GROZĪJUMI 001-001
iesnieguso Rūpniecības, pētniecības un enerģētikas komiteja

Ziņojums
Lina Gálvez Muñoz **A9-0426/2023**
Kibersolidaritātes akts

Regulas priekšlikums (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Grozījums Nr. 1

EIROPAS PARLAMENTA GROZĪJUMI *

Komisijas priekšlikumā

2023/0109 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA,

kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberapdraudējumu un kiberincidentus, tiem sagatavoties un uz tiem reaģēt*, un ar ko groza Regulu (ES) 2021/694*

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,

---

* Grozījumi: jaunais vai grozītais teksts ir norādīts treknā slīprakstā; svītrojumi ir apzīmēti ar simbolu ▌ .

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,

tā kā:

(1) Informācijas un komunikācijas tehnoloģiju lietošana un izmantošana visās saimnieciskās dzīves ***un demokrātijas*** nozarēs ir kļuvušas par fundamentāliem aspektiem***, taču vienlaikus ir radījušas iespējamu ievainojamību, jo*** mūsu publiskās pārvaldes iestādes, uzņēmumi un pilsoņi ir vairāk nekā jebkad agrāk cits ar citu saistīti un savstarpēji atkarīgi dažādās nozarēs un pārrobežu darbībās.

(2) ***Visā Savienībā un pasaulē gan izmantoto metožu, gan ietekmes ziņā*** pieaug kiberdrošības incidentu apjoms, biežums un ietekme, ieskaitot uzbrukumus piegādes ķēdēm, un to mērķis ir kiberspiegošana, izspiedējprogrammu izmantošana vai darbības traucēšana. Tie ievērojami apdraud tīklu un informācijas sistēmu darbību. Ņemot vērā strauji mainīgo apdraudējuma ainu, draudoši liela mēroga kiberincidenti, kas izraisa būtisku pārrāvumu vai kaitējumu ***ekonomikai, demokrātijai un*** kritiskajai infrastruktūrai ***visā Savienībā***, prasa labāku gatavību visos Savienības kiberdrošības satvara līmeņos. Minētais apdraudējums ir plašāks par Krievijas militāro agresiju pret Ukrainu, un tas visdrīzāk saglabāsies, jo pašreizējā ģeopolitiskajā saspīlējumā iesaistījušies daudzi valstu atbalstīti ***un*** krimināli ▌subjekti. Tādi kiberincidenti var kavēt sabiedrisku pakalpojumu sniegšanu un saimniecisku darbību, arī kritiskās vai sevišķi kritiskās nozarēs, radīt būtiskus finansiālus zaudējumus, mazināt lietotāju uzticēšanos, radīt būtisku kaitējumu Savienības ekonomikai un pat veselībai un dzīvībai bīstamas sekas. Bez tam kiberdrošības incidenti ir neprognozējami, jo tie mēdz rasties un izplesties pavisam īsā laikā, tos neierobežo nekāda ģeogrāfiska platība un tie notiek vienlaicīgi vai vienā mirklī izplatās daudzās valstīs. ***Tāpēc ir vajadzīga publiskā sektora, privātā sektora, akadēmisko aprindu, pilsoniskās sabiedrības un mediju cieša un saskaņota sadarbība. Turklāt Savienības reakcija ir jāsaskaņo ar starptautiskām struktūrām, kā arī ar uzticamiem un līdzīgi domājošiem starptautiskajiem partneriem. Uzticami un līdzīgi domājoši starptautiskie partneri ir valstis, kurām ir ar Savienību kopīgas vērtības — demokrātija, apņemšanās ievērot cilvēktiesības, efektīvs multilaterālisms un noteikumos balstīta kārtība saskaņā ar starptautiskās sadarbības satvariem un nolīgumiem. Lai nodrošinātu sadarbību ar uzticamiem un līdzīgi domājošiem starptautiskajiem partneriem un aizsardzību pret sistēmiskiem konkurentiem, nebūtu jāļauj vienībām, kas iedibinātas trešās valstīs, kuras nav Nolīguma par valsts iepirkumu (NVI) puses, piedalīties iepirkumā saskaņā ar šo regulu.***

(3) Ir jāstiprina rūpniecības un pakalpojumu nozaru konkurētspēja Savienībā visā digitalizētajā ekonomikā un jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā

---

1 OV C [...], [...], [...]. lpp.
2 OV C .., .., .. lpp.
3 OV C .., .., .. lpp.

tirgus kiberdrošību. Trijos dažādos konferences par Eiropas nākotni[1] priekšlikumos ir ieteikts palielināt pilsoņu, uzņēmumu, ***jo īpaši mikrouzņēmumu, mazo un vidējo uzņēmumu (MVU), tostarp jaunuzņēmumu***, un vienību, kuras darbina kritisko infrastruktūru, ***tostarp vietējo un reģionālo pašvaldību,*** noturību pret augošo kiberdrošības apdraudējumu, kas spēj nodarīt postu sabiedrībai un tautsaimniecībai. Tāpēc vajag ieguldīt infrastruktūrā un pakalpojumos ***un sekmēt spējas attīstīt kiberdrošības prasmes***, kas palīdzēs ātrāk atklāt kiberapdraudējumu un kiberdrošības incidentus un uz tiem reaģēt, un palīdzēt dalībvalstīm labāk sagatavoties būtiskiem un liela mēroga kiberdrošības incidentiem un reaģēt uz tiem. Savienībai arī jāpalielina savas spējas šajās jomās, galvenokārt datu vākšanai un kiberapdraudējuma un kiberincidentu analīzei.

(3a) Kiberuzbrukumi bieži tiek vērsti pret vietēja, reģionāla vai valsts mēroga sabiedrisko pakalpojumu sniedzējiem un infrastruktūrām. Vietējās pašvaldības ir viens no ievainojamākajiem mērķiem, jo tām trūkst finanšu resursu un cilvēkresursu. Tāpēc ir īpaši svarīgi, lai lēmumu pieņēmēji vietējā līmenī tiktu informēti par nepieciešamību palielināt digitālo noturību, vairot savas spējas mazināt kiberuzbrukumu ietekmi un izmantot šajā regulā paredzētās iespējas.

(4) Savienība jau ir noteikusi vairākus pasākumus, kam jāmazina kritisko infrastruktūru un vienību ievainojamība un jāuzlabo to noturība pret kiberapdraudējumu, to vidū Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555[2], Komisijas Ieteikums (ES) 2017/1584[3], Eiropas Parlamenta un Padomes Direktīva 2013/40/ES[4] un Eiropas Parlamenta un Padomes Regula (ES) 2019/881[5]. Bez tam Padomes ieteikumā par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai dalībvalstis tiek aicinātas veikt steidzamus un efektīvus pasākumus un lojāli, efektīvi, solidāri un koordinēti sadarboties savā starpā, ar Komisiju un citām attiecīgajām publiskajām iestādēm, kā arī ar attiecīgajām vienībām, lai pamatpakalpojumu sniegšanai iekšējā tirgū izmantoto kritisko infrastruktūru padarītu noturīgāku.

(5) Augošie kiberdrošības riski un vispārējā sarežģītā apdraudējuma vide, kurā nepārprotami draud strauja kiberincidentu pāriešana no vienas dalībvalsts uz citām un no trešas valsts uz Savienību, liek pastiprināt solidaritāti Savienības līmenī, lai labāk atklātu kiberdrošības apdraudējumu un kiberincidentus, tiem sagatavotos, ▌ uz tiem

---

1 https://futureu.europa.eu/lv/?locale=lv

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

3 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.).

4 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.*).

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.).

reaģētu ***un atkoptos pēc tiem***. Padomes secinājumos par ES nostāju kiberlietās[1] dalībvalstis arī aicinājušas Komisiju iesniegt priekšlikumu par jaunu Ārkārtēja stāvokļa reaģēšanas fondu kiberdrošībai.

(6) 2022. gada 10. novembrī pieņemtajā Kopīgajā paziņojumā par ES kiberaizsardzības politiku[2] tika izziņota ES kiberdrošības solidaritātes iniciatīva ar šādiem mērķiem: kopīgu ES spēju atklāt kiberapdraudējumu, apzināties stāvokli un reaģēt stiprināšana, veicinot ES drošības operāciju centru (DOC) ***tīkla*** izveidi, atbalstot ES līmeņa kiberdrošības rezervju pakāpenisku izveidi ar pakalpojumiem no uzticamiem privātiem pakalpojumu sniedzējiem un iespējamas kritisko vienību ievainojamības pārbaudi saskaņā ar ES riska novērtēšanas principiem.

(7) Ir jāstiprina kiberapdraudējuma un incidentu atklāšana un stāvokļa apzināšanās visā Savienībā un solidaritāte, uzlabojot dalībvalstu un Savienības gatavību un spējas ***nepieļaut būtiskus un liela mēroga kiberdrošības incidentus*** un reaģēt uz ***tiem***. Tādēļ Eiropas mērogā jāizveido DOC ***tīkls*** (Eiropas kibervairogs), lai veidotu un uzlabotu kopīgas spējas atklāt apdraudējumu un apzināties stāvokli***, tādējādi pastiprinot Savienības apdraudējumu atklāšanas un informācijas kopīgošanas spējas***; jāiedibina ***kiberdrošības ārkārtas*** mehānisms, kas palīdzētu dalībvalstīm sagatavoties būtiskiem un liela mēroga kiberdrošības incidentiem, uz tiem reaģēt un no tiem tūlīt atgūties; jāiedibina kiberdrošības incidentu izskatīšanas mehānisms konkrētu būtisku vai liela mēroga kiberdrošības incidentu izskatīšanai un novērtēšanai. Šīs darbības neskar Līguma par Eiropas Savienības darbību (LESD) 107. un 108. pantu.

(8) Lai šos mērķus sasniegtu, dažās jomās ir arī jāgroza Eiropas Parlamenta un Padomes Regula (ES) 2021/694[3]. Šai regulai jāgroza Regula (ES) 2021/694, programmas "Digitālā Eiropa" konkrēto mērķi Nr. 3 papildinot ar jauniem darbības mērķiem, kas attiecas uz Eiropas kibervairogu un ***kiberdrošības ārkārtas*** mehānismu, nolūkā garantēt digitālā vienotā tirgus noturību, veselumu un uzticamību, stiprināt spējas uzraudzīt kiberuzbrukumus un kiberapdraudējumu un reaģēt uz tiem un pastiprināt pārrobežu sadarbību kiberdrošībā. Ir jāparedz īpaši nosacījumi, ar kuriem minētajām darbībām var piešķirt finansiālu atbalstu, un jāiedibina paredzēto mērķu sasniegšanai nepieciešami pārvaldes un koordinācijas mehānismi. Citos Regulas (ES) 2021/694 grozījumos jāiekļauj saskaņā ar jaunajiem darbības mērķiem ierosināto darbību apraksti, kā arī izmērāmi rādītāji jauno darbības mērķu īstenošanas uzraudzībai.

(9) Darbību finansēšana atbilstoši šai regulai jānosaka Regulā (ES) 2021/694, kurai arī turpmāk vajadzētu būt relevantajam pamataktam attiecībā uz darbībām, kuras noteiktas programmas "Digitālā Eiropa" konkrētajā mērķī Nr. 3. Saskaņā ar piemērojamo Regulas (ES) 2021/694 noteikumu attiecīgajās darba programmās katrai darbībai tiks noteikti īpaši dalības nosacījumi.

(9a) Ņemot vērā ģeopolitiskās norises un pieaugošo kiberapdraudējuma ainu (EPP 52), kā arī mērķi nodrošināt šajā regulā noteikto pasākumu, jo īpaši Eiropas

---

1 Padomes secinājumi par Eiropas Savienības nostājas izveidi kiberlietās, kurus Padome apstiprināja 2022. gada 23. maija sanāksmē (9364/22).

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

3 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.).

kibervairoga un kiberdrošības ārkārtas mehānisma, darbības nepārtrauktību un turpmāku attīstību pēc 2027. gada, daudzgadu finanšu shēmā 2028.–2034. gadam ir jānodrošina īpaša budžeta pozīcija. Dalībvalstīm būtu arī jāapņemas atbalstīt visus pasākumus, kas vajadzīgi, lai visā Savienībā samazinātu kiberapdraudējumu un incidentus un stiprinātu solidaritāti.

(10) Šai regulai piemēro finansiālus pārnozaru noteikumus, ko Eiropas Parlaments un Padome pieņēmuši uz LESD 322. panta pamata. Minētie noteikumi ir izklāstīti ***Eiropas Parlamenta un Padomes Regulā (ES, Euratom) 2018/1046***[1] un nosaka galvenokārt Savienības budžeta izveides un izpildes procedūru, kā arī paredz finanšu subjektu atbildības pārbaudes. Uz LESD 322. panta pamata pieņemtajos noteikumos iekļauts arī vispārējs nosacītības režīms Savienības budžeta aizsardzībai, ko nosaka Eiropas Parlamenta un Padomes Regula (ES, *Euratom*) 2020/2092[2].

(11) Pareizai finanšu pārvaldībai vajadzīgi īpaši noteikumi par neizmantoto saistību un maksājumu apropriāciju pārnešanu uz priekšu. Ievērojot principu, ka Savienības budžets tiek noteikts katru gadu, šai regulai, ņemot vērā kiberdrošības vides neprognozējamās, ārkārtas un specifiskās iezīmes, būtu jāparedz iespējas pārnest neizmantotus līdzekļus, kuri pārsniedz ***Regulā (ES, Euratom) 2018/1046*** noteiktos, tā maksimalizējot ***kiberdrošības ārkārtas*** mehānisma spēju atbalstīt dalībvalstis kiberapdraudējuma efektīvā apkarošanā.

