotas, ievērojot Direktīvas (ES) 2022/2555 8. panta 1. punktu, sadarbojas arī ar vienībām, kuras skar būtiski kiberdrošības incidenti vai liela mēroga kiberdrošības incidenti. Pārstāvji, ar kuriem konsultējas, dara zināmus jebkādus iespējamos interešu konfliktus.

3. Incidenta pārskata ziņojumā, kas minēts šī panta 1. punktā, iekļauj konkrētā būtiskā kiberdrošības incidenta vai liela mēroga kiberdrošības incidenta pārskatu un analīzi, tostarp galvenos cēloņus, zināmas ļaunprātīgi izmantojamas ievainojamības un gūtās atziņas. *ENISA* nodrošina, ka ziņojums atbilst Savienības vai valstu tiesību aktiem par sensitīvas vai klasificētas informācijas aizsardzību. Pēc attiecīgo dalībvalstu vai citu 14. panta 3. punktā minētu incidenta skartu lietotāju pieprasījuma datus un informāciju, kas iekļauti ziņojumā, anonimizē. Tajā neiekļauj nekādu informāciju par aktīvi izmantotām ievainojamībām, kas nav novērstas.

4. Attiecīgā gadījumā incidenta pārskata ziņojumā sniedz ieteikumus Savienības pozīcijas uzlabošanai kiberjautājumos, un var iekļaut paraugpraksi un atziņas, kas gūtas no attiecīgajām ieinteresētajām personām.

5. *ENISA* var izdot incidenta pārskata ziņojuma publiski pieejamu redakciju. Minētajā ziņojuma redakcijā iekļauj tikai uzticamu publisku informāciju vai citu uzticamu informāciju ar attiecīgo dalībvalstu piekrišanu un – attiecībā uz informāciju, kas saistīta ar lietotāju, kā minēts 14. panta 3. punkta b) vai c) apakšpunktā, – ar minētā lietotāja piekrišanu.

V nodaļa
Nobeiguma noteikumi

22. pants

Grozījumi Regulā (ES) 2021/694

Regulu (ES) 2021/694 groza šādi:

1) regulas 6. pantu groza šādi:

a) panta 1. punktu groza šādi:

i) iekļauj šādu apakšpunktu:

"aa) atbalstīt ES kiberdrošības trauksmes sistēmas ("Eiropas kiberdrošības brīdināšanas sistēma"), kas izveidota ar Eiropas Parlamenta un Padomes Regulas (ES) .../...[*+] 3. pantu, izstrādi, tostarp tādu valsts kibercentru un pārrobežu kibercentru izveidi, ierīkošanu un darbību, kas veicina situācijas apzināšanos Savienībā un uzlabo Savienības kiberdraudu izlūkošanas spējas;

_____

[*] Eiropas Parlamenta un Padomes Regula (ES)…, ar ko nosaka pasākumus, lai stiprinātu solidaritāti un spējas Savienībā atklāt kiberdraudus un kiberincidentus, tiem sagatavoties un uz tiem reaģēt, un ar ko groza Regulu (ES) 2021/694 (OV L, …, ELI: …).";

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru un zemsvītras piezīmē ievietot minētās regulas numuru, datumu, OV atsauci un ELI atsauci.

ii) pievieno šādu apakšpunktu:

"g) izveidot un izmantot kiberdrošības ārkārtas mehānismu, kas izveidots ar Regulas (ES)…/…[+] 10. pantu, tostarp ES kiberdrošības rezerves, kas izveidotas ar 14. pantu minētajā Regulā ("ES kiberdrošības rezerves"), kas palīdz dalībvalstīm sagatavoties būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem un uz tiem reaģēt, papildus valstu resursiem un spējām un citiem Savienības līmenī pieejamiem atbalsta veidiem, un atbalstīt citus lietotājus, tiem reaģējot uz būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem;";

b) panta 2. punktu aizstāj ar šādu:

"2. Darbības saskaņā ar konkrēto mērķi Nr. 3 galvenokārt īsteno, izmantojot Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetences centru un Nacionālo koordinācijas centru tīklu saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2021/887[*]. Tomēr ES kiberdrošības rezerves īsteno Komisija saskaņā ar Regulas (ES) .../...[+] 14. panta 6. punktu. *ENISA*.

