Eiropas Savienības
Padome

Briselē, 2023. gada 20. aprīlī
(OR. en)

8512/23

Starpiestāžu lieta:
2023/0109 (COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

PRIEKŠLIKUMS

Sūtītājs:	Eiropas Komisijas ģenerālsekretāre, parakstījusi direktore *Martine DEPREZ*
Saņemšanas datums:	2023. gada 19. aprīlis
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretāre *Thérèse BLANCHET*
K-jas dok. Nr.:	COM(2023) 209 final
Temats:	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

Pielikumā ir pievienots dokuments COM(2023) 209 *final*.

Pielikumā: COM(2023) 209 *final*

EIROPAS
KOMISIJA

Strasbūrā, 18.4.2023.
COM(2023) 209 final

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

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Šis paskaidrojuma raksts ir pievienots Kibersolidaritātes akta priekšlikumam. Laikā, kad mūsu publiskās pārvaldes iestādes, uzņēmumi un iedzīvotāji ir cits ar citu pāri nozarēm un robežām saistīti un savstarpēji atkarīgi vairāk nekā jebkad agrāk, informācijas un komunikācijas tehnoloģiju lietošana un paļaušanās uz tām ir kļuvušas par fundamentāliem aspektiem visās saimnieciskās darbības jomās. Tāda plašāka digitālo tehnoloģiju ieviešana palielina pakļautību kiberdrošības incidentiem un to iespējamo ietekmi. Tajā pašā laikā dalībvalstis saskaras ar augošiem kiberdrošības riskiem un tādu apdraudējumu loku, kas kopumā ir komplekss, un pastāv acīmredzams risks, ka kiberincidentu sekas varētu strauji izplatīties no vienas dalībvalsts uz citām.

Turklāt kiberoperācijas arvien vairāk tiek integrētas hibrīdstratēģijā un militārajā stratēģijā, kas uz mērķi atstāj smagas sekas. Tā, pirms Krievijas militārās agresijas pret Ukrainu tika īstenota naidīgu kiberoperāciju stratēģija, kas turpinās vēl šobrīd, un tas maina izpratni un novērtējumu par ES kolektīvo gatavību pārvarēt kiberdrošības krīzes un ir pamudinājums steidzami rīkoties. Draudi, ka var notikt plašs incidents, kas radītu būtiskus traucējumus un kaitējumu kritiskajai infrastruktūrai, prasa lielāku gatavību visos ES kiberdrošības ekosistēmas līmeņos. Šie draudi neaprobežojas ar Krievijas militāro agresiju pret Ukrainu un ietver pastāvīgus valsts un nevalstisku subjektu radītus kiberdraudus, kas, visticamāk, saglabāsies, ņemot vērā, ka pašreizējā ģeopolitiskajā saspīlējumā ir iesaistīti daudzi valsts balstīti noziedzīgi subjekti un hakeri. Pēdējos gados krasi palielinājies kiberuzbrukumu skaits, ieskaitot uzbrukumus piegādes ķēdēm, kuru mērķis ir kiberspiegošana, izspiedējprogrammatūras izmantošana vai traucējumu radīšana. 2020. gadā uzbrukums uzņēmuma "SolarWinds" piegādes ķēdei skāra vairāk nekā 18 000 organizāciju visā pasaulē, ieskaitot valdības aģentūras un lielus uzņēmumus. Nopietni kiberdrošības incidenti var būt pārāk postoši, lai viena vai vairākas skartās dalībvalstis spētu ar tiem tikt galā vienas. Šā iemesla dēļ ir vajadzīga pastiprināta solidaritāte Savienības līmenī, lai labāk atklātu kiberdrošības apdraudējumus un incidentus, sagatavotos tiem un reaģētu uz tiem.

Kiberdraudu un kiberincidentu atklāšanā ir steidzami jāpaplašina informācijas apmaiņa un jāuzlabo mūsu kolektīvās spējas, lai krasi saīsinātu kiberdraudu atklāšanai vajadzīgo laiku un tie nespētu radīt plašu kaitējumu un lielas izmaksas[1]. Lai gan digitālās infrastruktūras savstarpējās savienotības dēļ daudziem kiberdrošības apdraudējumiem un incidentiem var būt

[1] Saskaņā ar *Ponemon Institute* un *IBM Security* ziņojumu vidējais laiks, kas tika patērēts pārkāpuma konstatēšanai, 2022. gadā bija 207 dienas un tā ierobežošana aizņēma vēl 70 dienas. Tajā pašā laikā 2022. gadā tādu datu aizsardzības pārkāpumu vidējās izmaksas, kuru dzīves cikls pārsniedz 200 dienas, bija 4,86 miljoni EUR; salīdzinājumam – tādu pārkāpumu vidējās izmaksas, kuru dzīves cikls ir īsāks par 200 dienām, bija 3,74 miljoni EUR (*Cost of a data breach 2022*, https://www.ibm.com/reports/data-breach).

pārrobežu dimensija, dalībvalstis ar attiecīgu informāciju joprojām apmainās maz. Lai palīdzētu atrisināt šo problēmu, tiks izveidots pārrobežu drošības operāciju centru (DOC) tīkls, kura mērķis būs uzlabot atklāšanas un reaģēšanas spējas.

Attiecībā uz gatavību kiberdrošības incidentiem un reaģēšanu uz tiem jānorāda, ka pašlaik Savienības līmenī sniegtā atbalsta apmērs un solidaritāte starp dalībvalstīm ir maza. Padomes 2021. gada oktobra secinājumos tika uzsvērta nepieciešamība novērst šos trūkumus, aicinot Komisiju iesniegt priekšlikumu par jaunu ārkārtējas reaģēšanas fondu kiberdrošības jomā[2].

Ar šo regulu īsteno arī 2020. gada decembrī pieņemto ES kiberdrošības stratēģiju[3], kurā paziņots par nodomu izveidot Eiropas kibervairogu, kas stiprinās kiberdraudu atklāšanas un informācijas apmaiņas spējas Eiropas Savienībā, apvienojot valstu un pārrobežu DOC vienā tīklā.