(11a) Ar šo regulu izveidotais kiberdrošības ārkārtas mehānisms un ES kiberdrošības rezerves ir jaunas iniciatīvas, kas netika paredzētas, izveidojot daudzgadu finanšu shēmu 2021.–2027. gadam, un finansējums šīm iniciatīvām ir paredzēts, lai pēc iespējas ierobežotu finansējuma samazināšanu citām programmas "Digitālā Eiropa" prioritātēm. Tāpēc finanšu resursu summa, kas paredzēta ES kiberdrošības rezervēm, būtu jāsamazina, un tā galvenokārt būtu jāiegūst no nepiešķirtajām rezervēm saskaņā ar daudzgadu finanšu shēmas maksimālajiem apjomiem vai jāpiesaista, izmantojot netematiskos daudzgadu finanšu shēmas īpašos instrumentus. Jebkāda līdzekļu iezīmēšana vai pārdale no pašreizējām programmām būtu jāsamazina līdz absolūtam minimumam, lai pašreizējās programmas, jo īpaši "Erasmus+", pasargātu no negatīvas ietekmes un nodrošinātu, ka minētās programmas var sasniegt tām izvirzītos mērķus.

(12) Lai efektīvāk nepieļautu un novērtētu kiberapdraudējumu un kiberincidentus**,** uz tiem reaģētu ***un no tiem atkoptos***, ir nepieciešams attīstīt plašākas zināšanas par Savienības teritorijā kritiskiem aktīviem un infrastruktūrām draudošām briesmām, kā arī par to ģeogrāfisko izplatību, savstarpējo saistību un iespējamām sekām tādu kiberuzbrukumu gadījumā, kas skar minētās infrastruktūras. ***Proaktīva pieeja iespējamu kiberdraudu apzināšanai, mazināšanai un nepieļaušanai ietver uzlabotu atklāšanas spēju***

---

1 ***Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2018/1046 (2018. gada 18. jūlijs) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam, ar kuru groza Regulas (ES) Nr. 1296/2013, (ES) Nr. 1301/2013, (ES) Nr. 1303/2013, (ES) Nr. 1304/2013, (ES) Nr. 1309/2013, (ES) Nr. 1316/2013, (ES) Nr. 223/2014, (ES) Nr. 283/2014 un Lēmumu Nr. 541/2014/ES un atceļ Regulu (ES, Euratom) Nr. 966/2012 (OV L 193, 30.7.2018., 1. lpp., ELI: https://eur-lex.europa.eu/eli/reg/2018/1046/oj?locale=lv).***

2 ***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.***

veicināšanu, jo tās ir nepieciešamas, lai apturētu pastāvīgos jaunos apdraudējumus. Apdraudējuma izlūkdati ir informācija, kas tiek vākta, analizēta un interpretēta, lai izprastu iespējamos apdraudējuma veidus un riskus. Liela datu apjoma analīze un korelācija parāda apdraudējuma modeļus, tendences un rādītājus, kas var atklāt ļaunprātīgas darbības vai vājās vietas. Jāizveido ***plašs*** Savienības DOC ***tīkls*** ("Eiropas kibervairogs"), kas sastāv no vairākām sadarbīgām pārrobežu platformām, kuras katra apvieno vairākus valstu DOC. Minētajai infrastruktūrai jākalpo valstu un Savienības kiberdrošības interesēm un vajadzībām, izmantojot jaunākās tehnoloģijas progresīvai datu vākšanai un analīzes rīkus, uzlabojot kiberapdraudējuma atklāšanas un pārvaldības spējas un nodrošinot stāvokļa apzināšanos reāllaikā. ***Valsts DOC ir centralizēta struktūra, kas ir atbildīga par apdraudējuma izlūkdatu pastāvīgu vākšanu un valsts jurisdikcijā esošo vienību kiberdrošības parametru uzlabošanu, nepieļaujot, atklājot un analizējot kiberdrošības apdraudējumus.*** Minētajai infrastruktūrai būtu jāpalīdz paplašināt kiberapdraudējuma un kiberincidentu atklāšanu un tādējādi papildināt un atbalstīt Savienības vienības un tīklus, kas atbild par krīžu pārvarēšanu Savienībā, īpaši ES Kiberkrīžu sadarbības organizāciju tīklu ("*EU-CyCLONe*"), kas definēts Eiropas Parlamenta un Padomes Direktīvā (ES) 2022/2555[1].

(13) ***Lai piedalītos kibervairoga darbībā,*** katrai dalībvalstij valsts līmenī būtu jānorīko publiska struktūra, kuras uzdevums ir attiecīgajā dalībvalstī koordinēt kiberapdraudējuma atklāšanas darbības. ***Dalībvalstis tiek mudinātas iekļaut valsts DOC struktūru to pastāvošajā kiberjomas sistēmā un pārvaldībā, lai neradītu papildu pārvaldības posmus un saskaņotu šo regulu ar jau spēkā esošajiem tiesību aktiem, tostarp Direktīvu 2022/2555.*** Šiem valstu līmeņa DOC vajadzētu darboties kā atsauces punktiem un vārtejai ***privātu un publisku vienību, jo īpaši valstu DOC,*** dalībai Eiropas kibervairogā un jānodrošina, ka informācija par kiberapdraudējumu no publiskām un privātām vienībām tiek valsts līmenī efektīvi un racionalizēti izplatīta un apkopota. ***Valstu DOC būtu jāstiprina sadarbība un informācijas apmaiņa starp publiskām un privātām vienībām, lai likvidētu pašreizējās komunikācijas barjeras. To darot, šie DOC var atbalstīt datu apmaiņas modeļu izveidi, un tiem būtu jāatvieglo un jāveicina informācijas apmaiņa uzticamā un drošā vidē. Ciešai un koordinētai sadarbībai starp publiskām un privātām struktūrām ir vissvarīgākā nozīme Savienības noturības stiprināšanā kiberdrošības jomā.***

(14) Eiropas kibervairoga sastāvā jāizveido vairāki pārrobežu kiberdrošības operāciju centri ("pārrobežu DOC"). Tajos apvienojami valstu DOC no vismaz trim dalībvalstīm, lai no pārrobežu apdraudējuma atklāšanas un informācijas kopīgošanas un pārvaldības būtu pilnīgs ieguvums. Pārrobežu DOC vispārīgajam mērķim jābūt stiprināt spējas analizēt, nepieļaut un atklāt kiberdrošības apdraudējumu un atbalstīt kvalitatīvu izlūkdatu par kiberdrošības apdraudējumiem sagatavošanu, ***cita starpā vācot un kopīgojot datus un informāciju par iespējamu uzlaušanu, jauniem ļaunprātīgiem draudiem un rīkiem, kas vēl nav izmantoti kiberincidentos, kā arī analīzes centienus, un to dara,*** kopīgojot datus no dažādiem publiskiem vai privātiem avotiem, kā arī uzticamā ***un drošā*** vidē***, ko nodrošina ar ENISA atbalstu,*** kopīgojot un koplietojot modernākos rīkus un kopīgi attīstot atklāšanas, analīzes un novēršanas spējas ***jautājumos, kas saistīti ar dalībvalstu operatīvo sadarbību***. ***Pārrobežu DOC būtu jāatvieglo un jāsekmē informācijas***

[1] Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris) par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību 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.).

apmaiņa uzticamā un drošā vidē un jānodrošina jaunas papildu spējas, izmantojot un savstarpēji papildinot esošos DOC un datorincidentu reaģēšanas vienības (“*CSIRT*”), kā arī citus attiecīgus subjektus.

(15) Valstī kiberapdraudējuma novērošanu, atklāšanu un analīzi parasti nodrošina publisko un privāto vienību DOC apvienojumā ar *CSIRT*. Turklāt saskaņā ar Direktīvu (ES) 2022/2555 *CSIRT* apmainās ar informāciju *CSIRT* tīklā. Pārrobežu DOC vajadzētu būt jaunai ***struktūrai***, kas ***tiek iekļauta jau pastāvošajā kiberdrošības infrastruktūrā, jo īpaši*** *CSIRT* ***tīklā***, tādējādi apkopojot un kopīgojot publisku un privātu vienību***, jo īpaši to DOC,*** datus par kiberapdraudējumu, tādu datu vērtību paaugstinot ar ekspertīzēm un kopīgi iegādātām infrastruktūrām un modernākajiem rīkiem un veicinot Savienības ***tehnoloģisko neatkarību, tās atvērto stratēģisko autonomiju, konkurētspēju un noturību, kā arī būtiskas kiberdrošības ekosistēmas izveidi, tostarp sadarbībā ar uzticamiem un līdzīgi domājošiem starptautiskajiem partneriem***. .

(16) Pārrobežu DOC vajadzētu darboties kā centrālam punktam, kurā iespējams plaši sakopot attiecīgus datus un kiberapdraudējuma izlūkdatus, jāveicina informācijas par apdraudējumu izplatīšana lielā un daudzveidīgā dalībnieku kopā (piemēram, datorapdraudējuma reaģēšanas vienību (“*CERT*”), *CSIRT*, informācijas apmaiņas un analīzes centru (“*ISAC*”), kritisko infrastruktūru operatoru vidū) ***ar mērķi sekmēt patlaban vērojamo saziņas barjeru likvidēšanu***. ***To darot, pārrobežu DOC varētu arī atbalstīt datu apmaiņas modeļu izveidi visā Savienībā.*** Informācijā, ar kuru apmainās pārrobežu DOC dalībnieki, var būt dati no tīkliem un sensoriem, apdraudējuma izlūkdatu plūsmas, aizskāruma rādītāji un kontekstualizēta informācija par kiberincidentiem, apdraudējumu un vājajām vietām***, tostarp datu un informācijas par iespējamiem uzlaušanas gadījumiem, jauniem ļaunprātīgiem draudiem un rīkiem, kas vēl nav izmantoti kiberincidentos, vākšana un kopīgošana, kā arī analīzes centieni***. Turklāt pārrobežu DOC arī būtu jānoslēdz sadarbības nolīgumi ar citiem pārrobežu DOC.

(17) Stāvokļa vienota apzināšanās attiecīgu iestāžu vidū ir nepieciešams priekšnoteikums visas Savienības gatavībai un koordinācijai būtiskos un liela mēroga kiberdrošības incidentos. Lai atbalstītu liela mēroga kiberdrošības incidentu un krīžu koordinētu pārvaldību operatīvā līmenī un nodrošinātu regulāru attiecīgas informācijas apmaiņu starp dalībvalstīm un Savienības iestādēm, struktūrām un aģentūrām, ar Direktīvu (ES) 2022/2555 ir izveidots *EU-CyCLONe*. Ieteikumā (ES) 2017/1584 par koordinētu reaģēšanu uz liela mēroga kiberdrošības incidentiem un krīzēm ir aplūkota visu attiecīgo subjektu loma. Direktīva (ES) 2022/2555 arī atsaucas uz Komisijas pienākumiem Savienības civilās aizsardzības mehānismā (“*UCPM*”), kas izveidots ar Eiropas Parlamenta un Padomes Lēmumu Nr. 1313/2013/ES[1], kā arī analītisku ziņojumu sniegšanā integrētajam krīzes politiskās reaģēšanas mehānismam (“*IPCR*”) ar ***Padomes*** Īstenošanas lēmumu (ES) 2018/1993[2] noteiktajā kārtībā. Tāpēc apstākļos, kad pārrobežu DOC iegūst informāciju, kas saistīta ar iespējamu vai notiekošu liela mēroga

---

1 ***Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu (Dokuments attiecas uz EEZ) (***OV L 347, 20.12.2013., 924. lpp.,
ELI: http://data.europa.eu/eli/dec/2013/1313/oj***).***

2 ***Padomes Īstenošanas lēmums (ES) 2018/1993 (2018. gada 11. 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).***

kiberdrošības incidentu, tiem jāsniedz attiecīga informācija *EU-CyCLONe*, *CSIRT* tīklam un Komisijai ***saskaņā ar Direktīvu (ES) 2022/2555***. Proti, kopīgojamajā informācijā attiecīgos apstākļos var būt tehniska informācija, informācija par uzbrucēja vai potenciālā uzbrucēja dabu un motīviem un augstāka līmeņa netehniska informācija par iespējamu vai notiekošu liela mēroga kiberdrošības incidentu. Šajā sakarā pienācīgi jāievēro princips "tiem, kam jāzina" un kopīgotās informācijas potenciālais jutīgums.

(18) Vienībām, kuras piedalās Eiropas kibervairogā, jānodrošina augsta līmeņa spēja savā starpā sadarboties, attiecīgi arī datu formātu, taksonomijas, datu apstrādes un datu analīzes rīku un drošu sakaru kanālu, lietojumprogrammu slāņa minimālā drošības līmeņa, stāvokļa apzināšanās infopaneļa un rādītāju jomā. Pieņemot vienotu taksonomiju un izstrādājot stāvokļa ziņojuma veidni kiberdrošības incidentu tehnisko cēloņu un ietekmes aprakstīšanai, jāņem vērā pašreizējais darbs saistībā ar paziņošanu par incidentiem Direktīvas (ES) 2022/2555 īstenošanas sakarā.

(19) Lai uzticamā ***un drošā*** vidē nodrošinātu plašu datu apmaiņu par kiberapdraudējumu no dažādiem avotiem, vienībām, kuras piedalās Eiropas kibervairogā, jābūt apgādātām ar pašiem modernākajiem un ļoti drošiem rīkiem, iekārtām un infrastruktūru***, un tām jānodrošina augsti kvalificēts personāls***. Tam jāļauj uzlabot kolektīvās atklāšanas spējas un laikus brīdināt iestādes un attiecīgās vienības, it īpaši – izmantojot jaunākās mākslīgā intelekta un datu analīzes tehnoloģijas.