---

[*] Eiropas Parlamenta un Padomes Regula (ES) 2021/887 (2021. gada 20. maijs), ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu (OV L 202, 8.6.2021., 1. lpp.).".

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru.

2) regulas 9. pantu groza šādi:

a) panta 2. punkta b), c) un d) apakšpunktus aizstāj ar šādiem:

"b) 1 760 806 000 EUR konkrētajam mērķim Nr. 2 – Mākslīgais intelekts;

c) 1 372 020 000 EUR konkrētajam mērķim Nr. 3 – Kiberdrošība un uzticamība;

d) 482 640 000 EUR konkrētajam mērķim Nr. 4 – Padziļinātas digitālās prasmes";

b) pievieno šādu punktu:

"8. Atkāpjoties no Finanšu regulas 12. panta 1. punkta, neizmantotās saistību un maksājumu apropriācijas darbībām ES kiberdrošības rezervju īstenošanas kontekstā un darbībām, kas atbalsta savstarpēju palīdzību, ievērojot Regulu …/…[+], ar kurām tiek īstenoti šīs regulas 6. panta 1. punkta g) apakšpunktā noteiktie mērķi, automātiski pārnes uz priekšu, un par tām var uzņemties saistības un samaksāt līdz nākamā finanšu gada 31. decembrim; Eiropas Parlamentu un Padomi informē par apropriācijām, kas pārnestas, ievērojot Finanšu regulas 12. panta 6. punktu.";

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru.

3) regulas 12. pantu groza šādi:

a) iekļauj šādus punktus:

"5.a Attiecībā uz tiesību subjektiem, kas ir iedibināti Savienībā, bet ko kontrolē no trešām valstīm, 5. punktu nepiemēro nevienai darbībai, ar ko īsteno Eiropas kiberdrošības trauksmes sistēmu, ja attiecībā uz minēto darbību ir izpildīti abi turpmāk minētie nosacījumi:

a) ņemot vērā kartēšanas rezultātus, kura īstenota, ievērojot Regulas (ES).../...[+] 9. panta 4. punktu, pastāv reāls risks, ka rīki, infrastruktūra vai pakalpojumi, kas ir vajadzīgi un pietiekami, lai minētā darbība pienācīgi sekmētu Eiropas kiberdrošības trauksmes sistēmas mērķi, nebūs pieejami no tiesību subjektiem, kas iedibināti vai ko uzskata par iedibinātiem dalībvalstīs un ko kontrolē dalībvalstis vai dalībvalstu valstspiederīgie;

b) drošības risks, kas saistīts ar iepirkumu no šādiem tiesību subjektiem Eiropas kiberdrošības trauksmes sistēmā, ir samērīgs ar ieguvumiem un neapdraud Savienības un tās dalībvalstu būtiskās drošības intereses.

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru.

5.b Attiecībā uz tiesību subjektiem, kas ir iedibināti Savienībā, bet ko kontrolē no trešām valstīm, 5. punktu nepiemēro darbībām, ar ko īsteno ES kiberdrošības rezerves, ja attiecībā uz konkrēto darbību ir izpildīti abi turpmāk minētie nosacījumi:

a) ņemot vērā kartēšanas rezultātus, kas veikta ievērojot Regulas (ES).../...[+] 14. panta 6. punktu, pastāv reāls risks, ka tehnoloģija, lietpratība vai spējas, kas vajadzīgas un pietiekamas, lai ES kiberdrošības rezerves pienācīgi pildītu savas funkcijas, nebūs pieejamas no tiesību subjektiem, kas iedibināti vai ko uzskata par iedibinātiem dalībvalstīs un ko kontrolē dalībvalstis vai dalībvalstu valstspiederīgie;

b) drošības risks, kas saistīts ar šādu tiesību subjektu iekļaušanu Eiropas kiberdrošības rezervēs, ir samērīgs ar ieguvumiem un neapdraud Savienības un tās dalībvalstu būtiskās drošības intereses.";