Šīs regulas pamatā ir pirmie soļi, kas jau sperti ciešā sadarbībā ar galvenajām ieinteresētajām personām un ko atbalsta programma "Digitālā Eiropa" (PDE). Konkrēti DOC jomā PDE kiberdrošības darba programmā 2021.–2022. gadam tika izsludināts uzaicinājums paust ieinteresētību par rīku un infrastruktūras kopīgu iepirkšanu ar mērķi izveidot pārrobežu drošības operāciju centrus un uzaicinājums pieteikties dotācijām, kas paredzētas tādu DOC spēju veidošanai, kuri strādā publiskā un privātā sektora organizāciju labā. Attiecībā uz gatavību incidentiem un reaģēšanu uz tiem Komisija ir izveidojusi īstermiņa programmu dalībvalstu atbalstīšanai ar papildu finansējumu, kas piešķirts Eiropas Savienības Kiberdrošības aģentūrai (*ENISA*), lai nekavējoties paaugstinātu gatavību smagiem kiberincidentiem un spējas reaģēt uz tiem. Abas darbības tika sagatavotas ciešā koordinācijā ar dalībvalstīm. Ar šo regulu tiek novērsti minēto darbību trūkumi, un tajā ir ņemtas vērā minēto darbību īstenošanā gūtās atziņas.

Visbeidzot, ar šo priekšlikumu tiek īstenota 10. novembrī pieņemtajā kopīgajā paziņojumā par kiberaizsardzību[4] paustā apņemšanās sagatavot priekšlikumu ES kibersolidaritātes iniciatīvai ar šādiem mērķiem: stiprināt kopīgas atklāšanas, situācijas apzināšanās un reaģēšanas spējas ES, pakāpeniski veidot ES līmeņa kiberdrošības rezervi no uzticamu privāto pakalpojumu sniedzēju pakalpojumiem un atbalstīt kritisko vienību testēšanu.

Ņemot vērā iepriekš minēto, Komisija nāk klajā ar šo Kibersolidaritātes aktu, kura mērķis ir stiprināt solidaritāti Savienības līmenī, lai labāk atklātu kiberdrošības apdraudējumu un incidentus, sagatavotos tiem un reaģētu uz tiem, un to paredzēts panākt, īstenojot šādus konkrētus mērķus:

---

2 *Council conclusions on the development of the European Union's cyber posture approved by the Council at its meeting on 23 May 2022* (9364/22).

3 Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberdrošības stratēģija digitālajai desmitgadei", JOIN(2020) 18 final.

4 Kopīgs paziņojums Eiropas Parlamentam un Padomei "ES kiberaizsardzības politika", JOIN(2022) 49 final.

- stiprināt kiberdraudu un kiberincidentu kopīgu atklāšanu un situācijas apzināšanos ES un tādējādi veicināt Eiropas tehnoloģisko suverenitāti kiberdrošībā;

- pastiprināt kritisko vienību gatavību visā ES un stiprināt solidaritāti, attīstot kopīgās spējas reaģēt uz ievērojamiem vai plašiem kiberdrošības incidentiem, tostarp darīt pieejamu atbalstu reaģēšanai uz incidentiem PDE asociētajām trešām valstīm;

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

Šos mērķus īsteno ar šādām darbībām:

- izvērst DOC Eiropas mēroga infrastruktūru (Eiropas kibervairogs), lai veidotu un uzlabotu kopīgas atklāšanas un situācijas apzināšanās spējas;

- izveidot kiberavārijas mehānismu, lai palīdzētu dalībvalstīm sagatavoties ievērojamiem un plašiem kiberdrošības incidentiem, uz tiem reaģēt un no tiem nekavējoties atkopties. Atbalstu reaģēšanai uz incidentiem dara pieejamu arī Eiropas Savienības iestādēm, struktūrām, birojiem un aģentūrām (ISBA);

- izveidot Eiropas kiberdrošības incidentu pārskatīšanas mehānismu konkrētu ievērojamu vai liela mēroga incidentu pārskatīšanai un novērtēšanai.

Eiropas kibervairogs un kiberavārijas mehānisms tiks atbalstīti ar finansējumu no PDE, kas ar šo leģislatīvo instrumentu tiks grozīta, lai tajā iekļautu iepriekš minētās darbības, paredzētu finansiālu atbalstu to attīstīšanai un precizētu finansiālā atbalsta saņemšanas nosacījumus.

- **Saskanība ar spēkā esošajiem noteikumiem konkrētajā politikas jomā**

ES satvars ietver vairākus tiesību aktus, kas jau ir spēkā vai ierosināti Savienības līmenī, lai mazinātu ievainojamību, palielinātu kritisko vienību noturību pret kiberdrošības riskiem un atbalstītu liela mēroga kiberdrošības incidentu un krīžu koordinētu pārvaldību, sevišķi Direktīvu, ar ko paredz pasākumus nolūkā panākt vienādi augstu tīklu un informācijas sistēmu drošības līmeni visā Savienībā ("TID2 direktīva")[5], Kiberdrošības aktu[6], Direktīvu

[5] 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 (TID2 direktīva).

[6] 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).

par uzbrukumiem informācijas sistēmām[7] un Komisijas Ieteikumu (ES) 2017/1584 par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm[8].

Kibersolidaritātes aktā ierosinātās darbības attiecas uz situācijas apzināšanos, informācijas apmaiņu, kā arī atbalstu gatavībai kiberincidentiem un reaģēšanai uz tiem. Šīs darbības atbilst Savienības līmenī spēkā esošā tiesiskā regulējuma, sevišķi Direktīvas (ES) 2022/2555 ("TID2 direktīva"), mērķiem un palīdz tos sasniegt. Kibersolidaritātes akts balstīsies galvenokārt uz pastāvošajiem kiberdrošības operatīvās sadarbības un krīžu pārvarēšanas satvariem un atbalstīs tos, sevišķi Eiropas Kiberkrīžu sadarbības organizāciju tīklu (*EU-CyCLONe*) un datordrošības incidentu reaģēšanas vienību (*CSIRT*) tīklu.