(20) Vācot un kopīgojot datus un ar tiem apmainoties, Eiropas kibervairogam būtu jāstiprina Savienības tehnoloģiskā suverenitāte, ***tās stratēģiskā autonomija, konkurētspēja un noturība, kā arī ES būtiskas kiberdrošības ekosistēma***. Kvalitatīvu kūrētu datu sakopošanai arī jāveicina progresīvu mākslīgā intelekta un datu analīzes tehnoloģiju attīstība. ***Mākslīgais intelekts darbojas visefektīvāk, ja to papildina cilvēka veikta analīze. Tāpēc kvalificētam darbaspēkam joprojām ir būtiska nozīme augstas kvalitātes datu apkopošanā.*** Tā jāsekmē, Eiropas kibervairogu savienojot ar Eiropas augstas veiktspējas datošanas infrastruktūru, kas izveidota ar Padomes Regulu (ES) 2021/1173[1].

(21) Lai gan Eiropas kibervairogs ir civils projekts, kiberaizsardzības kopienai varētu būt labums no tādām spēcīgākām civilpersonu spējām atklāt apdraudējumu un apzināties situāciju, kuras izstrādātas kritiskās infrastruktūras aizsardzībai. Pārrobežu DOC ar Komisijas un Eiropas Kiberdrošības kompetences centra (*ECCC*) atbalstu un sadarbībā ar Savienības Augsto pārstāvi ārlietās un drošības politikā ("Augsto pārstāvi") būtu pakāpeniski jāizstrādā īpaši ***piekļuves nosacījumi un aizsardzības pasākumu*** protokoli un standarti, tostarp drošības pārbaudes un drošības nosacījumi, kas ļautu sadarboties ar kiberaizsardzības kopienu, ***ievērojot iestāžu civilo raksturu un finansējuma galamērķi un tādējādi izmantojot aizsardzības kopienai pieejamos līdzekļus***. Eiropas kibervairoga attīstība būtu jāpapildina ar atziņām, kas turpmāk ļautu sadarboties ar tīkliem un platformām, kuras kiberaizsardzības kopienā atbild par informācijas koplietošanu***, un tas jādara, cieši sadarbojoties ar Augsto pārstāvi un pilnībā ievērojot tiesības un brīvības***.

(22) Informācijas koplietošanai Eiropas kibervairoga dalībnieku starpā jāatbilst spēkā esošajām juridiskajām prasībām, it sevišķi Savienības un valstu datu aizsardzības tiesību

---

[1] Padomes Regula (ES) 2021/1173 (2021. gada 13. jūlijs) par Eiropas Augstas veiktspējas datošanas kopuzņēmuma izveidi un ar ko atceļ Regulu (ES) 2018/1488 (OV L 256, 19.7.2021., 3. lpp., ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

aktiem, kā arī Savienības konkurences noteikumiem, kas reglamentē informācijas apmaiņu. Tādā mērā, kādā nepieciešama personas datu apstrāde, informācijas saņēmējam jāīsteno tehniski un organizatoriski pasākumi, kas sargā datu subjektu tiesības un brīvības, un dati jāiznīcina, kolīdz tie vairs nav nepieciešami norādītajam mērķim, un jāinformē struktūra, kas datus dara pieejamus, ka dati ir iznīcināti.

(23) Neskarot LESD 346. pantu, tādas informācijas apmaiņai, kas ir konfidenciāla saskaņā ar Savienības vai valstu ***tiesību aktiem***, jāaprobežojas tikai ar tādu informāciju, kas ir būtiska un samērīga ar apmaiņas mērķi. Tādas informācijas apmaiņai jāsaglabā informācijas konfidencialitāte un jāaizsargā attiecīgo struktūru drošība un komercintereses, pilnībā ievērojot komercnoslēpumu un uzņēmuma noslēpumu.

(24) Ņemot vērā to, ka dalībvalstis skar aizvien lielāks kiberincidentu risks un skaits, ir jāizveido krīzes atbalsta instruments, kas uzlabotu Savienības noturību pret būtiskiem un liela mēroga kiberdrošības incidentiem un dalībvalstu darbības papildinātu ar ārkārtas finansiālu atbalstu būtiskāko dienestu gatavībai, reaģēšanai un tūlītējai atkopšanai. Minētajam instrumentam 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 kiberdrošības incidentus un krīzes nepieļaut, 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.

(25) ***Kiberdrošības ārkārtas*** mehānismam jāparedz atbalsts dalībvalstīm, papildinot to pasākumus un resursus, un citas pastāvošas atbalsta iespējas, kad jāreaģē uz būtiskiem un liela mēroga kiberdrošības incidentiem un nekavējoties jāatkopjas no tiem, piemēram, pakalpojumi, ko sniedz Eiropas Savienības Kiberdrošības aģentūra (“*ENISA*”) saskaņā ar tās pilnvarām, koordinēta reaģēšana un *CSIRT* tīkla palīdzība, *EU-CyCLONe* sniegtais seku mazināšanas atbalsts, kā arī dalībvalstu savstarpējā palīdzība, arī LES 42. panta 7. punkta kontekstā, *PESCO* ātrās kiberreaģēšanas vienībām[1] un ātrās hibrīdreaģēšanas vienībām. Tam jāapmierina vajadzība nodrošināt, ka ir pieejami specializēti līdzekļi, kas atbalsta gatavību kiberdrošības incidentiem un reaģēšanu uz tiem visā Savienībā un trešās valstīs.

(26) Šis instruments neskar procedūras un regulējumu, kuru mērķis ir koordinēt Savienības līmeņa reaģēšanu krīzēs, it īpaši *UCPM*[2], *IPCR*[3], un Direktīvu (ES) 2022/2555. Tas var veicināt vai papildināt darbības, kuras tiek īstenotas LES 42. panta 7. punkta sakarā vai LESD 222. pantā noteiktajos apstākļos. Attiecīgā gadījumā šā instrumenta izmantošana jākoordinē arī ar kiberdiplomātijas rīkkopas pasākumu īstenošanu.

(27) Saskaņā ar šo regulu sniegtajai palīdzībai jāatbalsta un jāpapildina dalībvalstu līmenī veiktās darbības. Tālab jānodrošina cieša sadarbība un apspriešanās starp Komisiju**,** ***ENISA*** un skarto dalībvalsti. Pieprasot ***kiberdrošības ārkārtas*** mehānisma atbalstu, dalībvalstij jāsniedz attiecīga informācija, kas pamato atbalsta nepieciešamību.

---

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

2 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.).

3 Integrētie krīzes situāciju politiskās reaģēšanas mehānismi (*IPCR*) un saskaņā ar Komisijas Ieteikumu (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.

(28) Direktīvā (ES) 2022/2555 ir noteikts, ka dalībvalstīm jāizraugās vai jāizveido viena vai vairākas kiberkrīzes pārvaldības iestādes un jānodrošina, ka tām ir pietiekami resursi savu uzdevumu efektīvai un lietderīgai pildīšanai. Tajā arī noteikts, ka dalībvalstīm ir jāapzina spējas, līdzekļi un procedūras, ko var izmantot krīzes gadījumā, kā arī jāpieņem valsts plāns reaģēšanai uz liela mēroga kiberdrošības incidentiem un krīzēm, kurā ir noteikti 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 sev jānodrošina 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 stiprināt gatavību, kā arī darbības reaģēšanai uz incidentu, lai mazinātu būtisku un liela mēroga kiberdrošības incidentu ietekmi, atbalstītu tūlītēju atkopšanos no tiem un/vai atjaunotu būtiskāko dienestu darbību.

(29) Lai gatavības darbību ietvaros veicinātu konsekventu pieeju un stiprinātu drošību visā Savienībā un tās iekšējā tirgū, jāsniedz atbalsts koordinētai tādu vienību kiberdrošības pārbaudei un novērtēšanai, kuras darbojas saskaņā ar Direktīvu (ES) 2022/2555 apzinātās sevišķi kritiskās nozarēs. Šajā nolūkā Komisijai ar *ENISA* atbalstu un sadarbībā ar TID sadarbības grupu, kas izveidota ar Direktīvu (ES) 2022/2555, regulāri jānosaka attiecīgās nozares vai apakšnozares, kurām jābūt tiesīgām saņemt finansiālu atbalstu koordinētai pārbaudes pasākumiem Savienības līmenī. Nozares vai apakšnozares jāizraugās no Direktīvas (ES) 2022/2555 I pielikuma ("Sevišķi kritiskās nozares"). Koordinētās pārbaudes pamatā jābūt kopīgiem riska scenārijiem un metodikai. Nozaru atlasē un riska scenāriju izstrādē jāņem vērā attiecīgie Savienības mēroga riska novērtējumi un riska scenāriji, ieskaitot izvairīšanos no dublēšanās, piemēram, riska izvērtēšana un riska scenāriji, kurus izmantot aicināts Padomes secinājumos par Eiropas Savienības pozīcijas izstrādi kiberlietās, kas jāveic Komisijai, Augstajam pārstāvim un TID sadarbības grupai, koordinējoties ar attiecīgām civilām un militārām struktūrām un aģentūrām un izveidotiem tīkliem, to vidū *EU-CyCLONe*, kā arī sakaru tīklu un infrastruktūru riska novērtējums, kas pieprasīts Nevēras kopīgajā ministru aicinājumā un ko veic TID sadarbības grupa ar Komisijas un *ENISA* atbalstu un sadarbībā ar Eiropas Elektronisko sakaru regulatoru iestādi (*BEREC*), koordinētā riska novērtēšana, kas veicama saskaņā ar Direktīvas (ES) 2022/2555 22. pantu, un digitālās darbības noturības pārbaude, kas paredzēta Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554[1]. Nozaru atlasē jāņem vērā arī Padomes ieteikums par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai.

(30) Turklāt ***kiberdrošības ārkārtas*** mehānismam jāsniedz atbalsts citām gatavības veicināšanas darbībām un jāatbalsta gatavība citās nozarēs, uz kurām neattiecas tādu vienību koordinēta pārbaude, kuras darbojas sevišķi kritiskās nozarēs. Minētajās darbībās var ietilpt dažādi valstu gatavības pasākumi.

(31) ***Kiberdrošības ārkārtas*** mehānismam arī jāsniedz atbalsts reaģēšanas darbībām kiberdrošības incidentos, lai mazinātu būtisku un liela mēroga kiberdrošības incidentu ietekmi, atbalstītu tūlītēju atkopšanos vai atjaunotu būtiskāko dienestu darbību.

---

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

Attiecīgā gadījumā tam jāpapildina *UCPM*, lai nodrošinātu visaptverošu pieeju reaģēšanai uz kiberincidentu ietekmi uz pilsoņiem.

(32) ***Kiberdrošības ārkārtas*** mehānismam jāatbalsta palīdzība, ko dalībvalstis sniedz dalībvalstij, kuru skāris būtisks vai liela mēroga kiberdrošības incidents, ieskaitot *CSIRT* tīklu, kas noteikts Direktīvas (ES) 2022/2555 15. pantā. Jāļauj dalībvalstīm, kuras sniedz palīdzību, iesniegt lūgumus segt izmaksas, kas saistītas ar ekspertu vienību nosūtīšanu savstarpējai palīdzībai. Atlīdzināmajās izmaksās var būt kiberdrošības ekspertu ceļa, uzturēšanās un dienas naudas izdevumi.

(33) Lai atbalstītu reaģēšanas un tūlītējas atkopšanas darbības būtisku vai liela mēroga kiberdrošības incidentu gadījumos, pakāpeniski jāveido Savienības līmeņa kiberdrošības rezerves, kas sastāv no pārvaldīto drošības pakalpojumu privāto sniedzēju pakalpojumiem. ES kiberdrošības rezervēm būtu jānodrošina dienestu pieejamība un gatavība***un vienlaikus jāstiprina Savienības noturība, cita starpā tādu Eiropā pārvaldītu drošības pakalpojumu sniedzēju iesaiste, kas ir MVU, un jānodrošina kiberdrošības ekosistēmas izveide, jo īpaši iesaistot mikrouzņēmumus, MVU un jaunuzņēmumus, un veicot investīcijas pētniecībā un inovācijā, lai izstrādātu mūsdienīgas tehnoloģijas, piemēram, ar mākoņdatošanu un mākslīgo intelektu saistītas tehnoloģijas***. ***Uzticamiem pakalpojumu sniedzējiem, tostarp MVU, vajadzētu būt iespējai savstarpēji sadarboties, lai izpildītu iepriekš minētos kritērijus.*** Pakalpojumiem no ES kiberdrošības rezervēm jāpalīdz valstu iestādēm papildus darbībām valsts līmenī sniegt palīdzību skartajām vienībām, kuras darbojas kritiskās vai sevišķi kritiskās nozarēs. ***Tāpēc kiberdrošības rezervēm būtu jāstimulē investīcijas pētniecībā un inovācijā, lai veicinātu šo tehnoloģiju izstrādi. Attiecīgā gadījumā ar uzticamajiem pakalpojumu sniedzējiem un potenciālajiem kiberdrošības rezervju lietotājiem varētu veikt kopīgas mācības, lai nodrošinātu rezervju efektīvu darbību.*** Pieprasot atbalstu no ES kiberdrošības rezervēm, dalībvalstīm jāprecizē atbalsts, kas skartajai vienībai sniegts valsts līmenī, un tas jāņem vērā, novērtējot dalībvalsts pieprasījumu. Ar līdzīgiem nosacījumiem pakalpojumus no ES kiberdrošības rezervēm var izmantot arī Savienības iestāžu, struktūru***, biroju*** un aģentūru atbalstīšanai. ***Komisijai būtu jānodrošina dalībvalstu iesaistīšanās un plaša informācijas apmaiņa ar tām, lai izvairītos no dublēšanās ar līdzīgām iniciatīvām, tostarp Ziemeļatlantijas līguma organizācijā (NATO).***

(34) Lai izvēlētos privātos pakalpojumu sniedzējus pakalpojumu sniegšanai ES kiberdrošības rezervju sakarā, ir jānosaka minimālo kritēriju kopums, kas būtu jāiekļauj uzaicinājumā iesniegt piedāvājumus, lai atlasītu šos pakalpojumu sniedzējus, tādējādi nodrošinot, ka tiek apmierinātas to dalībvalstu iestāžu un vienību vajadzības, kuras darbojas kritiskās vai sevišķi kritiskās nozarēs. ***Būtu jāveicina tādu mazāku pakalpojumu sniedzēju līdzdalība, kuri darbojas reģionālā un vietējā līmenī.***