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru.

b) panta 6. punktu aizstāj ar šādu:

"6. Pienācīgi pamatotu drošības apsvērumu dēļ darba programmā var arī paredzēt, ka tiesību subjekti, kas iedibināti asociētajās valstīs, un tiesību subjekti, kas iedibināti Savienībā, bet ko kontrolē no trešām valstīm, visās darbībās, kas īstenojamas saskaņā ar konkrēto mērķi Nr. 1 un Nr. 2, vai atsevišķās šādi īstenojamās darbībās ir tiesīgi piedalīties tikai tad, ja ir ievērotas prasības, kuras minētajiem tiesību subjektiem ir jāpilda, lai garantētu Savienībai un tās dalībvalstīm būtiski svarīgu drošības interešu aizsardzību un lai nodrošinātu klasificētu dokumentu un informācijas aizsardzību. Minētās prasības nosaka darba programmā.

Attiecībā uz tiesību subjektiem, kas ir iedibināti Savienībā, bet ko kontrolē no trešām valstīm, pirmo daļu piemēro arī darbībām, ar ko īsteno konkrēto mērķi Nr. 3:

a) īstenot Eiropas kiberdrošības trauksmes sistēmu gadījumos, kad piemēro 5.a punktu, un

b) īstenot ES kiberdrošības rezerves gadījumos, kad piemēro 5.b punktu.";

4) regulas 14. panta 2. punktu aizstāj ar šādu:

"2. Finansējumu no Programmas var sniegt jebkurā Finanšu regulā noteiktā veidā, tostarp izmantojot iepirkumu kā galveno finansēšanas veidu, vai kā dotācijas un godalgas.

Ja darbības mērķa sasniegšana prasa inovatīvu preču un pakalpojumu iepirkumu, dotācijas var piešķirt tikai saņēmējiem, kuri ir līgumslēdzējas iestādes vai līgumslēdzēji, kas definēti attiecīgi Eiropas Parlamenta un Padomes Direktīvās 2014/24/ES* un 2014/25/ES**.

Ja darbības mērķa sasniegšanai ir nepieciešams sagādāt inovatīvas preces vai pakalpojumus, kas tirgū vēl nav plaši pieejami, līgumslēdzēja iestāde vai līgumslēdzējs vienā un tajā pašā iepirkuma procedūrā var piešķirt vairāku līgumu slēgšanas tiesības.

Pienācīgi pamatotu sabiedriskās drošības apsvērumu dēļ līgumslēdzēja iestāde vai līgumslēdzējs var prasīt, lai līguma izpilde notiktu Savienības teritorijā.

Īstenojot ES kiberdrošības rezervju iepirkuma procedūras, Komisija un *ENISA* var rīkoties kā centralizēto iepirkumu struktūra, veicot iepirkumu ar Programmu asociēto trešo valstu uzdevumā vai vārdā saskaņā ar šīs regulas 10. pantu. Komisija un *ENISA* var arī rīkoties kā vairumtirgotājs, pērkot, glabājot un minētajām trešajām valstīm pārdodot tālāk vai ziedojot preces un pakalpojumus, ieskaitot nomu. Atkāpjoties no Eiropas Parlamenta un Padomes Regulas (ES) 2024/2509*** 168. panta 3. punkta, vienas trešās valsts pieprasījums ir pietiekams, lai pilnvarotu Komisiju vai *ENISA* rīkoties.