Pārrobežu DOC platformām būtu jāveido jauna spēja, kas papildina *CSIRT* tīklu, apvienojot un kopīgojot publisko un privāto struktūru datus par kiberdrošības apdraudējumiem, palielinot šādu datu vērtību ar ekspertu veiktu analīzi un mūsdienīgiem rīkiem un veicinot Savienības spēju un tehnoloģiskās suverenitātes attīstību.

Visbeidzot, šis priekšlikums atbilst Padomes Ieteikumam par Savienības mēroga koordinētu pieeju kritiskās infrastruktūras noturības stiprināšanai[9], kurā dalībvalstis tiek aicinātas veikt steidzamus un iedarbīgus pasākumus un lojāli, efektīvi, solidāri un koordinēti sadarboties savā starpā, ar Komisiju un citām attiecīgām publiskā sektora iestādēm, kā arī ar attiecīgajām vienībām, lai uzlabotu tās kritiskās infrastruktūras noturību, ko izmanto pamatpakalpojumu sniegšanai iekšējā tirgū.

- **Saskanība ar citām Savienības politikas jomām**

Priekšlikums saskan ar citiem ārkārtas mehānismiem un protokoliem krīžu pārvarēšanai, piemēram, integrēto krīzes situāciju politiskās reaģēšanas mehānismu (*IPCR*). Kibersolidaritātes akts papildinās šos krīžu pārvarēšanas satvarus un protokolus, sniedzot īpašu atbalstu gatavībai kiberdrošības incidentiem un reaģēšanai uz tiem. Priekšlikums saskanēs arī ar ES ārējo darbību, kura tiek īstenota, reaģējot uz liela mēroga incidentiem kopējās ārpolitikas un drošības politikas (KĀDP) ietvaros, un kurā cita starpā tiek izmantota ES kiberdiplomātijas rīkkopa. Priekšlikums papildinās darbības, kas tiek īstenotas saskaņā ar Līguma par Eiropas Savienību 42. panta 7. punktu vai situācijās, kuras noteiktas Līguma par Eiropas Savienības darbību 222. pantā.

[7] 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.

[8] Priekšlikums Eiropas Parlamenta un Padomes regulai par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulu (ES) 2019/1020, COM(2022) 454 final.

[9] Padomes Ieteikums (2022. gada 8. decembris) par Savienības mēroga koordinētu pieeju kritiskās infrastruktūras noturības stiprināšanai (dokuments attiecas uz EEZ), 2023/C 20/01.

Tas arī papildina Savienības civilās aizsardzības mehānismu (*UCPM*)[10], kas izveidots 2013. gada decembrī un papildināts ar jaunu 2021. gada maijā pieņemtu tiesību aktu[11], kurš stiprina *UCPM* novēršanas, gatavības un reaģēšanas pīlārus un sniedz Eiropas Savienībai papildu spējas reaģēt uz jauniem riskiem Eiropā un pasaulē, kā arī palielina *rescEU* rezervi.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

Šā priekšlikuma juridiskais pamats ir Līguma par Eiropas Savienības darbību (LESD) 173. panta 3. punkts un 322. panta 1. punkta a) apakšpunkts. LESD 173. pants nosaka, ka Savienība un dalībvalstis nodrošina vajadzīgos apstākļus Savienības rūpniecības konkurētspējai. Šīs regulas mērķis ir stiprināt rūpniecības un pakalpojumu sektora konkurētspēju Eiropā visā digitalizētajā ekonomikā un veicināt to digitālo pārveidi, paaugstinot kiberdrošības līmeni digitālajā vienotajā tirgū. Konkrētāk, tās mērķis ir palielināt kritiskās un sevišķi kritiskās nozarēs darbojošos iedzīvotāju, uzņēmumu un vienību noturību pret augošajiem kiberdrošības apdraudējumiem, kuriem var būt postoša ietekme uz sabiedrību un ekonomiku.

Priekšlikuma pamatā ir arī LESD 322. panta 1. punkta a) apakšpunkts, jo tajā ir iekļauti īpaši pārnešanas noteikumi, atkāpjoties no gada pārskata principa, kas noteikts Eiropas Parlamenta un Padomes Regulā (ES, Euratom) 2018/1046 ("Finanšu regula")[12]. Pareizas finanšu pārvaldības nolūkā un ņemot vērā kiberdrošības kopainas un kiberdraudu neparedzamo, ārkārtējo un īpašo raksturu, kiberavārijas mehānismam jāpiemīt zināmai elastībai attiecībā uz budžeta pārvaldību, sevišķi – jāļauj uz nākamo finanšu gadu automātiski pārnest neizmantotās saistību un maksājumu apropriācijas darbībām, ar kurām īsteno regulā noteiktos mērķus. Tā kā jaunais noteikums rada problēmas saistībā ar Finanšu regulu, šo jautājumu varētu risināt pašreizējās sarunās par Finanšu regulas pārstrādāšanu.

• Subsidiaritāte (neekskluzīvas kompetences gadījumā)

Tā kā kiberdrošības apdraudējumiem ir spēcīgs pārrobežu raksturs un aug to risku un incidentu skaits, kuru sekas sniedzas pāri valstu un nozaru robežām un papildus tieši skartajam produktam ietekmē vēl citus produktus, dalībvalstis vienas pašas nevar ar labiem rezultātiem sasniegt šīs intervences mērķus un ir vajadzīga kopīga rīcība un solidaritāte Savienības līmenī.

---

10 Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu (dokuments attiecas uz EEZ).

11 Eiropas Parlamenta un Padomes Regula (ES) 2021/836 (2021. gada 20. maijs), ar ko groza Lēmumu Nr. 1313/2013/ES par Savienības civilās aizsardzības mehānismu (dokuments attiecas uz EEZ).

12 Eiropas Parlamenta un Padomes Regula (ES, Euratom) 2018/1046 (2018. gada 18. jūlijs) par finanšu noteikumiem, ko piemēro Savienības vispārējam budžetam (OV L 193, 30.7.2018., 1. lpp.).