(35) Atbalstot ES kiberdrošības rezervju izveidi, Komisija var apsvērt pieprasījumu *ENISA* sagatavot Regulai (ES) 2019/881 atbilstošu kandidātu sertifikācijas shēmu, kas attiektos uz pārvaldītiem drošības pakalpojumiem jomās, uz kurām attiecas ***kiberdrošības ārkārtas*** mehānisms. ***Lai izpildītu no šā noteikuma izrietošos papildu uzdevumus, ENISA būtu jāsaņem pienācīgs papildu finansējums.***

(36) Lai tuvinātu šīs regulas mērķus veicināt kopīgu stāvokļa apzināšanos, uzlabot Savienības noturību un sagādāt iespēju efektīvi reaģēt uz būtiskiem un liela mēroga kiberdrošības incidentiem, *EU-CyCLONe*, *CSIRT* tīklam vai Komisijai jāvar lūgt *ENISA* izskatīt un novērtēt apdraudējumu, vājās vietas un seku mazināšanas darbības konkrēta

būtiska vai liela mēroga kiberdrošības incidenta sakarā. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* sadarbībā ar attiecīgajām ieinteresētajām personām, ieskaitot privātā sektora, dalībvalstu, Komisijas un citu attiecīgo ES iestāžu, struktūru***, biroju*** un aģentūru pārstāvjus, jāsagatavo incidenta pārskata ziņojums. Attiecībā uz privāto sektoru *ENISA* veido kanālus informācijas apmaiņai ar specializētiem pakalpojumu sniedzējiem, arī pārvaldītu drošības risinājumu pagādātājiem un pārdevējiem, lai palīdzētu izpildīt *ENISA* uzdevumu visā Savienībā panākt vienādi augstu kiberdrošību. Pamatojoties uz sadarbību ar ieinteresētajām personām, ieskaitot privāto sektoru, pārskata ziņojumam par konkrētiem incidentiem jābūt mērķim pēc incidenta novērtēt tā cēloņus, ietekmi un seku mazinājumu. Īpaša uzmanība jāpievērš to pārvaldīto drošības pakalpojumu sniedzēju ieguldījumam un pieredzei, kuri atbilst šīs regulas noteiktajiem visaugstākās profesionālās godprātības, objektivitātes un nepieciešamo tehnisko zināšanu nosacījumiem. Ziņojums jāiesniedz *EU-CyCLONe*, *CSIRT* tīklam un Komisijai un jāizmanto to darbā. Ja incidents ir saistīts ar trešu valsti, Komisijai par to jāinformē arī Augstais pārstāvis.

(37) Ņemot vērā kiberdrošības uzbrukumu neparedzamību un to, ka tie mēdz neaprobežoties ar noteiktu ģeogrāfisku apgabalu un ka ir ļoti iespējama to izplatīšanās citos apgabalos, tad, stiprinot kaimiņvalstu noturību un spēju efektīvi reaģēt uz būtiskiem un liela mēroga kiberdrošības incidentiem, tiek veicināta visas Savienības aizsardzība. Tāpēc ar programmu "Digitālā Eiropa" asociētās trešās valstis var saņemt atbalstu no ES kiberdrošības rezervēm, ja tāds ir paredzēts attiecīgajā asociācijas nolīgumā ar programmu "Digitālā Eiropa". Savienībai jāatbalsta finansējums asociētajām trešajām valstīm attiecīgo šīm valstīm paredzēto partnerību un finansēšanas instrumentu ietvaros. Atbalstam jāaptver dienesti, kas paredzēti reaģēšanai uz būtiskiem vai liela mēroga kiberdrošības incidentiem un tūlītējai atkopšanai. Šīs regulas nosacījumi ES kiberdrošības rezervēm un uzticamiem pakalpojumu sniedzējiem jāpiemēro, arī atbalstot ar programmu "Digitālā Eiropa" asociētās trešās valstis.

(37a) Trešās valstis varētu piekļūt resursiem un atbalstam saskaņā ar šo regulu, izmantojot atbalstu reaģēšanai uz incidentiem no ES kiberdrošības rezervēm. Turklāt, lai sniegtu konkrētus pakalpojumus, izmantojot ES kiberdrošības rezerves, var būt vajadzīgi reaģēšanas uz incidentiem pakalpojumu sniedzēji no trešām valstīm, tostarp programmas "Digitālā Eiropa" asociētajām trešām valstīm vai citām starptautiskām partnervalstīm, kā arī NATO dalībvalstīm. Atkāpjoties no Regulas (ES, Euratom) 2018/1046, lai stiprinātu Savienības tehnoloģisko suverenitāti, tās atvērto stratēģisko autonomiju, konkurētspēju un noturību un aizsargātu Savienības stratēģiskos aktīvus, intereses vai drošību, vienībām, kas iedibinātas trešās valstīs, kuras nav NVI puses un kurām nav veikta izvērtēšana Eiropas Parlamenta un Padomes Regulas (ES) 2019/452[1] nozīmē, un vajadzības gadījumā seku mazināšanas pasākumi, ņemot vērā šajā regulā noteiktos mērķus, nebūtu jāļauj piedalīties. Šīs regulas ārējai dimensijai būtu jāatbilst noteikumiem, kas paredzēti asociācijas nolīgumā atbilstīgi programmai "Digitālā Eiropa". Trešo valstu dalība būtu jāpakļauj sabiedrības kontrolei, kurā piedalās likumdevēji, lai nodrošinātu iedzīvotāju līdzdalību šajā procesā.

[1] Eiropas Parlamenta un Padomes Regula (ES) 2019/452 (2019. gada 19. marts), ar ko izveido regulējumu ārvalstu tiešo ieguldījumu Savienībā izvērtēšanai (OV L 79I , 21.3.2019., 1. lpp., ELI: http://data.europa.eu/eli/reg/2019/452/oj.

(38) Lai nodrošinātu vienveidīgus nosacījumus šīs regulas īstenošanai, Komisijai jāsaņem īstenošanas pilnvaras noteikt pārrobežu DOC sadarbspējas nosacījumus, noteikt pārrobežu DOC un Savienības struktūru informācijas koplietošanas kārtību iespējamos vai notiekošos liela mēroga kiberdrošības incidentos, noteikt tehniskās prasības, kas nodrošina Eiropas kibervairoga drošību, noteikt ES kiberdrošības rezervēm nepieciešamo reaģēšanas pakalpojumu veidus un skaitu un sīkāk izstrādāt ES kiberdrošības rezervju atbalsta pakalpojumu piešķiršanas kārtību. Minētās pilnvaras īstenojamas saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) Nr. 182/2011*.

---

* ***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).***

(38a) Lai efektīvi īstenotu Eiropas kibervairogu un kiberdrošības ārkārtas mehānismu, ir nepieciešams kvalificēts personāls, kas spēj uzticami sniegt attiecīgos kiberdrošības pakalpojumus atbilstoši augstākajiem standartiem. Tāpēc pastāv bažas par to, ka Savienība saskaras ar talantu trūkumu, ko raksturo kvalificētu speciālistu trūkums, taču vienlaikus strauji pieaug apdraudējumi, kā atzīts Komisijas 2023. gada 18. aprīļa paziņojumā par Kiberprasmju akadēmiju. Ir svarīgi novērst šo talantu trūkumu, stiprinot sadarbību un koordināciju starp dažādām ieinteresētajām personām, tostarp privāto sektoru, akadēmiskajām aprindām, dalībvalstīm, Komisiju un ENISA, nolūkā visās teritorijās paplašināt un radīt sinerģiju ieguldījumiem izglītībā un apmācībā, attīstot publiskā un privātā sektora partnerības, atbalstot pētniecības un inovācijas iniciatīvas, izstrādājot un savstarpēji atzīstot kopīgus standartus un kiberdrošības prasmju sertifikāciju, tostarp izmantojot Eiropas kiberdrošības prasmju satvaru. Tam būtu arī jāveicina kiberdrošības speciālistu mobilitāte Savienībā. Šīs regulas mērķim vajadzētu būt veicināt daudzveidīgāku kiberdrošības darbaspēku. Visiem pasākumiem, kuru mērķis ir uzlabot kiberdrošības prasmes, ir vajadzīgi aizsardzības līdzekļi, lai izvairītos no intelektuālā darbaspēka emigrācijas un darbaspēka mobilitātes riska.

(38b) Visā Savienībā ir jāstiprina specializētas, starpdisciplināras un vispārējas prasmes un kompetences, īpašu uzmanību pievēršot sievietēm, jo kiberdrošības jomā joprojām pastāv dzimumu atšķirības, proti, sievietes veido tikai 20 % no vidēji pasaulē šajā jomā nodarbināto skaita. Sievietēm ir jāpiedalās un jābūt daļai no digitālās nākotnes un tās pārvaldības izstrādes.

(38c) Pētniecības un inovācijas stiprināšana kiberdrošības jomā ir paredzēta, lai vairotu Savienības noturību un atvērto stratēģisko autonomiju. Tāpat ir svarīgi radīt sinerģiju ar pētniecības un inovācijas programmām un pastāvošajiem instrumentiem un iestādēm un stiprināt sadarbību un koordināciju starp dažādām ieinteresētajām personām, tostarp privāto sektoru, pilsonisko sabiedrību, akadēmiskajām aprindām, dalībvalstīm, Komisiju un ENISA;

(38d) Šai regulai būtu jāsekmē tas, lai tiktu pildīta Eiropas Deklarācijā par digitālajām tiesībām un principiem digitālajai desmitgadei minētā apņemšanās aizsargāt mūsu demokrātiju, cilvēku, uzņēmumu un publisko iestāžu intereses pret kiberdrošības riskiem un kibernoziedzību, tostarp datu aizsardzības pārkāpumiem un identitātes zādzībām vai manipulācijām. Šīs regulas piemērošanai būtu arī jāpalīdz uzlabot citu

tiesību aktu īstenošanu, piemēram, attiecībā uz mākslīgo intelektu, datu privātumu un datu regulējumu kiberdrošības un kibernoturības jomā.

(38e) Šīs regulas sekmīgai īstenošanai ir svarīgi vairot kiberdrošības kultūru, kas ietver drošību, tostarp digitālajā vidē, kā sabiedrisku labumu. Tāpēc tādu pasākumu izstrādei, kuru mērķis ir iesaistīt iedzīvotājus un palielināt viņu informētību, vajadzētu būt papildu līdzeklim, ar kura palīdzību garantēt mūsu demokrātiju un pamatvērtību aizsardzību.

(38f) Lai papildinātu dažus nebūtiskus šīs regulas elementus, būtu jādeleģē Komisijai pilnvaras pieņemt aktus saskaņā ar LESD 290. pantu nolūkā precizēt nosacījumus pārrobežu DOC sadarbspējai, noteikt procedūru informācijas apmaiņai starp pārrobežu DOC, no vienas puses, un EU-CyCLONe, CSIRT tīklu un Komisiju, no otras puses, precizēt ES kiberdrošības rezervēm nepieciešamo reaģēšanas pakalpojumu veidus un to skaitu un sīkāk precizēt ES kiberdrošības rezervju atbalsta pakalpojumu piešķiršanas kārtību. 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*. 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.

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

(39) ***Ņemot vērā to, ka*** šīs regulas ***mērķus, proti, stiprināt Savienības kiberapdraudējuma novēršanas, atklāšanas, reaģēšanas un atkopšanās spējas un izveidot vispārēju sistēmu saziņas trūkuma novēršanai, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet minētos mērķus var labāk sasniegt Savienības līmenī,*** Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteiktajiem subsidiaritātes un proporcionalitātes principiem. ***Saskaņā ar minētajā pantā noteikto proporcionalitātes principu*** šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai,

IR PIEŅĒMUŠI ŠO REGULU.

I nodaļa

VISPĀRĪGI MĒRĶI, PRIEKŠMETS UN DEFINĪCIJAS

1. pants

Priekšmets un mērķi

1. Šī regula nosaka pasākumus, kuru mērķis ir stiprināt spējas Savienībā atklāt kiberdrošības apdraudējumu un incidentus, tiem sagatavoties un uz tiem reaģēt, sevišķi ar šādām darbībām:

a) drošības operāciju centru Eiropas mēroga ***tīkla*** (“Eiropas kibervairoga”) ierīkošana, lai izveidotu un uzlabotu kopīgas atklāšanas un stāvokļa apzināšanās spējas;

b) ***kiberdrošības ārkārtas*** mehānisma izveide, kas palīdzētu dalībvalstīm sagatavoties būtiskiem un liela mēroga kiberdrošības incidentiem, uz tiem reaģēt un pēc tiem tūdaļ atkopties;

c) Eiropas kiberdrošības incidentu izskatīšanas mehānisma izveide būtisku vai liela mēroga incidentu izskatīšanai un novērtēšanai.

2. Šīs regulas mērķis ir Savienības līmenī stiprināt solidaritāti, tiecoties uz šādiem specifiskiem mērķiem:

a) stiprināt Savienības kiberapdraudējuma un incidentu kopīgu atklāšanu un stāvokļa apzināšanos, tā ļaujot ***atbalstīt Savienības un dalībvalstu rūpniecisko jaudu kiberdrošības nozarē, un*** stiprināt Savienības rūpniecības***, jo īpaši mikrouzņēmumu un MVU, tostarp jaunuzņēmumu,*** un pakalpojumu nozaru konkurētspēju visā digitālajā ekonomikā, un veicināt Savienības tehnoloģisko suverenitāti***, tās atvērto stratēģisko autonomiju, konkurētspēju un noturību minētajā nozarē, stiprinot kiberdrošības ekosistēmu, lai spēcinātu Savienības spējas, tostarp sadarbībā ar starptautiskajiem partneriem***;

b) visā Savienībā stiprināt to vienību gatavību, kuras darbojas kritiskās un sevišķi kritiskās nozarēs, un stiprināt solidaritāti, attīstot spējas vienoti reaģēt būtiska vai liela mēroga kiberdrošības incidenta gadījumā, cita starpā Savienības atbalstu reaģēšanai uz kiberdrošības incidentiem darot pieejamu programmas “Digitālā Eiropa” (“PDE”) asociētajām trešām valstīm;

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

ca) koordinēti attīstīt darbaspēka prasmes, zinātības spējas un kompetences, lai panāktu kiberdrošību un veidotu sinerģiju ar Kiberdrošības prasmju akadēmiju.