Īstenojot ES kiberdrošības rezervju iepirkuma procedūras, Komisija un *ENISA* var rīkoties kā centralizēto iepirkumu struktūra, veicot iepirkumu Savienības iestāžu, struktūru, biroju vai aģentūru uzdevumā vai vārdā. Komisija un *ENISA* var arī rīkoties kā vairumtirgotājs, pērkot, glabājot un pārdodot tālāk vai ziedojot Savienības iestādēm, struktūrām, birojiem vai aģentūrām preces un pakalpojumus, ieskaitot nomu. Atkāpjoties no Regulas (ES, *Euratom*) 2024/2509 168. panta 3. punkta, vienas Savienības iestādes, struktūras, biroja vai aģentūras pieprasījums ir pietiekams, lai pilnvarotu Komisiju vai *ENISA* rīkoties.

Programmā var noteikt arī finansēšanu finansiālu instrumentu veidā finansējuma apvienošanas darbībās.

---

* Eiropas Parlamenta un Padomes Direktīva 2014/24/ES (2014. gada 26. februāris) par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

** Eiropas Parlamenta un Padomes Regula (ES) 2024/2509 (2024. gada 23. septembris) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam ... (OV L, 2024/2509..., ELI: http://data.europa.eu/eli/reg/2024/2509/oj...).

*** Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2024/2509 (2024. gada 23. septembris) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam (OV L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).”;

5) pievieno šādu pantu:

“*16.a pants*

Tiesību normu kolīzijas

Darbībām, ar kurām īsteno Eiropas kiberdrošības trauksmes sistēmu, piemērojamie noteikumi ir Regulas (ES) .../...[+] 4., 5. un 9. panta noteikumi. Ja ir kolīzija starp šīs regulas noteikumiem un Regulas (ES) .../...[+] 4., 5. un 9. pantu, prevalē pēdējie un tos piemēro minētajām konkrētajām darbībām.

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru.

Attiecībā uz ES kiberdrošības rezervēm īpaši noteikumi ar Programmu asociēto trešo valstu dalībai ir noteikti Regulas (ES) .../…[+]. 19. pantā. Ja ir kolīzija starp šīs regulas noteikumiem un Regulas (ES) .../... [+] 19. pantu, prevalē pēdējais un to piemēro minētajām konkrētajām darbībām.";

6) regulas 19. pantu aizstāj ar šādu:

"*19. pants*
Dotācijas

Programmas dotācijas piešķir un pārvalda saskaņā ar Finanšu regulas VIII sadaļu, un ar tām var segt līdz 100 % attiecināmo izmaksu, neskarot Finanšu regulas 190. pantā noteikto līdzfinansēšanas principu. Tādas dotācijas piešķir un pārvalda tā, kā noteikts katram konkrētajam mērķim.

Dalībvalstīm, kas atlasītas, ievērojot Regulas (ES) .../...[+] 9. pantu, un mitināšanas konsorcijam, kas minēts Regulas (ES) .../…[+] 5. pantā, atbalstu dotāciju veidā *ECCC* var saskaņā ar Finanšu regulas 195. panta 1. punkta d) apakšpunktu tieši piešķirt bez uzaicinājuma iesniegt priekšlikumus.

Atbalstu dotāciju veidā kiberdrošības ārkārtas mehānismam *ECCC* saskaņā ar Finanšu regulas 195. panta 1. punkta d) apakšpunktu var tieši piešķirt dalībvalstīm bez uzaicinājuma iesniegt priekšlikumus.

[+] OV: lūgums tekstā ievietot dokumentā PE-CONS 94/24 (2023/0109(COD)) ietvertās regulas numuru.

Attiecībā uz darbībām savstarpējas palīdzības atbalstam, kas paredzētas Regulas (ES) .../...+ 18. pantā, *ECCC* informē Komisiju un *ENISA* par dalībvalstu tiešo dotāciju pieprasījumiem bez uzaicinājuma iesniegt priekšlikumus.

Attiecībā uz darbībām savstarpējas palīdzības atbalstam, kas paredzētas Regulas (ES) .../...+ 18. pantā, un saskaņā ar Finanšu regulas 193. panta 2. punkta otrās daļas a) apakšpunktu pienācīgi pamatotos gadījumos par attiecināmām var uzskatīt arī izmaksas, kas radušās pirms dotācijas pieteikuma iesniegšanas.”;

7) I un II pielikumu groza saskaņā ar šīs regulas pielikumu.