Pieredze cīņā pret kiberdraudiem, kas izriet no kara pret Ukrainu, kā arī atziņas, kas gūtas Francijas prezidentūras laikā īstenotajās kiberdrošības mācībās (*EU CyCLES*), liecina: lai panāktu solidaritāti ES līmenī, būtu jāizstrādā konkrēti savstarpējā atbalsta mehānismi, sevišķi sadarbība ar privāto sektoru. Ņemot to vērā, Padomes 2022. gada 23. maija secinājumos par Eiropas Savienības kiberdrošības statusa uzlabošanu Komisija tika aicināta iesniegt priekšlikumu par jaunu ārkārtējas reaģēšanas fondu kiberdrošības jomā.

Savienības līmenī sniegtais atbalsts un īstenotās darbības, kuru mērķis ir uzlabot kiberdrošības apdraudējumu atklāšanu un palielināt gatavību un reaģēšanas spējas, sniegtu pievienoto vērtību, jo tādējādi tiktu novērsta centienu dublēšanās Savienībā un dalībvalstīs. Tas ļautu labāk izmantot pastāvošos resursus un uzlabot koordināciju un informācijas apmaiņu par gūtajām atziņām. Kiberavārijas mehānisms arī paredz no ES kiberdrošības rezerves sniegt atbalstu PDE asociētajām trešām valstīm.

Atbalsts, kas tiks sniegts dažādajās iniciatīvās, kuras tiks izveidotas un finansētas Savienības līmenī, papildinās, nevis dublēs valstu spējas atklāt kiberdraudus un kiberincidentus, apzināties situāciju, sagatavoties šiem draudiem un incidentiem un reaģēt uz tiem.

• Proporcionalitāte

Paredzētās darbības nepārsniedz to, kas ir vajadzīgs, lai sasniegtu regulas vispārīgos un konkrētos mērķus. Šajā regulā paredzētās darbības neietekmē dalībvalstu atbildību par valsts drošību, sabiedrisko drošību un noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem. Tās arī neietekmē kritiskās un sevišķi kritiskās nozarēs darbojošos vienību juridisko pienākumu pieņemt kiberdrošības pasākumus saskaņā ar TID2 direktīvu.

Darbības, uz kurām attiecas šī regula, papildina minētos centienus un pasākumus, palīdzot izveidot infrastruktūru labākai apdraudējumu atklāšanai un analīzei un sniedzot atbalstu gatavības un reaģēšanas darbībām, kas veicamas ievērojamu vai plašu incidentu gadījumā.

• Juridiskā instrumenta izvēle

Priekšlikums ir par Eiropas Parlamenta un Padomes regulu. Šis ir vispiemērotākais juridiskais instruments, jo tikai regula ar tās tieši piemērojamajām tiesību normām var nodrošināt Eiropas kibervairoga un kiberavārijas mehānisma izveidei un darbībai nepieciešamo vienādības pakāpi, paredzot atbalstu no PDE to izveidei, kā arī skaidrus nosacījumus šā atbalsta izmantošanai un piešķiršanai.

3. RETROSPEKTĪVU IZVĒRTĒJUMU, APSPRIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- **Apspriešanās ar ieinteresētajām personām**

Šajā regulā paredzētās darbības atbalstīs programma "Digitālā Eiropa", par ko notika plaša apspriešanās. Turklāt tās balstīsies uz pirmajiem soļiem, kas jau ir veikti ciešā sadarbībā ar galvenajām ieinteresētajām personām. Attiecībā uz DOC Komisija ciešā sadarbībā ar dalībvalstīm Eiropas Kiberdrošības kompetences centra (*ECCC*) ietvaros ir izstrādājusi koncepcijas dokumentu par pārrobežu DOC platformu izstrādi un uzaicinājumu paust ieinteresētību. Šajā saistībā tika veikts valstu DOC spēju apsekojums un *ECCC* tehniskajā darba grupā, kas pulcē dalībvalstu pārstāvjus, tika apspriestas kopīgas pieejas un tehniskās prasības. Notika arī viedokļu apmaiņa ar rūpniecības sektora pārstāvjiem, sevišķi *ENISA* izveidotajā DOC ekspertu grupā un Eiropas Kiberdrošības organizācijā (*ECSO*).

Papildus tam attiecībā uz gatavību incidentiem un reaģēšanu uz tiem Komisija ir izveidojusi īstermiņa programmu dalībvalstu atbalstam, izmantojot papildu finansējumu, kas piešķirts Eiropas Savienības Kiberdrošības aģentūrai no PDE, lai nekavējoties paaugstinātu gatavību smagiem kiberincidentiem un spējas reaģēt uz tiem. Dalībvalstu un rūpniecības sektora pārstāvju atsauksmes, kas apkopotas šīs īstermiņa programmas īstenošanas laikā, jau sniedz vērtīgas atziņas, kas izmantotas ierosinātās regulas sagatavošanā, lai novērstu konstatētās nepilnības. Tas bija pirmais solis, kas sperts saskaņā ar Padomes secinājumiem par kiberdrošības statusu, kuros Komisijai tika prasīts nākt klajā ar priekšlikumu par jaunu ārkārtas reaģēšanas fondu kiberdrošības jomā.

Turklāt 2023. gada 16. februārī, pamatojoties uz diskusiju dokumentu, notika darbseminārs ar dalībvalstu ekspertiem par kiberavārijas mehānismu. Šajā darbseminārā piedalījās visas dalībvalstis, un 11 dalībvalstis papildus tam iesniedza arī savas pārdomas rakstveidā.

- **Ietekmes novērtējums**

Priekšlikuma steidzamības dēļ ietekmes novērtējums nav veikts. Šajā regulā paredzētās darbības atbalstīs programma "Digitālā Eiropa", un tās ir saskaņā ar darbībām, kas noteiktas PDE regulā, par kuru tika veikts īpašs ietekmes novērtējums. Šī regula neradīs būtisku administratīvo ietekmi vai ietekmi uz vidi, kas būtu lielāka par to, kura jau novērtēta PDE regulas ietekmes novērtējumā.