3. Šī regula neskar to, ka primārā atbildība par valsts drošību, sabiedrisko drošību un noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem ir dalībvalstīm.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

(-1a) “valsts drošības operāciju centrs” jeb “valsts DOC” ir centralizēta valsts struktūra, kas pastāvīgi vāc un analizē kiberapdraudējuma izlūkdatus un uzlabo kiberdrošības parametrus saskaņā ar 4. pantu;

(1) **"pārrobežu drošības operāciju centrs"** ***jeb*** **"pārrobežu DOC"** ir daudzvalstu platforma, kas koordinētā tīkla struktūrā apvieno valstu DOC ***saskaņā ar 5. pantu;***

(2) **"publiska struktūra"** ir publisko tiesību ***subjekti***, kas ***definēti*** Eiropas Parlamenta un Padomes Direktīvas 2014/24/ES[1] 2. panta 1. punkta 4) apakšpunktā;

(3) **"mitināšanas konsorcijs"** ir konsorcijs, ko veido iesaistītās valstis, kuras pārstāv valstu DOC ***saskaņā ar 5. pantu***;

(4) **"vienība"** ir Direktīvas (ES) 2022/2555 6. panta 38. punktā definēta vienība;

(4a) "kritiskā vienība" ir Eiropas Parlamenta un Padomes Direktīvas (ES) 2022/2557[2] 2. panta 1) punktā definēta kritiskā vienība;

(5) **"vienības, kas darbojas kritiskās vai sevišķi kritiskās nozarēs"**, ir ***vienības*** Direktīvas (ES) 2022/2555 I un II pielikumā ***uzskaitītajās nozarēs***;

(5a) "incidenta risināšana" ir incidenta risināšana, kā definēts Direktīvas (ES) 2022/2555 6. panta 8) punktā;

(5b) "risks" ir Direktīvas (ES) 2022/2555 6. panta 9) punktā definēts risks;

(6) **"kiberapdraudējums"** ir Regulas (ES) 2019/881 2. panta 8) punktā definēti kiberdraudi;

(6a) "būtisks kiberapdraudējums" ir Direktīvas (ES) 2022/2555 6. panta 11) punktā definēti būtiski kiberdraudi;

(7) **"būtisks kiberdrošības incidents"** ir kiberdrošības incidents, kas atbilst Direktīvas (ES) 2022/2555 23. panta 3. punktā noteiktajiem kritērijiem;

(8) **"liela mēroga kiberdrošības incidents"** ir Direktīvas (ES) 2022/2555 6. panta 7) punktā definēts incidents;

(9) **"gatavība"** ir gatavība un spēja nodrošināt efektīvu un ātru reaģēšanu uz būtisku vai liela mēroga kiberdrošības incidentu, kas panāktas iepriekšējas riska novērtēšanas un novērošanas rezultātā;

(10) **"reaģēšana"** ir rīcība būtiska vai liela mēroga kiberdrošības incidenta gadījumā vai tā laikā, vai pēc tā, lai pārvarētu tā tūlītējās un īslaicīgās negatīvās sekas;

(10a) "pārvaldītu drošības pakalpojumu sniedzējs" ir Direktīvas (ES) 2022/2555 6. panta 40) punktā definēts pārvaldītu drošības pakalpojumu sniedzējs;

(11) **"uzticami *pārvaldītu drošības* pakalpojumu sniedzēji"** ir ▌pārvaldītu drošības pakalpojumu sniedzēji, kas ***saskaņā ar šīs regulas 16. pantu atlasīti iekļaušanai ES kiberdrošības rezervēs***.

---

1 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.).

2 ***Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2557 (2022. gada 14. decembris) par kritisko vienību noturību un Padomes Direktīvas 2008/114/EK atcelšanu (OV L 333, 27.12.2022., 164. lpp., ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***

II nodaļa

EIROPAS KIBERVAIROGS

3. pants

Eiropas kibervairoga izveide

1. Lai attīstītu progresīvas Savienības spējas atklāt, analizēt un apstrādāt datus par kiberapdraudējumu un ***nepieļaut incidentus*** Savienībā, tiek ***izveidots drošības operāciju tīkls*** ("Eiropas kibervairogs"). Tas sastāv no visiem valstu drošības operāciju centriem ("valsts DOC") un pārrobežu drošības operāciju centriem ("pārrobežu DOC").

Eiropas kibervairoga īstenošanas darbības atbalsta ar programmas "Digitālā Eiropa" finansējumu un īsteno saskaņā ar Regulu (ES) 2021/694, sevišķi tās konkrēto mērķi Nr. 3.

2. Eiropas kibervairogs:

a) caur pārrobežu DOC gan valstu, gan ES līmenī sakopo un kopīgo dažādu avotu datus par kiberapdraudējumu un incidentiem un ***attiecīgā gadījumā veic informācijas apmaiņu ar CSIRT tīklu***;

b) rada kvalitatīvu lietā liekamu informāciju un kiberapdraudējuma izlūkdatus, izmantojot pašus modernākos rīkus, sevišķi mākslīgo intelektu un datu analīzes tehnoloģijas;

c) veicina labāku aizsardzību un reaģēšanu uz kiberapdraudējumu***, tostarp sniedzot konkrētus ieteikumus vienībām***;

d) veicina kiberapdraudējuma ātrāku atklāšanu un stāvokļa apzināšanos visā Savienībā;

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

To izstrādā sadarbībā ar Eiropas augstas veiktspējas datošanas infrastruktūru, kas izveidota atbilstoši Regulai (ES) 2021/1173.

4. pants

Valstu drošības operāciju centri

1. ***Lai varētu piedalīties*** Eiropas kibervairogā, katra dalībvalsts norīko vismaz vienu savu DOC. Valsts DOC ir ***centralizēta struktūrvienība*** publiskā sektora ***struktūrā***. ***Ja iespējams, valstu DOC iekļauj CSIRT vai citās pastāvošās kiberdrošības infrastruktūrās un pārvaldībā.***

Tam ir spēja būt par uzziņas avotu un vārteju citām publiskām un privātām organizācijām valsts līmenī, ***jo īpaši to DOC,*** lai vāktu un analizētu informāciju par kiberdrošības apdraudējumu un incidentiem***, attiecīgā gadījumā kopīgojot šo infromāciju ar CSIRT tīkla biedriem minētajā dalībvalstī,*** un sekmētu pārrobežu DOC izveidi. Tā rīcībā ir pašas modernākās tehnoloģijas, kuras spēj atklāt, apkopot un analizēt datus par kiberdrošības apdraudējumu un incidentiem ***un tos nepieļaut***.

Valsts DOC vai CSIRT var pieprasīt savu valsts kritisko vienību telemetrijas, sensoru vai reģistrēšanas datus no pārvaldītu drošības pakalpojumu sniedzējiem, kas sniedz pakalpojumu kritiskajai vienībai. Minētos datus kopīgo saskaņā ar Savienības datu aizsardzības tiesību aktiem un vienīgi ar mērķi atbalstīt valstu DOC vai CSIRT kiberdrošības apdraudējumu un incidentu atklāšanā un nepieļaušanā.

2. Pēc uzaicinājuma izteikt ieinteresētību Eiropas Kiberdrošības kompetences centrs (*ECCC*) ***var atlasīt*** valstu DOC dalībai ar *ECCC* kopīgā rīku un infrastruktūru iepirkumā. *ECCC* var atlasītajiem valstu DOC piešķirt dotācijas šo rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 50 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet dalībvalsts sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras *ECCC* un valsts DOC noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.

3. Valsts DOC, kas atlasīts saskaņā ar 2. punktu, apņemas pieteikties dalībai pārrobežu DOC divu gadu laikā no dienas, kad rīki un infrastruktūra tiek iegādāti vai kad tas saņem dotācijas finansējumu – atkarībā no tā, kas notiek agrāk. Ja valsts DOC līdz tam laikam nav kļuvis par pārrobežu DOC dalībnieku, tas nav tiesīgs saņemt Savienības papildatbalstu uz šīs regulas pamata.

5. pants

Pārrobežu drošības operāciju centri

1. Mitināšanas konsorcijs, kurā ir vismaz trīs dalībvalstis, ko pārstāv to DOC un kas ir apņēmušās kopīgā darbā koordinēt kiberatklāšanas un kiberapdraudējuma novērošanas darbības, ir tiesīgs piedalīties pārrobežu DOC izveides darbībās. ***Pārrobežu DOC darbības mērķis ir atklāt un analizēt kiberdrošības apdraudējumu, nepieļaut incidentus un atbalstīt kvalitatīvu izlūkdatu sagatavošanu, jo īpaši daloties datos no dažādiem publiskiem un privātiem avotiem, kā arī uzticamā un drošā vidē kopīgojot modernākos rīkus un kopīgi attīstot kiberapdraudējuma atklāšanas, analīzes, profilakses un aizsardzības spējas.***

2. Pēc uzaicinājuma izteikt ieinteresētību *ECCC* ***var atlasīt*** mitināšanas konsorciju dalībai ar *ECCC* kopīgā rīku un infrastruktūru iepirkumā. *ECCC* var mitināšanas konsorcijam piešķirt dotāciju rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 75 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet mitināšanas

konsorcijs sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras *ECCC* un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.

2.a Atkāpjoties no Regulas (ES, Euratom) 2018/1046 176. panta, vienības, kas ir iedibinātas trešās valstīs, kuras nav NVI puses, nepiedalās kopīgajā rīku un infrastruktūru iepirkumā.

3. Mitināšanas konsorcija dalībnieki noslēdz rakstisku konsorcija nolīgumu, kurā izklāstīta iekšējā kārtība mitināšanas un izmantošanas līguma īstenošanai.

4. Likuma priekšā pārrobežu DOC pārstāv valsts DOC, kas darbojas kā koordinācijas DOC, vai mitināšanas konsorcijs, ja tas ir juridiska persona. Koordinācijas DOC atbild par mitināšanas un izmantošanas līguma un šīs regulas prasību izpildi.

6. pants

Sadarbība un informācijas apmaiņa pārrobežu DOC ietvaros un starpā

1. Mitināšanas konsorcija dalībnieki savā starpā apmainās ar būtisku informāciju pārrobežu DOC ietvaros, ieskaitot informāciju par kiberapdraudējumu, gandrīz notikušiem incidentiem, vājajām vietām, metodēm un procedūrām, aizskāruma rādītājiem, apdraudētāju taktiku, specifiskas ziņas par apdraudētājiem, kiberdrošības brīdinājumus un ieteikumus par kiberdrošības rīku konfigurāciju kiberuzbrukumu atklāšanai, ja informācijas apmaiņa:

a) ***uzlabo kiberapdraudējuma izlūkdatu apmaiņu starp valstu un pārrobežu DOC un nozares ISAC, lai nepieļautu, atklātu vai mazinātu apdraudējumu;***

b) un uzlabo kiberdrošību, sevišķi – paplašinot informētību par kiberapdraudējumu, ierobežojot vai iegrožojot apdraudējuma spēju izplatīties, atbalstot virkni aizsardzības spēju, vājo vietu izlabošanu un uzrādīšanu, apdraudējuma atklāšanas, savaldīšanas un novēršanas metodes, mazināšanas stratēģijas vai reaģēšanas un atkopšanās posmus vai veicinot publiskā un privātā sektora sadarbību kiberapdraudējuma izpētē.

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

a) apņemšanos kopīgot ***būtiskus 1. punktā minētos datus*** un nosacījumus, kuriem atbilstīgi ar minēto informāciju jāmainās;

b) pārvaldes sistēmu, kas stimulē dalīšanos informācijā ar visiem dalībniekiem;

c) mērķrādītājus ieguldījumam progresīvu mākslīgā intelekta un datu analīzes rīku izstrādē.

3. Lai veicinātu informācijas apmaiņu starp pārrobežu DOC ***un nozares ISAC***, pārrobežu DOC nodrošina augsta līmeņa sadarbspēju ***savā starpā un, ja iespējams, ar nozares ISAC***. Lai veicinātu pārrobežu DOC savstarpējo sadarbspēju ***un sadarbspēju ar nozares ISAC, informācijas apmaiņas standartus un protokolus var saskaņot ar starptautiskajiem standartiem un nozares paraugpraksi***. ***Veicina arī kiberinfrastruktūru, pakalpojumu un rīku kopīgu iepirkumu. Turklāt Komisija pēc apspriešanās ar ECCC un ENISA ir***

pilnvarota līdz ... [seši mēneši no šīs regulas stāšanās spēkā dienas] pieņemt deleģētos aktus saskaņā ar 20.a pantu, lai šo regulu papildinātu, sīkāk precizējot sadarbspējas nosacījumus***, ciešā sadarbībā ar pārrobežu DOC un pamatojoties uz starptautiskiem standartiem un nozares paraugpraksi***.