23. pants

Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 14. panta 7. punktā minētos deleģētos aktus Komisijai piešķir uz piecu gadu laikposmu no ... [šīs regulas spēkā stāšanās diena]. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais 9 mēnešus pirms 5 gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais 3 mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 14. panta 7. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar katras dalībvalsts ieceltajiem ekspertiem saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

5. Tiklīdz Komisija pieņem deleģēto aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

6. Saskaņā ar 14. panta 7. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

24. pants

Komiteju procedūra

1. Komisijai palīdz ar Programmas "Digitālā Eiropa" koordinācijas komiteja, kas minēta Regulas (ES) 2021/694 31. panta 1. punktā. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011 nozīmē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

25. pants

Izvērtēšana un pārskatīšana

1. Līdz ...[divi gadi no šīs regulas spēkā stāšanās dienas] un pēc tam vismaz reizi četros gados Komisija izvērtē šajā regulā noteikto pasākumu darbību un iesniedz ziņojumu Eiropas Parlamentam un Padomei.

2. Šā panta 1. punktā minētajā izvērtējumā jo īpaši vērtē:

a) izveidoto valstu kibercentru un pārrobežu kibercentru skaitu, tās informācijas, ar kuru veikta dalīšanās, apjomu, tostarp, ja iespējams, ietekmi uz *CSIRT* tīkla darbu, un to, cik lielā mērā tie ir palīdzējuši stiprināt kiberdraudu un incidentu kopīgu atklāšanu Savienībā un situācijas apzināšanos par tiem, kā arī modernāko tehnoloģiju attīstību, un *PDE* finansējuma izmantošanu kopīgi iepirktajām kiberdrošības infrastruktūrām, rīkiem vai pakalpojumiem un, ja informācija ir pieejama, sadarbības līmeni starp valstu kibercentriem un būtisko un svarīgo vienību nozaru un starpnozaru kopienām, kā minēts Direktīvas (ES) 2022/2555 3. pantā;

b) to kiberdrošības ārkārtas mehānisma darbību izmantošanu un efektivitāti, ar ko atbalsta gatavību, tostarp apmācību, reaģēšanu uz un sākotnēju atkopšanos no būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem, tostarp *PDE* finansējuma izmantošanu un kiberdrošības ārkārtas mehānisma īstenošanā gūto pieredzi un ieteikumus;

c) ES kiberdrošības rezervju izmantošanu un efektivitāti attiecībā uz lietotāju veidiem, tostarp *PDE* finansējuma izmantošanu, pakalpojumu ieviešanu, tostarp to veidu, vidējo laiku, kas vajadzīgs atbildei uz pieprasījumiem un ES kiberdrošības rezerves izmantošanai, to pakalpojumu procentuālo daļu, kas pārveidoti par gatavības pakalpojumiem saistībā ar incidentu novēršanu un reaģēšanu uz tiem, kā arī ES kiberdrošības rezervju īstenošanā gūtās atziņas un ieteikumus;

d) ES kiberdrošības rezervju devumu Savienības rūpniecības un pakalpojumu, tostarp mikrouzņēmumu un mazo un vidējo uzņēmumu, kā arī jaunuzņēmumu, konkurētspējas stiprināšanā visā Savienības digitālajā ekonomikā un devumu kopējā mērķa stiprināt kiberdrošības prasmes un spējas sasniegšanā.

3. Pamatojoties uz 1. punktā minētajiem ziņojumiem, Komisija attiecīgā gadījumā iesniedz Eiropas Parlamentam un Padomei leģislatīva akta priekšlikumu grozījumu izdarīšanai šajā regulā.