Turklāt tā balstās uz pirmajām darbībām, kas izstrādātas ciešā sadarbībā ar galvenajām ieinteresētajām personām, kā izklāstīts iepriekš, un ar to atsaucas uz Komisijai pausto dalībvalstu aicinājumu līdz 2022. gada trešā ceturkšņa beigām iesniegt priekšlikumu par jaunu ārkārtas reaģēšanas fondu kiberdrošības jomā.

Runājot tieši par Eiropas kibervairoga ietvaros īstenoto situācijas apzināšanos un draudu atklāšanu, jānorāda, ka PDE kiberdrošības darba programmas 2021.–2022. gadam ietvaros tika izsludināts uzaicinājums paust ieinteresētību par rīku un infrastruktūras kopīgu iepirkšanu ar mērķi izveidot pārrobežu drošības operāciju centrus un uzaicinājums pieteikties dotācijām, kas paredzētas tādu DOC spēju veidošanai, kuri strādā publiskā un privātā sektora organizāciju labā.

Gatavības incidentiem un reaģēšanas uz tiem jomā Komisija, kā minēts iepriekš, ir izveidojusi īstermiņa programmu, kurā dalībvalstīm tiek sniegts atbalsts no PDE un kuru īsteno *ENISA*. Aptvertie pakalpojumi ietver gatavības nodrošināšanas darbības, piemēram, ielaušanās testēšanu kritiskajās vienībās, lai noteiktu to ievainojamību. Tā arī vairo iespējas palīdzēt dalībvalstīm tādu smagu incidentu gadījumā, kas skar kritiskās vienības. *ENISA* jau īsteno šo īstermiņa programmu un ir jau sniegusi attiecīgas atziņas, kas ir ņemtas vērā, gatavojot šo regulu.

- **Pamattiesības**

Veicinot digitālās informācijas drošību, šis priekšlikums palīdzēs aizsargāt tiesības uz brīvību un drošību saskaņā ar ES Pamattiesību hartas 6. pantu un tiesības uz privātās un ģimenes dzīves neaizskaramību saskaņā ar ES Pamattiesību hartas 7. pantu. Aizsargājot uzņēmumus no kiberuzbrukumiem, kas rada ekonomisku kaitējumu, priekšlikums veicinās arī darījumdarbības brīvību saskaņā ar ES Pamattiesību hartas 16. pantu un tiesības uz īpašumu saskaņā ar ES Pamattiesību hartas 17. pantu. Visbeidzot, aizsargājot kritiskās infrastruktūras integritāti kiberuzbrukumu gadījumā, priekšlikums veicinās tiesības uz veselības aprūpi saskaņā ar ES Pamattiesību hartas 35. pantu un tiesības piekļūt pakalpojumiem ar vispārēju tautsaimniecisku nozīmi saskaņā ar ES Pamattiesību hartas 36. pantu.

4. IETEKME UZ BUDŽETU

Šajā regulā paredzētās darbības tiks atbalstītas ar finansējumu, kas piešķirts saskaņā ar PDE stratēģisko mērķi "kiberdrošība".

Kopējais budžets ietver palielinājumu 100 miljonu EUR apmērā, ko šajā regulā ierosināts pārdalīt no citiem PDE stratēģiskajiem mērķiem. Tādējādi jaunā kopējā summa, kas pieejama kiberdrošības darbībām programmā "Digitālā Eiropa", būs 842,8 miljoni EUR

Ar daļu no papildu 100 miljoniem EUR tiks palielināts *ECCC* pārvaldītais budžets, lai īstenotu ar DOC un gatavību saistītas darbības to darba programmas(-u) ietvaros. Turklāt ar šo papildu finansējumu atbalstīs arī ES kiberdrošības rezerves izveidi.

Tas papildina budžetu, kas jau paredzēts līdzīgām darbībām galvenajā PDE un PDE kiberdrošības darba programmā 2023.–2027. gadam, un tas varētu palielināt kopējo summu līdz 551 miljonam EUR 2023.–2027. gadam, bet 115 miljoni EUR jau bija atvēlēti šai jomai

2021.–2022. gada izmēģinājumu projektos. Kopējais budžets, ieskaitot dalībvalstu iemaksas, varētu sasniegt 1,109 miljardus EUR.

Pārskats par saistītajām izmaksām ir iekļauts šim priekšlikumam pievienotajā tiesību akta priekšlikuma finanšu pārskatā.

5. CITI ELEMENTI

• Īstenošanas plāni un uzraudzīšanas, izvērtēšanas un ziņošanas kārtība

Lai novērtētu jauno noteikumu iedarbīgumu, Komisija uzraudzīs to īstenošanu, piemērošanu un atbilstību tiem. Komisija četru gadu laikā pēc šīs regulas piemērošanas sākuma dienas iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs regulas izvērtēšanu un pārskatīšanu.

• Detalizēts konkrētu priekšlikuma noteikumu skaidrojums

Vispārīgie mērķi, priekšmets un definīcijas (I nodaļa)

I nodaļā ir izklāstīti regulas mērķi stiprināt solidaritāti Savienības līmenī, lai labāk atklātu kiberdrošības apdraudējumus un incidentus, sagatavotos tiem un reaģētu uz tiem, it īpaši stiprināt kiberdraudu un kiberincidentu kopīgu atklāšanu un situācijas apzināšanos Savienībā, stiprināt to vienību gatavību, kuras darbojas kritiskās un sevišķi kritiskās nozarēs visā Savienībā, stiprināt solidaritāti, attīstot kopīgas spējas reaģēt uz ievērojamiem vai liela mēroga kiberdrošības incidentiem, un uzlabot Savienības noturību, pārskatot un novērtējot ievērojamus vai liela mēroga incidentus. Minētajā nodaļā ir izklāstītas arī darbības, ar kurām šie mērķi tiks sasniegti: Eiropas kibervairoga izvēršana, kiberavārijas mehānisma izveide un Kiberdrošības incidentu pārskatīšanas mehānisma izveide. Tajā arī sniegtas aktā izmantotās definīcijas.