4. Pārrobežu DOC cits ar citu ***un attiecīgā gadījumā ar nozares ISAC*** noslēdz sadarbības nolīgumus, kuros nosaka pārrobežu platformu informācijas kopīgošanas ***un sadarbspējas*** principus***, ņemot vērā jau pastāvošos attiecīgos informācijas apmaiņas mehānismus, kas paredzēti Direktīvā (ES) 2022/2555***. ***Attiecīgā gadījumā pārrobežu DOC slēdz sadarbības līgumus ar nozares ISAC. Potenciāla vai notiekoša liela mēroga kiberdrošības incidenta kontekstā informācijas apmaiņas mehānismi atbilst attiecīgajiem Direktīvas (ES) 2022/2555 noteikumiem.***

7. pants

Sadarbība un dalīšanās informācijā ar *CSIRT tīklu*

1. Ja pārrobežu DOC ***kopīgas situācijas apzināšanās nolūkā*** iegūst informāciju par potenciālu vai notiekošu liela mēroga kiberdrošības incidentu, ***koordinējošais DOC*** bez liekas kavēšanās sniedz attiecīgo informāciju ***savai CSIRT vai kompetentajai iestādei, kas par to tālāk ziņo*** *EU-CyCLONe*, *CSIRT* tīklam***,*** Komisijai ***un ENISA atbilstīgi*** to ***attiecīgajām*** krīzes pārvarēšanas ***funkcijām un procedūrām*** saskaņā ar Direktīvu (ES) 2022/2555. ***Šis punkts neuzliek papildu pienākumus publiskām vai privātām struktūrām ziņot par potenciālu vai notiekošu liela mēroga kiberdrošības incidentu, lai izpildītu Direktīvā (ES) 2022/2555 noteiktos pienākumus.***

2. Komisija ***tiek pilnvarota pēc apspriešanās ar CSIRT tīklu pieņemt deleģētos aktus saskaņā ar 20.a pantu, lai šo regulu papildinātu, paredzot šā panta*** 1. punktā noteiktās informācijas kopīgošanas kārtību ***saskaņā ar Direktīvu (ES) 2022/2555***.

8. pants

Drošība

1. Dalībvalstis, kuras piedalās Eiropas kibervairogā, Eiropas kibervairoga infrastruktūrai nodrošina ***augsta līmeņa konfidencialitāti,*** datu drošību un fizisko drošību un gādā, lai infrastruktūra tiek pienācīgi pārvaldīta un kontrolēta, to sargājot no apdraudējuma un nodrošinot tās un sistēmu drošību, ieskaitot to datu drošību, ar kuriem infrastruktūrā notiek apmaiņa.

2. Dalībvalstis, kuras piedalās Eiropas kibervairogā, nodrošina, ka informācijas kopīgošana Eiropas kibervairogā ar vienībām, kuras nav dalībvalstu publiskās struktūras, negatīvi neietekmē Savienības drošības intereses.

3. Komisija var pieņemt īstenošanas aktus, nosakot tehniskās prasības dalībvalstīm 1. un 2. punktā noteikto pienākumu izpildei. Minētos īstenošanas aktus pieņem saskaņā ar šīs regulas 21. panta 2. punktā minēto pārbaudes procedūru. ***Tie atbilst Direktīvām (ES) 2022/2555 un***

(ES) 2022/2557. Savos īstenošanas aktos Komisija ar Augstā pārstāvja atbalstu ievēro attiecīgā aizsardzības līmeņa drošības standartus, lai veicinātu sadarbību ar militārām iestādēm.

III nodaļa

KIBERDROŠĪBAS ĀRKĀRTAS MEHĀNISMS

9. pants

Kiberdrošības ārkārtas **mehānisma izveide**

1. Lai uzlabotu Savienības noturību pret ievērojamu kiberdrošības apdraudējumu un solidāri sagatavotos būtisku un liela mēroga kiberdrošības incidentu īslaicīgai ietekmei un to mazinātu, tiek izveidots ***kiberdrošības ārkārtas*** mehānisms (“mehānisms”).

2. ▌ Mehānisma īstenošanas darbības atbalsta ar finansēm no programmas “Digitālā Eiropa” un īsteno saskaņā ar Regulu (ES) 2021/694, sevišķi tās konkrēto mērķi Nr. 3.

10. pants

Darbību veidi

1. Mehānisms atbalsta šādas darbības:

a) gatavības darbības, ieskaitot koordinētas gatavības pārbaudes visā Savienībā vienībām, kuras darbojas sevišķi kritiskās nozarēs;

b) reaģēšanas darbības, kas atbalsta reaģēšanu uz būtiskiem un liela mēroga kiberdrošības incidentiem un tūlītēju atkopšanos pēc tiem un kas jāveic uzticamiem ***pārvaldītu drošības pakalpojumu*** sniedzējiem, kuri piedalās ES kiberdrošības rezervēs, kas izveidotas ar 12. pantu;

c) savstarpējas palīdzības darbības, kas ietver palīdzības sniegšanu no vienas dalībvalsts valsts iestādēm citai dalībvalstij, sevišķi tā, kā noteikts Direktīvas (ES) 2022/2555 11. panta 3. punkta f) apakšpunktā.

1.a Pēc mehānisma iedarbināšanas Komisija katru gadu izvērtē mehānisma pozitīvo un negatīvo darbību un publicē par to ziņojumu, cita starpā norādot, vai ir vajadzīga turpmāka sadarbība vai apmācība.

11. pants

Koordinētas vienību gatavības pārbaudes

1. Lai visā Savienībā atbalstītu koordinētas 10. panta 1. punkta a) apakšpunktā minēto vienību gatavības pārbaudes, Komisija pēc apspriešanās ar TID sadarbības grupu un *ENISA* nosaka attiecīgās nozares vai apakšnozares no Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajām sevišķi kritiskajām nozarēm, kuru vienības var pakļaut koordinētai gatavības pārbaudei, ņemot vērā iegūtos un plānotos koordinētos riska novērtējumus un noturības pārbaudes Savienības līmenī***, saskaņā ar kārtību, kas paredzēta tām vienībām, kuras darbojas Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajās sevišķi kritiskajās nozarēs***.

2. TID sadarbības grupa sadarbībā ar Komisiju, *ENISA*, Augsto pārstāvi ***un vienībām, kam saskaņā ar 1. punktu piemēro koordinētas gatavības pārbaudes,*** izstrādā kopīgus riska scenārijus un metodiku koordinētajiem ***gatavības*** pārbaudes pasākumiem***, uz kuru pamata izstrādā saskaņotu darba plānu***. ***Vienības, kurām piemēro koordinētās gatavības pārbaudes, izstrādā un īsteno sanācijas plānu, kurā sniegti ieteikumi, kas izriet no gatavības pārbaužu rezultātiem.***

TID sadarbības grupa var sniegt informāciju par nozaru vai apakšnozaru prioritāšu noteikšanu koordinētajiem gatavības pārbaudes pasākumiem.

12. pants

ES kiberdrošības rezervju izveide

1. Lai palīdzētu 3. punktā minētajiem lietotājiem reaģēt vai atbalstīt reaģēšanu uz būtiskiem vai liela mēroga kiberdrošības incidentiem, kā arī tūlīt atkopties no tādiem incidentiem, tiek izveidotas ES kiberdrošības rezerves.

Ja izrādās, ka iepirktos pakalpojumus nevar pilnībā izmantot, lai sniegtu atbalstu reaģēšanai uz būtiskiem vai liela mēroga incidentiem, šos pakalpojumus izņēmuma kārtā var pārveidot par mācībām vai apmācību incidentu risināšanai, un līgumslēdzēja iestāde tos pēc pieprasījuma var sniegt lietotājiem.

2. ES kiberdrošības rezerves veido reaģēšanas uz incidentiem pakalpojumi no uzticamiem ***pārvaldītu drošības*** pakalpojumu sniedzējiem, kas atlasīti pēc 16. pantā noteiktajiem kritērijiem. ***ES kiberdrošības*** rezervēs ietilpst pakalpojumi, par kuriem iepriekš uzņemtas saistības. Pakalpojumi ir sniedzami visās dalībvalstīs***, un tie stiprina Savienības tehnoloģisko suverenitāti, tās atvērto stratēģisko autonomiju, konkurētspēju un noturību kiberdrošības nozarē, tostarp veicinot inovāciju visas Savienības digitālajā vienotajā tirgū***.

3. ES kiberdrošības rezervju pakalpojumu lietotāju vidū ir:

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

b) Savienības iestādes, struktūras un aģentūras***, kā minēts Eiropas Parlamenta un Padomes Regulas (ES) .../2023[1] 3. panta 1) punktā, un CERT-EU***.

[1] ***Regula (ES) .../2023, ar ko paredz pasākumus nolūkā panākt vienādi augsta līmeņa kiberdrošību Savienības iestādēs, struktūrās, birojos un aģentūrās (OV C ..., ..., ... lpp., ELI: ...).***

4. Šā panta 3. punkta a) apakšpunktā minētie lietotāji izmanto ES kiberdrošības rezervju pakalpojumus, lai reaģētu vai atbalstītu reaģēšanu uz būtiskiem vai liela mēroga incidentiem, kas ietekmē vienības, kuras darbojas kritiskās vai sevišķi kritiskās nozarēs, un tūlītēju atkopšanos no tiem.

5. Komisijai ir vispārēja atbildība par ES kiberdrošības rezerves īstenošanu. Komisija ***sadarbībā ar TID2 koordinācijas grupu*** nosaka ES kiberdrošības rezervju prioritātes un attīstību saskaņā ar 3. punktā minēto lietotāju prasībām un uzrauga to īstenošanu, kā arī nodrošina savstarpēju papildināmību, konsekvenci, sinerģiju un saikni ar citām atbalsta darbībām saskaņā ar šo regulu, kā arī citām Savienības darbībām un programmām.

6. Komisija ES kiberdrošības rezervju darbību un administrēšanu ▌ ar iemaksu nolīgumiem pilnīgi vai daļēji ***uztic*** *ENISA*.

7. Lai atbalstītu Komisiju ES kiberdrošības rezervju izveidē, *ENISA* pēc apspriešanās ar dalībvalstīm un Komisiju sagatavo ***kartējumu par vajadzīgajiem pakalpojumiem, tostarp vajadzīgajām kiberdrošības jomā strādājošo prasmēm un spējām, un attiecīgā gadījumā pārvaldītu drošības pakalpojumu sniedzējiem, kā arī citiem kiberdrošības nozares pārstāvjiem***. Pēc apspriešanās ar Komisiju *ENISA* sagatavo līdzīgu kartējumu, ***kas ietver pārvaldītu drošības pakalpojumu sniedzējus un attiecīgā gadījumā citus kiberdrošības nozares pārstāvjus,*** lai apzinātu to trešo valstu vajadzības, kuras ir tiesīgas uz atbalstu no ES kiberdrošības rezervēm saskaņā ar 17. pantu. Attiecīgā gadījumā Komisija apspriežas ar Augsto pārstāvi ***un informē Padomi par trešo valstu vajadzībām***.

8. Komisija ***tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 20.a pantu, lai šo regulu papildinātu, precizējot*** ES kiberdrošības rezervēm nepieciešamo reaģēšanas pakalpojumu veidus un skaitu. ▌..

13. pants

ES kiberdrošības rezervju atbalsta pieprasījumi

1. Šīs regulas 12. panta 3. punktā minētie lietotāji var no ES kiberdrošības rezervēm pieprasīt pakalpojumus, kas atbalstītu reaģēšanu uz būtiskiem vai liela mēroga kiberdrošības incidentiem un tūlītēju atkopšanos no tiem.

2. Lai saņemtu atbalstu no ES kiberdrošības rezervēm, 12. panta 3. punktā minētie lietotāji veic pasākumus, kas mazina tā incidenta sekas, par kuru tiek pieprasīts atbalsts, ieskaitot tiešas tehniskās palīdzības un citu resursu sniegšanu, lai palīdzētu reaģēt uz incidentu, un tūlītējas atkopšanas pasākumus.

3. Šīs regulas 12. panta 3. punkta a) apakšpunktā minēto lietotāju atbalsta pieprasījumus nosūta Komisijai un *ENISA* caur vienoto kontaktpunktu, ko dalībvalsts norīkojusi vai nodibinājusi saskaņā ar Direktīvas (ES) 2022/2555 8. panta 3. punktu.

4. Par saskaņā ar šo pantu iesniegtajiem pieprasījumiem reaģēt uz incidentu un atbalstīt tūlītēju atkopšanu dalībvalstis informē *CSIRT* tīklu un attiecīgā gadījumā *EU-CyCLONe*.

5. Pieprasījumā reaģēt uz incidentu un atbalstīt tūlītēju atkopšanu ir:

a) atbilstoša informācija par skarto vienību un incidenta iespējamo ietekmi, un pieprasītā atbalsta plānoto izmantošanu, ieskaitot norādi par aplēstajām vajadzībām;

b) informācija par pasākumiem, kas veikti, lai mazinātu incidentu, par kuru tiek pieprasīts atbalsts, kā minēts 2. punktā;

c) informācija par citādu atbalstu, kas pieejams skartajai vienībai, ieskaitot spēkā esošas vienošanās par reaģēšanu uz incidentiem un tūlītējas atkopšanas pakalpojumiem, kā arī apdrošināšanas līgumus, kas potenciāli aptver tāda veida incidentu.

6. *ENISA* sadarbībā ar Komisiju un TID sadarbības grupu izstrādā veidni, lai vienkāršotu ES kiberdrošības rezervju atbalsta pieprasījumu iesniegšanu.

7. Komisija ***tiek pilnvarota pieņemt deleģētos aktus saskaņā ar 20.a pantu, lai šo regulu papildinātu, sīkāk precizējot*** ES kiberdrošības rezervju atbalsta pakalpojumu piešķiršanas kārtību. ▌

14. pants

ES kiberdrošības rezervju atbalsta īstenošana

1. ES kiberdrošības rezervju atbalsta pieprasījumus Komisija izvērtē ar *ENISA* palīdzību vai tā, kā noteikts iemaksu nolīgumos saskaņā ar 12. panta 6. punktu, un atbildi ***bez liekas kavēšanās un katrā ziņā ne vēlāk kā 24 stundu laikā*** nosūta 12. panta 3. punktā minētajiem lietotājiem.