26. pants

Stāšanās spēkā

Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē,

Eiropas Parlamenta vārdā —	*Padomes vārdā —*
priekšsēdētāja	*priekšsēdētājs / priekšsēdētāja*

PIELIKUMS

Regulu (ES) 2021/694 groza šādi:

1) I pielikuma iedaļu "Konkrētais mērķis Nr. 3 – Kiberdrošība un uzticamība" aizstāj ar šādu:

"Konkrētais mērķis Nr. 3 – Kiberdrošība un uzticamība

Programma stimulē būtisko spēju pastiprināšanu, veidošanu un iegūšanu, lai apsargātu Savienības digitālo ekonomiku, sabiedrību un demokrātiju, stiprinot Savienības kiberdrošības rūpniecisko potenciālu un konkurētspēju, kā arī uzlabojot gan privātā, gan publiskā sektora spēju pasargāt iedzīvotājus un uzņēmumus no kiberdraudiem, tostarp atbalstot Direktīvas (ES) 2016/1148 īstenošanu.

Sākotnējās un attiecīgos gadījumos sekojošās darbībās saskaņā ar šo mērķi ietilpst:

1. Ar dalībvalstīm kopīgas investīcijas progresīvā kiberdrošības aprīkojumā, infrastruktūrās un zinātībā, kas ir būtiski, lai kritiskās infrastruktūras un digitālo vienoto tirgu aizsargātu kopumā. Tādas kopīgas investīcijas varētu ietvert investīcijas kvantiskās iekārtās un datu resursos kiberdrošības un situācijas apzināšanās kibertelpā vajadzībām, tostarp valstu kibercentros un pārrobežu kibercentros, kas veido Eiropas kiberdrošības trauksmes sistēmu, kā arī citos rīkos, kas visā Eiropā padarāmi pieejami publiskajam un privātajam sektoram.

2. Pastāvošo tehnoloģisko jaudu paplašināšana un dalībvalstīs esošo kompetences centru tīklošanās, un šo jaudu atbilstības publiskā sektora un rūpniecības vajadzībām nodrošināšana, tostarp ar izstrādājumiem un pakalpojumiem, kas digitālajā vienotajā tirgū nostiprina kiberdrošību un uzticamību.

3. Efektīvu un modernu kiberdrošības un uzticamības risinājumu plašas ieviešanas nodrošināšana dalībvalstīs. Ieviešanā ietilpst ražojumu aizsargātības un drošuma stiprināšana no izstrādes līdz komercializācijai.

4. Atbalsts kiberdrošības prasmju deficīta pārvarēšanai, ņemot vērā dzimumu līdzsvaru, piemēram, saskaņojot kiberdrošības prasmju programmas, tās pielāgojot specifiskām nozaru vajadzībām un atvieglojot piekļuvi mērķētām specializētām apmācībām.

5. Dalībvalstu solidaritātes veicināšana, sagatavojoties būtiskiem kiberdrošības incidentiem un liela mēroga kiberdrošības incidentiem un reaģējot uz tiem, izmantojot kiberdrošības pakalpojumus pāri robežām, tostarp atbalstu publisko iestāžu savstarpējai palīdzībai un uzticamu pārvaldītu drošības pakalpojumu sniedzēju rezervju izveidei Savienības līmenī.”;

2) II pielikuma iedaļu “Konkrētais mērķis Nr. 3 – Kiberdrošība un uzticamība” aizstāj ar šādu:

“Konkrētais mērķis Nr. 3 – Kiberdrošība un uzticamība

3.1. Kopējā iepirkuma rezultātā iegūto kiberdrošības infrastruktūru vai rīku skaits, vai tie abi, tostarp saistībā ar Eiropas kiberdrošības trauksmes sistēmu

3.2. To lietotāju un lietotāju kopienu skaits, kuri iegūst piekļuvi Eiropas kiberdrošības iekārtām

3.3. To darbību skaits, ar kurām atbalsta gatavību kiberdrošības incidentiem un reaģēšanu uz tiem saskaņā ar kiberdrošības ārkārtas mehānismu”.

Attiecībā uz šo aktu ir sniegts paziņojums un tas ir pieejams [OV lūgums norādīt: OV C, XXX, XX.XX.2024., XX. lpp.] un šajā saitē: [OV: lūgums ievietot saiti uz paziņojumu].