Eiropas kibervairogs (II nodaļa)

Ar II nodaļu ir izveidots Eiropas kibervairogs, un tajā ir izklāstīti tā dažādie elementi un dalības nosacījumi. Pirmkārt, tajā ir paziņots Eiropas kibervairoga vispārējais mērķis, proti, attīstīt Savienībā augsta līmeņa spējas atklāt, analizēt un apstrādāt datus par kiberdraudiem un kiberincidentiem Savienībā, kā arī konkrētie darbības mērķi. Tajā noteikts, ka Savienības finansējumu Eiropas kibervairogam īsteno saskaņā ar PDE regulu.

Tajā pašā nodaļā arī aprakstīts to vienību veids, kuras veido Eiropas kibervairogu. Vairogs sastāv no valstu drošības operāciju centriem (“valsts DOC”) un pārrobežu drošības operāciju centriem (“pārrobežu DOC”). Katra iesaistītā dalībvalsts ieceļ valsts DOC. Tas darbojas kā uzziņas centrs un vārti uz citām publiskām un privātām organizācijām valsts līmenī, lai vāktu un analizētu informāciju par kiberdrošības apdraudējumiem un incidentiem un sniegtu

ieguldījumu pārrobežu DOC izveidē. Pēc uzaicinājuma paust ieinteresētību *ECCC* var izraudzīties valsts DOC, kas piedalīsies rīku un infrastruktūras iepirkumā kopā ar *ECCC* un saņems dotāciju šo rīku un infrastruktūras ekspluatācijai. Ja valsts DOC saņem Savienības atbalstu, tas apņemas divu gadu laikā pieteikties dalībai pārrobežu drošības operāciju centrā.

Pārrobežu DOC ir konsorcijs, kurā ietilpst vismaz trīs dalībvalstis, ko pārstāv valstu DOC un kas ir apņēmušās strādāt kopā, lai koordinētu savas kiberdraudu atklāšanas un kiberdraudu uzraudzības darbības. Pēc sākotnējā uzaicinājuma paust ieinteresētību *ECCC* var atlasīt mitinātājkonsorciju, kas piedalīsies rīku un infrastruktūras iepirkumā kopā ar *ECCC* un saņems dotāciju šo rīku un infrastruktūras ekspluatācijai. Mitinātājkonsorcija dalībnieki noslēdz rakstisku konsorcija nolīgumu, kurā izklāstīta to iekšējā kārtība. Pēc tam šajā nodaļā ir sīki izklāstītas prasības attiecībā uz informācijas apmaiņu starp pārrobežu DOC dalībniekiem un informācijas apmaiņu starp pārrobežu DOC un citiem pārrobežu DOC, kā arī ar attiecīgajām ES vienībām. Valstu DOC, kas piedalās pārrobežu DOC, savstarpēji apmainās ar attiecīgo informāciju, kas saistīta ar kiberdraudiem, un sīkāka šīs apmaiņas kārtība, tostarp apņemšanās kopīgot ievērojamu datu apjomu un ar to saistītie nosacījumi, būtu jānosaka konsorcija nolīgumā. Pārrobežu DOC nodrošina augsta līmeņa sadarbspēju savā starpā. Pārrobežu DOC būtu arī jānoslēdz sadarbības nolīgumi ar citiem pārrobežu DOC, norādot informācijas apmaiņas principus. Ja pārrobežu DOC iegūst informāciju par potenciālu vai notiekošu liela mēroga kiberdrošības incidentu, tie sniedz attiecīgu informāciju *EU-CyCLONe*, *CSIRT* tīklam un Komisijai, ņemot vērā attiecīgo lomu, kas tiem saskaņā ar Direktīvu (ES) 2022/2555 ir piešķirta krīzes pārvarēšanā. II nodaļas noslēgumā ir precizēti drošības nosacījumi dalībai Eiropas kibervairogā.

Kiberavārijas mehānisms (III nodaļa)

Ar III nodaļu ir izveidots kiberavārijas mehānisms, kura mērķis ir uzlabot Savienības noturību pret smagiem kiberdrošības apdraudējumiem un solidāri sagatavoties ievērojamu un liela mēroga kiberdrošības incidentu un krīžu īstermiņa ietekmei un mazināt to. Darbības, ar kurām īsteno kiberavārijas mehānismu, atbalsta ar finansējumu no PDE. Mehānisms paredz darbības, kas veicina gatavību, ieskaitot tādu vienību koordinētu testēšanu, kuras darbojas sevišķi kritiskās nozarēs, reaģēšanu uz ievērojamiem vai liela mēroga kiberdrošības incidentiem un tūlītēju atgūšanos no tiem vai mazina ievērojamus kiberdraudus, un savstarpējās palīdzības darbības.

Ārkārtējas reaģēšanas mehānisma kiberdrošības jomā gatavības nodrošināšanas darbības ietver tādu vienību koordinētu gatavības testēšanu, kuras darbojas sevišķi kritiskās nozarēs. Komisijai pēc apspriešanās ar *ENISA* un TID sadarbības grupu būtu regulāri jānosaka, kurās no Direktīvas (ES) 2022/2555 I pielikumā uzskaitītajām sevišķi kritiskajām nozarēm un apakšnozarēm vienībām var veikt koordinētu gatavības testēšanu ES līmenī.

Lai īstenotu reaģēšanai uz incidentiem ierosinātās darbības, ar šo regulu izveido ES kiberdrošības rezervi, kas sastāv no reaģēšanas uz incidentiem pakalpojumiem, kurus

sniedz saskaņā ar šajā regulā noteiktajiem kritērijiem atlasīti uzticami pakalpojumu sniedzēji. ES kiberdrošības rezerves pakalpojumu lietotāji ietver dalībvalstu kiberkrīžu pārvaldības iestādes un *CSIRT*, kā arī Savienības iestādes, struktūras un aģentūras. Komisijai ir vispārēja atbildība par ES kiberdrošības rezerves īstenošanu, un tā var pilnībā vai daļēji uzticēt *ENISA* ES kiberdrošības rezerves darbības nodrošināšanu un pārvaldību.