2. Prioritāto pieprasījumu noteikšanas nolūkā, ja vienlaikus saņemti vairāki pieprasījumi, attiecīgi ņemami vērā šādi kritēriji:

a) kiberdrosības incidenta smagums;

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

c) iespējamā ietekme uz skartajām dalībvalstīm vai lietotājiem;

d) incidenta ***apmērs un*** iespējamais pārrobežu raksturs, kā arī risks, ka tas izplatīsies citās dalībvalstīs vai citu lietotāju vidū;

e) pasākumi, ko lietotājs veicis, lai palīdzētu reaģēt, un tūlītējas atkopšanas pasākumi, kas minēti 13. panta 2. punktā un 13. panta 5. punkta b) apakšpunktā.

3. ES kiberdrošības rezervju pakalpojumus sniedz saskaņā ar īpašiem nolīgumiem starp pakalpojumu sniedzēju un lietotāju, kuram tiek sniegts atbalsts no ES kiberdrošības rezervēm. Nolīgumos iekļauj atbildības nosacījumus ***un visus citus noteikumus, ko nolīguma puses uzskata par vajadzīgiem attiecīgā pakalpojuma sniegšanai***.

4. Šā panta 3. punktā minēto nolīgumu pamatā ***ir*** veidnes, ko *ENISA* sagatavojusi pēc apspriešanās ar dalībvalstīm ***un attiecīgā gadījumā citiem ES kiberdrošības rezervju lietotājiem***.

5. Komisija un *ENISA* neuzņemas līgumisku atbildību par kaitējumu, ko trešām personām nodarījuši pakalpojumi, kuri sniegti ES kiberdrošības rezervju īstenošanā***, izņemot gadījumus, kad pakalpojumu sniedzēja pieteikuma izvērtēšanā pieļauta liela nolaidība, vai gadījumā, kad Komisija vai ENISA ir ES kiberdrošības rezervju lietotāji saskaņā ar 14. panta 3. punktu***.

6. Viena mēneša laikā pēc atbalsta darbības beigām lietotāji iesniedz Komisijai***,*** *ENISA****, CSIRT tīklam un attiecīgā gadījumā EU-CyCLONe*** kopsavilkuma ziņojumu par sniegto

pakalpojumu, sasniegtajiem rezultātiem un gūto mācību. Ja lietotājs ir no trešas valsts, kā noteikts 17. pantā, ziņojumu dara zināmu Augstajam pārstāvim.
Ziņojumā ievēro Savienības un valsts tiesību aktus par sensitīvas vai klasificētas informācijas aizsardzību.

7. Komisija regulāri ***un vismaz divas reizes gadā*** ziņo TID sadarbības grupai par atbalsta izmantošanu un rezultātiem. ***Tā aizsargā konfidenciālu informāciju saskaņā ar Savienības vai valstu tiesību normām par sensitīvas vai klasificētas informācijas aizsardzību.***

15. pants

Koordinācija ar krīzes pārvarēšanas mehānismiem

1. Gadījumos, kad būtisku vai liela mēroga kiberdrošības incidentu cēlonis vai sekas ir katastrofa, kas definēta Lēmumā Nr. 1313/2013/ES[1], šajā regulā paredzētais atbalsts reaģēšanai uz tādiem incidentiem papildina Lēmuma Nr. 1313/2013/ES darbības, to neskarot.

2. Liela mēroga pārrobežu kiberdrošības incidenta gadījumā, kad tiek iedarbināti integrēti krīzes situāciju politiskās reaģēšanas mehānismi (*IPCR*), šajā regulā paredzēto atbalstu reaģēšanai uz tādu incidentu sniedz saskaņā ar attiecīgajiem *IPCR* protokoliem un procedūrām.

3. Apspriežoties ar Augsto pārstāvi, ***kiberdrošības ārkārtas*** mehānisma atbalsts var papildināt palīdzību, ko sniedz kopīgajā ārpolitikā un drošības politikā un kopīgajā drošības un aizsardzības politikā, arī caur kiberdrošības ātrās reaģēšanas vienībām. Tas var arī papildināt vai veicināt palīdzību, ko dalībvalsts sniedz citai dalībvalstij uz ***LES*** 42. panta 7. punkta pamata.

4. ***Kiberdrošības ārkārtas*** mehānisma atbalsts var ietilpt Savienības un dalībvalstu kopīgajā reaģēšanā LESD 222. pantā minētajos apstākļos.

16. pants

Uzticami pakalpojumu sniedzēji

1. Iepirkuma procedūrās ES kiberdrošības rezervju izveidei līgumslēdzēja iestāde rīkojas saskaņā ar Regulā (ES, *Euratom*) 2018/1046 noteiktajiem principiem un saskaņā ar šādiem principiem:

a) nodrošināt, ka ES kiberdrošības rezerves ietver pakalpojumus, kurus var ieviest visās dalībvalstīs, īpaši ņemot vērā valsts prasības, kas attiecas uz tādu pakalpojumu sniegšanu, ieskaitot sertifikāciju vai akreditāciju;

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

c) nodrošināt, ka ES kiberdrošības rezerves rada ES pievienoto vērtību, sekmējot Regulas (ES) 2021/694 3. panta mērķu sasniegšanu, tostarp veicinot kiberdrošības prasmju attīstību ES***, un dzimumu līdzsvara panākšanu nozarē, un stiprinot Savienības tehnoloģisko suverenitāti, atvērtu stratēģisko autonomiju, konkurētspēju un noturību***.

[1] 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.).

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

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

b) pakalpojumu sniedzējs, tā meitasuzņēmumi un apakšuzņēmēji izveido sistēmu, lai aizsargātu sensitīvu informāciju, kas saistīta ar pakalpojumu, sevišķi pierādījumus, konstatējumus un ziņojumus, un ievēro Savienības drošības noteikumus par slepenotas ES informācijas aizsardzību;

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;

e) pakalpojumu sniedzējam ir attiecīgais IT sistēmu drošības līmenis;

f) pakalpojumu sniedzējs ir aprīkots ar pieprasītajam pakalpojumam nepieciešamo ***modernāko*** aparatūru un programmatūras tehnisko aprīkojumu ***un attiecīgā gadījumā atbilst Eiropas Parlamenta un Padomes Regulas (ES) .../...[1] (2022/0272(COD)) prasībām***;

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

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

i) pakalpojumu sniedzējs spēj pakalpojumu sniegt to dalībvalstu vietējā valodā ***vai vienā no to Savienības iestāžu darba valodām***, kurās tas var pakalpojumu nodrošināt;

j) kad ir ieviesta ***Eiropas kiberdrošības*** sertifikācijas shēma ***pārvaldītiem*** drošības ***pakalpojumiem saskaņā ar Regulu*** (ES) 2019/881, pakalpojumu sniedzējs tiek sertificēts pēc minētās shēmas ***divu gadu laikā pēc shēmas pieņemšanas***.

ja) pakalpojumu sniedzējs spēj sniegt pakalpojumu neatkarīgi, nevis kā komplekta daļu, tādējādi saglabājot lietotāja iespēju pāriet pie cita pakalpojumu sniedzēja;

jb) piemērojot 12. panta 1. punktu, pakalpojumu sniedzējs piedāvājuma priekšlikumā iekļauj iespēju neizmantotos incidentu reaģēšanas pakalpojumus pārvērst mācību vai apmācības pakalpojumos;

jc) pakalpojumu sniedzējs ir iedibināts Savienībā, un tā vadības izpildstruktūras atrodas Savienībā, asociētā valstī vai trešā valstī, kas ir Nolīguma par valsts iepirkumu (NVI) puse Pasaules Tirdzniecības organizācijas kontekstā;

jd) . pakalpojumu sniedzēju nekontrolē neasociēta trešā valsts vai neasociētas trešās valsts vienība, kas nav NVI puse, vai arī tādai vienībai ir veikta izvērtēšana Regulas (ES) 2019/452 nozīmē un vajadzības gadījumā ir veikti seku mazināšanas pasākumi,

[1] Eiropas Parlamenta un Padomes Regula (ES) .../... (… gada …) (OV L ..., ELI: ...).

ņemot vērā šajā regulā izvirzītos mērķus.

17. pants

Atbalsts trešām valstīm

1. Trešas valstis var pieprasīt ES kiberdrošības rezervju atbalstu, ja to paredz asociācijas nolīgumi, kas noslēgti par to dalību programmā "Digitālā Eiropa".

2. Atbalsts no ES kiberdrošības rezervēm ir saskaņā ar šo regulu un atbilst 1. punktā minēto asociācijas nolīgumu īpašajiem nosacījumiem.

3. Lietotājos no asociētajām trešām valstīm, kam ir tiesības saņemt pakalpojumus no ES kiberdrošības rezervēm, ietilpst kompetentās iestādes, kā *CSIRT* un kiberkrīzes pārvaldības iestādes.

4. Ikkatra treša valsts, kas tiesīga prasīt atbalstu no ES kiberdrošības rezervēm, norīko iestādi, kura šīs regulas izpildē būs vienots kontaktpunkts.

5. Pirms atbalsta saņemšanas no ES kiberdrošības rezervēm trešās valstis sniedz Komisijai un Augstajam pārstāvim informāciju par savu kibernoturību un riska pārvaldības spējām, ieskaitot vismaz informāciju par valsts pasākumiem, kas veikti, lai sagatavotos būtiskiem vai liela mēroga kiberdrošības incidentiem, kā arī informāciju par atbildīgajām valsts vienībām, to vidū *CSIRT* vai līdzvērtīgām vienībām, to spējām un tām piešķirtajiem resursiem. Ja šīs regulas 13. un 14. panta noteikumi attiecas uz dalībvalstīm, tos piemēro trešām valstīm tā, kā noteikts 1. punktā.

6. Komisija ***bez liekas kavēšanās informē Padomi un*** ar Augsto pārstāvi koordinē darbību saistībā ar saņemtajiem pieprasījumiem un no ES kiberdrošības rezervēm trešām valstīm piešķirtā atbalsta īstenošanu.

IV nodaļa

KIBERDROŠĪBAS INCIDENTU IZSKATĪŠANAS MEHĀNISMS

18. pants

Kiberdrošības incidentu izskatīšanas mehānisms

1. Pēc Komisijas, *EU-CyCLONe* vai *CSIRT* tīkla pieprasījuma *ENISA* izskata un novērtē apdraudējumu, vājās vietas un seku mazināšanas darbības, kas attiecas uz konkrētu būtisku vai liela mēroga kiberdrošības incidentu. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* iesniedz incidenta pārskata ziņojumu *CSIRT* tīklam, *EU-CyCLONe* un Komisijai, lai palīdzētu tiem veikt to uzdevumus, sevišķi Direktīvas (ES) 2022/2555 15. un 16. pantā noteiktos uzdevumus. Attiecīgā gadījumā Komisija ziņojumu iesniedz Augstajam pārstāvim.

2. Lai sagatavotu 1. punktā minēto incidentu pārskata ziņojumu, *ENISA* sadarbojas ar ***un apkopo atsauksmes no*** visām attiecīgajām ieinteresētajām personām, ieskaitot dalībvalstu, Komisijas, citu attiecīgo ES iestāžu, struktūru***, biroju*** un aģentūru pārstāvjus, ***valstu un pārrobežu DOC*** pārvaldīto drošības pakalpojumu sniedzējus un kiberdrošības pakalpojumu

lietotājus***, un izmanto arī garantijas un uzraudzību, kas vajadzīga, lai nodrošinātu, ka kiberdrošības pakalpojumu nozares dalībnieki atbalsta gūtās atziņas un identificēto paraugpraksi***. Attiecīgā gadījumā *ENISA* sadarbojas arī ar būtisku vai liela mēroga kiberdrošības incidentu skartām vienībām. Lai atbalstītu izskatīšanu, *ENISA* var konsultēties arī ar citādām ieinteresētām personām. Pārstāvji, ar kuriem konsultējas, dara zināmus iespējamos interešu konfliktus.

3. Ziņojumā iekļauj konkrētā būtiskā vai liela mēroga kiberdrošības incidenta pārskatu un analīzi, aptverot galvenos cēloņus, vājās vietas un gūto mācību. Saskaņā ar Savienības vai valstu tiesību normām par jutīgas vai slepenotas informācijas aizsardzību tajā aizsargā konfidenciālu informāciju. ***Tajā neiekļauj nekādu informāciju par aktīvi izmantotām vājajām vietām, kuru ievainojamība joprojām nav novērsta.***

3.a Šā panta 1. punktā minētajā ziņojumā iekļauj atziņas, kas gūtas saskaņā ar Direktīvas (ES) 2022/2555 19. pantu veiktajā salīdzinošajā izvērtēšanā.