Lai saņemtu atbalstu no ES kiberdrošības rezerves, lietotājiem pašiem būtu jāveic pasākumi, lai mazinātu tā incidenta sekas, par kuru tiek pieprasīts atbalsts. Pieprasījumos piešķirt atbalstu no ES kiberdrošības rezerves būtu jāiekļauj vajadzīgā attiecīgā informācija par incidentu un lietotāju jau veiktajiem pasākumiem. Šajā nodaļā ir aprakstīta arī īstenošanas kārtība, ieskaitot ES kiberdrošības rezervei iesniegto pieprasījumu novērtēšanu.

Regulā ir paredzēti arī iepirkuma principi un atlases kritēriji attiecībā uz uzticamiem ES kiberdrošības rezerves pakalpojumu sniedzējiem.

Trešās valstis var pieprasīt atbalstu no ES kiberdrošības rezerves, ja to paredz asociācijas nolīgumi, kas noslēgti par to dalību programmā "Digitālā Eiropa". Šajā nodaļā ir sīkāk aprakstīti šādas dalības nosacījumi un kārtība.

Kiberdrošības incidentu pārskatīšanas mehānisms (IV nodaļa)

Pēc Komisijas, *EU-CyCLONe* vai *CSIRT* tīkla pieprasījuma *ENISA* būtu jāpārskata un jānovērtē apdraudējumi, ievainojamība un ietekmes mazināšanas darbības, kas ir saistīti ar konkrētu ievērojamu vai liela mēroga kiberdrošības incidentu. *ENISA* būtu jāsagatavo minētais pārskats un novērtējums incidenta pārskata ziņojuma veidā un tas būtu jāiesniedz *CSIRT* tīklam, *EU-CyCLONe* un Komisijai, lai palīdzētu tiem veikt to uzdevumus. Ja incidents ir saistīts ar trešu valsti, Komisijai ziņojums būtu jānodod Augstajam pārstāvim. Ziņojumā būtu jāiekļauj gūtās atziņas un attiecīgā gadījumā ieteikumi, kā uzlabot Savienības kiberdrošības statusu.

Nobeiguma noteikumi (V nodaļa)

V nodaļā ir ietverti grozījumi PDE regulā un Komisijas pienākums sagatavot Eiropas Parlamentam un Padomei regulārus ziņojumus par regulas izvērtēšanu un pārskatīšanu. Komisija ir pilnvarota pieņemt īstenošanas aktus saskaņā ar 21. pantā minēto pārbaudes procedūru, lai precizētu nosacījumus sadarbspējai starp pārrobežu DOC; noteiktu procesuālo kārtību informācijas apmaiņai starp pārrobežu DOC un Savienības vienībām par iespējamu vai notiekošu liela mēroga kiberdrošības incidentu; noteiktu tehniskās prasības, lai nodrošinātu datu drošību un infrastruktūras fizisko drošību augstā līmenī un aizsargātu Savienības drošības intereses, kad notiek informācijas apmaiņa ar vienībām, kas nav dalībvalstu publiskās struktūras; precizētu ES kiberdrošības rezervei nepieciešamo reaģēšanas pakalpojumu veidus un skaitu un vēl vairāk precizētu sīki izklāstīto kārtību, kādā tiek piešķirti atbalsta pakalpojumi no ES kiberdrošības rezerves.

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

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas dalībvalstu parlamentiem,

ņemot vērā Revīzijas palātas atzinumu[13],

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[14],

ņemot vērā Reģionu komitejas atzinumu[15],

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Informācijas un komunikācijas tehnoloģiju lietošana un izmantošana visās saimnieciskās dzīves nozarēs ir kļuvušas par fundamentāliem aspektiem laikā, kad mūsu pārvaldes, uzņēmumi un pilsoņi ir cits ar citu pāri nozarēm un robežām saistīti un savstarpēji atkarīgi vairāk nekā jebkad agrāk.

2) Aug kiberincidentu apjoms, biežums un ietekme, ieskaitot uzbrukumus piegādes ķēdēm, un to mērķis ir kiberspiegošana, izspiedējprogrammu izmantošana vai darbības traucēšana. Tie ievērojami apdraud tīklu un informācijas sistēmu darbību. Ņemot vērā strauji mainīgo apdraudējuma ainu, draudoši plaši kiberincidenti, kas izraisa būtisku pārrāvumu vai kaitējumu kritiskajai infrastruktūrai, prasa labāku gatavību visos Savienības kiberdrošības satvara līmeņos. Apdraudējums ir plašāks par Krievijas militāro agresiju pret Ukrainu – ticams, ka tas saglabāsies, jo pašreizējā ģeopolitiskajā saspīlējumā iesaistījušies daudzi valstu atbalstīti krimināli un hakeristiski subjekti. Tādi kiberincidenti var kavēt sabiedrisku pakalpojumu sniegšanu un

[13] OV C .., .., .. lpp.
[14] OV C , , . lpp.
[15] OV C , , . lpp.

saimniecisku darbību, arī kritiskās vai ļoti kritiskās nozarēs, radīt būtiskus finansiālus zaudējumus, mazināt lietotāju uzticēšanos, radīt būtisku kaitējumu Savienības ekonomikai un pat veselībai un dzīvībai bīstamas sekas. Bez tam kiberincidenti ir neprognozējami, jo tie mēdz rasties un izplesties pavisam īsā laikā, tos neierobežo nekāda ģeogrāfiska platība un tie notiek vienlaicīgi vai vienā mirklī izplatās daudzās valstīs.

(3) Ir jāstiprina rūpniecības un pakalpojumu nozaru konkurētspēja Savienībā visā digitalizētajā ekonomikā un jāatbalsta to digitālā pārveide, nostiprinot digitālā vienotā tirgus kiberdrošību. Trijos dažādos konferences par Eiropas nākotni[16] priekšlikumos ir ieteikts palielināt pilsoņu, uzņēmumu un vienību, kuras darbina kritisko infrastruktūru, noturību pret augošo kiberdrošības apdraudējumu, kas spēj nodarīt postu sabiedrībai un tautsaimniecībai. Tāpēc vajag ieguldīt infrastruktūrā un pakalpojumos, kas palīdzēs veicīgāk atklāt kiberapdraudējumu un kiberincidentus un uz tiem reaģēt, un palīdzēt dalībvalstīm labāk sagatavoties ievērojamiem un plašiem kiberincidentiem un dot tiem pretsparu. Savienībai arī jāpalielina savas spējas šajās jomās, galvenokārt datu vākšanai un kiberapdraudējuma un kiberincidentu analīzei.