4. Attiecīgā gadījumā ziņojumā sniedz konkrētus ieteikumus***, tostarp visām attiecīgajām ieinteresētajām personām,*** Savienības pozīcijas uzlabošanai kiberjautājumos;

5. Ja iespējams, ziņojuma redakciju dara pieejamu atklātībā. Redakcijā iekļauj tikai publisku informāciju.

V nodaļa

NOBEIGUMA NOTEIKUMI

19. pants

Grozījumi Regulā (ES) 2021/694

Regulu (ES) 2021/694 groza šādi:

(1) regulas 6. pantu groza šādi:

a) 1. punktu groza šādi:

(***i***) iekļauj šādu aa) apakšpunktu:

"aa) atbalstīt ES kibervairoga izstrādi, ieskaitot tādu valsts un pārrobežu DOC platformu izstrādi, ierīkošanu un darbību, kuras veicina stāvokļa apzināšanos Savienībā un uzlabo Savienības kiberapdraudējuma izlūkošanas spējas";

(***ii***) pievieno šādu g) apakšpunktu:

"g) izveidot un izmantot ***kiberdrošības ārkārtas*** mehānismu, kas palīdz dalībvalstīm sagatavoties būtiskiem kiberdrošības incidentiem un uz tiem reaģēt, papildus valstu resursiem un spējām un citiem Savienības līmenī pieejamiem atbalsta veidiem, un izveidot arī ES kiberdrošības rezerves";

b) 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*, izņemot ES kiberdrošības rezervju īstenošanas darbības, ko īsteno Komisija un *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., ***ELI: http://data.europa.eu/eli/reg/2021/887/oj).";***

(2) regulas 9. pantu groza šādi:

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

"b) 1 776 956 000 EUR konkrētajam mērķim Nr. 2 – Mākslīgais intelekts;

c) ***1 620 566 000*** EUR konkrētajam mērķim Nr. 3 – Kiberdrošība un uzticamība;

d) ***500 347 000*** EUR konkrētajam mērķim Nr. 4 – Padziļinātas digitālās prasmes";

aa) iekļauj šādu jaunu 2.a punktu:

"(2a) Šā panta 2. punkta c) apakšpunktā minēto summu galvenokārt izmanto Programmas 6. panta 1. punkta a)–f) apakšpunktā minēto darbības mērķu sasniegšanai.";

ab) iekļauj šādu jaunu 2.b punktu:

"(2b) ES kiberdrošības rezervju izveidei un īstenošanai paredzētā summa nepārsniedz 27 miljonus EUR laikposmam, kurā paredzēts īstenot Regulu, kas nosaka pasākumus, kuri stiprina solidaritāti un spējas Savienībā atklāt kiberdrošības apdraudējumu un incidentus, tiem sagatavoties un uz tiem reaģēt.";

b) pievieno šādu 8. punktu:

"8. Atkāpjoties no Regulas (ES, *Euratom*) 2018/1046 12. panta 4. punkta, neizmantotās saistību un maksājumu apropriācijas darbībām ***ES kiberdrošības rezervju īstenošanas kontekstā***, ar kurām tiek īstenoti šīs regulas 6. panta 1. punkta g) apakšpunktā izklāstītie mērķi, automātiski pārnes uz priekšu, un par tām var uzņemties saistības un samaksāt līdz nākamā finanšu gada 31. decembrim.";

Komisija informē Eiropas Parlamentu un Padomi par apropriācijām, kas pārnestas saskaņā ar Regulas (ES, Euratom) 2018/1046 12. panta 6. punktu.

(3) regulas 14. panta 2. punktu aizstāj ar šādu:

“2. Finansējumu no Programmas var sniegt jebkurā ***Regulā (ES, Euratom) 2018/1046*** noteiktā veidā, arī izmantojot iepirkumu kā galveno finansēšanas veidu, vai 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[27] un 2014/25/ES[28].

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 ar Regulas (ES) 2023***/…*** 12. pantu izveidoto ES kiberdrošības rezervju iepirkuma procedūras, Komisija un *ENISA* var rīkoties kā centralizēto iepirkumu struktūra, iepērkot ar Programmu asociēto trešo valstu uzdevumā vai vārdā saskaņā ar 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 Regulas (ES) ***.../…*** 169. panta 3. punkta, vienas trešās valsts pieprasījums ir pietiekams, lai pilnvarotu Komisiju vai *ENISA* rīkoties.

Īstenojot ar Regulas (ES) 2023/***…*** 12. pantu izveidoto ES kiberdrošības rezervju iepirkuma procedūras, Komisija un *ENISA* var rīkoties kā centralizēto iepirkumu struktūra, iepērkot Savienības iestāžu, struktūru un aģentūru uzdevumā vai vārdā. Komisija un *ENISA* var arī rīkoties kā vairumtirgotājs, pērkot, glabājot un pārdodot tālāk vai ziedojot Savienības iestādēm, struktūrām un aģentūrām preces un pakalpojumus, ieskaitot nomu. Atkāpjoties no Regulas (ES) ***…/…*** 169. panta 3. punkta, vienas Savienības iestādes, struktūras vai aģentūras pieprasījums ir pietiekams, lai pilnvarotu Komisiju vai *ENISA* rīkoties.

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

(4) pievieno šādu 16.a pantu:

“***16.a pants***

Darbībām, kuras īsteno ar Regulas (ES) 2023/XX 3. pantu izveidoto Eiropas kibervairogu, piemērojamie noteikumi ir Regulas (ES) 2023/***…*** 4. un 5. panta noteikumi. Gadījumā, ja šīs regulas noteikumi ir pretrunā Regulas (ES) 2023/***...*** 4. un 5. pantam, noteicošie ir pēdējie un tos piemēro minētajām konkrētajām darbībām.***”;***

(5) regulas 19. pantu aizstāj ar šādu:

"Programmas dotācijas piešķir un pārvalda saskaņā ar ***Regulas (ES, Euratom) 2018/1046*** VIII sadaļu, un ar tām var segt līdz 100 % attiecināmo izmaksu, neskarot Finanšu ***Regulas (ES, Euratom) 2018/1046*** 190. pantā noteikto līdzfinansēšanas principu. Tādas dotācijas piešķir un pārvalda tā, kā noteikts katram konkrētajam mērķim.

Regulas ***(ES) .../...*** 4. pantā minētajiem valstu DOC un Regulas ***(ES) .../...*** 5. pantā minētajam mitināšanas konsorcijam atbalstu dotāciju veidā *ECCC* var saskaņā ar ***Regulas (ES, Euratom) 2018/1046*** 195. panta 1. punkta d) apakšpunktu tieši piešķirt bez uzaicinājuma iesniegt priekšlikumus.

Atbalstu dotāciju veidā ***kiberdrošības ārkārtas*** mehānismam, kas noteikts Regulas ***(ES) .../...*** 10. pantā, *ECCC* var saskaņā ar ***Regulas (ES, Euratom) 2018/1046*** 195. panta 1. punkta d) apakšpunktu tieši piešķirt dalībvalstīm bez uzaicinājuma iesniegt priekšlikumus.

Sakarā ar Regulas ***(ES) .../...*** 10. panta 1. punkta c) apakšpunktā minētajām darbībām *ECCC* informē Komisiju un *ENISA* par dalībvalstu tiešo dotāciju pieprasījumiem bez uzaicinājuma iesniegt priekšlikumus.

Lai atbalstītu savstarpēju palīdzību reaģēšanai uz būtisku vai liela mēroga kiberdrošības incidentu, kas definēts Regulas ***(ES) .../...*** 10. panta c) punktā, un saskaņā ar ***Regulas (ES, Euratom) 2018/1046*** 193. panta 2. punkta otrās daļas a) apakšpunktu pienācīgi pamatotos gadījumos par attiecināmām var uzskatīt arī izmaksas, kas radušās pirms dotācijas pieteikuma iesniegšanas.";

(6) Regulas (ES) 2021/694 I un II pielikumu groza saskaņā ar šīs regulas pielikumu.

19.a pants
Papildu resursi ENISA vajadzībām

ENISA saņem papildu resursus, lai veiktu savus papildu uzdevumus, kas tai uzticēti ar šo regulu. Minētais papildu atbalsts, tostarp finansējums, neapdraud citu Savienības programmu, jo īpaši programmas "Digitālā Eiropa", mērķu sasniegšanu.

20. pants

Izvērtēšana ***un pārskatīšana***

1. [***Divus*** gadus ***no*** šīs regulas piemērošanas sākuma datuma] ***un turpmāk reizi divos gados*** Komisija ***izvērtē šajā regulā noteikto pasākumu darbību un iesniedz ziņojumu*** Eiropas Parlamentam un Padomei.

2. Izvērtēšanā jo īpaši vērtē:

a) pārrobežu DOC izmantošanu un pievienoto vērtību, kā arī to, cik lielā mērā tie palīdz ātrāk atklāt kiberapdraudējumu un uz to reaģēt, kā arī apzināties situāciju; valstu DOC aktīvu līdzdalību Eiropas kibervairogā, tostarp izveidoto valstu DOC un pārrobežu DOC skaitu un to, cik lielā mērā tas ir veicinājis praksē izmantojamas augstas kvalitātes informācijas un kiberapdraudējuma izlūkdatu sagatavošanu un apmaiņu; kopējā iepirkuma rezultātā izveidoto kiberdrošības infrastruktūru vai iegūto rīku, vai abu minēto skaitu; to sadarbības nolīgumu skaitu, kas noslēgti starp pārrobežu DOC un nozares ISAC; CSIRT tīklam paziņoto incidentu skaitu un to ietekmi uz CSIRT tīkla darbību;

b) kiberdrošības ārkārtas mehānisma pozitīvo un negatīvo darbību, tostarp to, vai ir vajadzīga turpmāka sadarbība vai apmācība;

c) šīs regulas devumu Savienības noturības un atvērtas stratēģiskās autonomijas stiprināšanā, attiecīgo rūpniecības nozaru, mikrouzņēmumu un MVU, tostarp jaunuzņēmumu, konkurētspējas uzlabošanā un kiberdrošības prasmju attīstīšanā ES;

d) ES kiberdrošības rezervju izmantošanu un pievienoto vērtību, tostarp uzticamu drošības pakalpojumu sniedzēju skaitu ES kiberdrošības rezervēs; to darbību skaitu, veidu, izmaksas un ietekmi, kas veiktas, lai atbalstītu reaģēšanu uz kiberdrošības incidentiem, kā arī minēto pakalpojumu lietotājus un sniedzējus; vidējo laiku, kas Komisijai vajadzīgs apstiprināšanai, ES kiberdrošības rezervēm — reaģēšanai un lietotājiem — lai atkoptos no incidentiem; to, vai ES kiberdrošības rezervju darbības joma būtu jāpaplašina, iekļaujot arī gatavības incidentiem pakalpojumus vai kopīgus pasākumus ar uzticamiem pārvaldītu drošības pakalpojumu sniedzējiem un potenciālajiem ES kiberdrošības rezervju lietotājiem, lai vajadzības gadījumā nodrošinātu ES kiberdrošības rezervju efektīvu darbību;

e) šīs regulas devumu to kiberdrošības nozares darbaspēka prasmju un kompetenču attīstīšanā un uzlabošanā, kas vajadzīgas, lai stiprinātu Savienības spēju atklāt un nepieļaut kiberdrošības apdraudējumus un incidentus, reaģēt uz tiem un atgūties no tiem;

f) šīs regulas devumu modernāko tehnoloģiju ieviešanā un attīstībā Savienībā.

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

20.a pants

Deleģēšanas īstenošana

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

2. Pilnvaras pieņemt 6. panta 3. punktā, 7. panta 2. punktā, 12. panta 8. punktā un 13. panta 7. punktā minētos deleģētos aktus Komisijai piešķir uz ... gadiem no ... [leģislatīvā pamatakta spēkā stāšanās diena vai cita abu likumdevēju noteikta diena]. Komisija sagatavo ziņojumu par pilnvaru deleģēšanu vēlākais deviņus mēnešus pirms ... gadu laikposma beigām. Pilnvaru deleģēšana tiek automātiski pagarināta uz tāda paša ilguma laikposmiem, ja vien Eiropas Parlaments vai Padome neiebilst pret šādu pagarinājumu vēlākais trīs mēnešus pirms katra laikposma beigām.

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 6. panta 3. punktā, 7. panta 2. punktā, 12. panta 8. punktā un 13. 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 6. panta 3. punktu, 7. panta 2. punktu, 12. panta 8. punktu un 13. 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].

21. pants

Komiteju procedūra

1. Komisijai palīdz Programmas “Digitālā Eiropa” koordinācijas komiteja, kas izveidota ar Regulu (ES) 2021/694. 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.

22. 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.

Strasbūrā,

Eiropas Parlamenta vārdā — priekšsēdētāja	*Padomes vārdā — priekšsēdētājs*

PIELIKUMS

Regulu (ES) 2021/694 groza šādi:

(1) I pielikuma iedaļu/nodaļu "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 sargātu Savienības digitālo ekonomiku, sabiedrību un demokrātiju, stiprinot Savienības kiberdrošības rūpniecisko potenciālu un konkurētspēju, kā arī uzlabojot gan privātā, gan publiskā sektora spēju pasargāt pilsoņus un uzņēmumus no kiberapdraudējuma, cita starpā atbalstot Direktīvas (ES) 2016/1148 īstenošanu.

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

1. Ar dalībvalstīm kopīgi ieguldījumi progresīvā kiberdrošības aprīkojumā, infrastruktūrās un zinātībā, kas ir būtiski, lai kritiskās infrastruktūras un digitālo vienoto tirgu aizsargātu kopumā. Tādi kopīgi ieguldījumi var būt ieguldījumi kvantiskās iekārtās un datu resursos kiberdrošības un stāvokļa apzināšanās kibertelpā vajadzībām, ***ieskaitot valstu DOC un pārrobežu DOC, kas veido Eiropas kibervairogu***, 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, arī 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 novēršanai***, īpašu uzmanību pievēršot dzimumu līdzsvara panākšanai nozarē***, piemēram, saskaņojot kiberdrošības prasmju programmas, tās pielāgojot specifiskām nozaru vajadzībām***, tostarp īstenojot starpdisciplināru un vispārēju ievirzi,*** un atvieglojot piekļuvi mērķtiecīgām specializētām apmācībām***, lai ļautu visām personām un teritorijām gūt labumu no šajā regulā paredzētajām iespējām***.

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

(2) II pielikuma iedaļu/nodaļu "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***, kas veido kiberdrošības vairoga daļu***.

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

3.3. To darbību skaits***, veids, izmaksas un ietekme, kuras veiktas, lai sekmētu*** gatavību kiberdrošības incidentiem un reaģēšanu uz tiem atbilstīgi ***kiberdrošības ārkārtas*** mehānismam. ***Tas, cik lielā mērā lietotājs ir īstenojis gatavības pārbaužu ieteikumus, kā arī vidējais laiks, kas Komisijai vajadzīgs apstiprināšanai, ES kiberdrošības rezervēm — reaģēšanai un lietotājam — lai atkoptos no incidentiem.”***