(4) Savienība jau ir noteikusi vairākus pasākumus, kam jāmazina kritisko infrastruktūru un vienību neaizsargātība un jāuzlabo to noturība pret kiberapdraudējumu, to vidū: Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555[17], Komisijas Ieteikums (ES) 2017/1584[18], Eiropas Parlamenta un Padomes Direktīva 2013/40/ES[19] un Eiropas Parlamenta un Padomes Regula (ES) 2019/881[20]. Bez tam Padomes ieteikumā par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai dalībvalstis tiek aicinātas veikt steidzamus un efektīvus pasākumus un lojāli, efektīvi, solidāri un koordinēti sadarboties savā starpā, ar Komisiju un citām attiecīgajām publiskajām iestādēm, kā arī ar attiecīgajām vienībām, lai pamatpakalpojumu sniegšanai iekšējā tirgū izmantoto kritisko infrastruktūru padarītu noturīgāku.

(5) Augošās briesmas kiberdrošībai un vispārējā sarežģītā apdraudējuma vide, kurā nepārprotami draud strauja kiberincidentu pārmešanās no dalībvalsts uz dalībvalsti un no trešas valsts uz Savienību, liek pastiprināt solidaritāti Savienības līmenī, lai labāk atklātu kiberdrošības apdraudējumu un kiberincidentus, tiem sagatavotos un uz tiem reaģētu. Padomes secinājumos par ES nostāju kiberlietās[21] dalībvalstis arī aicinājušas Komisiju iesniegt priekšlikumu par jaunu Ārkārtēja stāvokļa reaģēšanas fondu kiberdrošībai.

---

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

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

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

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

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

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

(6) 2022. gada 10. novembrī pieņemtajā Kopīgajā paziņojumā par ES kiberaizsardzības politiku[22] tika izziņota ES kiberdrošības solidaritātes iniciatīva ar šādiem mērķiem: kopīgu ES spēju atklāt kiberapdraudējumu, apzināties stāvokli un reaģēt stiprināšana, veicinot ES drošības operāciju centru (DOC) infrastruktūras izvēršanu, atbalstot ES līmeņa kiberdrošības rezervju pakāpenisku izveidi ar pakalpojumiem no uzticamiem privātiem pakalpojumu sniedzējiem un iespējamas kritisko vienību neaizsargātības pārbaudi uz ES riska novērtēšanas pamata.

(7) Ir jāstiprina kiberapdraudējuma un kiberincidentu atklāšana un stāvokļa apzināšanās visā Savienībā un solidaritāte, uzlabojot dalībvalstu un Savienības gatavību un spējas reaģēt uz ievērojamiem un plašiem kiberincidentiem. Tādēļ Eiropas mērogā jāievieš DOC infrastruktūra (Eiropas kibervairogs), lai veidotu un uzlabotu kopīgas spējas atklāt apdraudējumu un apzināties stāvokli; jāiedibina kiberavārijas mehānisms, kas palīdzētu dalībvalstīm sagatavoties ievērojamiem un plašiem kiberincidentiem, uz tiem reaģēt un no tiem tūlīt atkopties; jāiedibina kiberincidentu izskatīšanas mehānisms konkrētu ievērojamu vai plašu kiberincidentu izskatīšanai un novērtēšanai. Šīs darbības neskar Līguma par Eiropas Savienības darbību (LESD) 107. un 108. pantu.

(8) Lai šos mērķus sasniegtu, dažās jomās ir arī jāgroza Eiropas Parlamenta un Padomes Regula (ES) 2021/694[23]. 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 kiberavārijas 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 jānosaka 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 jābūt attiecīgajam pamataktam 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.

(10) Šai regulai piemēro finansiālus pārnozaru noteikumus, ko Eiropas Parlaments un Padome pieņēmuši uz LESD 322. panta pamata. Minētie noteikumi ir izklāstīti Finanšu regulā 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.

---

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

23 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.).

(11) Pareizai finanšu pārvaldībai vajadzīgi īpaši noteikumi par neizmantoto saistību un maksājumu apropriāciju pārnešanu uz priekšu. Ievērojot principu Savienības budžetu noteikt katru gadu, šai regulai, ņemot vērā kiberdrošības vides neprognozējamo, ārkārtējo un specifisko dabu, ir jāparedz iespējas pārnest uz priekšu neizmantotus līdzekļus, kuri pārsniedz Finanšu regulā noteiktos, tā maksimalizējot kiberavārijas mehānisma spēju atbalstīt dalībvalstis kiberapdraudējuma efektīvā apkarošanā.

(12) Lai efektīvāk novērstu un novērtētu kiberapdraudējumu un kiberincidentus un uz tiem reaģētu, ir nepieciešams attīstīt plašākas zināšanas par kritiskiem aktīviem un infrastruktūrām Savienības teritorijā draudošām briesmām, kā arī par to ģeogrāfisko izplatību, savstarpējo saistību un iespējamām sekām kiberuzbrukumā, kas skartu minētās infrastruktūras. Jāizvērš plaša Savienības DOC infrastruktūra ("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. Minētajai infrastruktūrai 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[24].

(13) Katrai dalībvalstij valsts līmenī jānorīko publiska struktūra, dodot tai uzdevumu attiecīgajā dalībvalstī koordinēt kiberapdraudējuma atklāšanas darbības. Šiem DOC valsts līmenī jābūt par uzziņas avotu un vārteju dalībai Eiropas kibervairogā un jānodrošina, ka informācija par kiberapdraudējumu no publiskām un privātām vienībām tiek valsts līmenī efektīvi un racionalizēti izplatīta un apkopota.

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

(15) Valstī kiberapdraudējuma novērošanu, atklāšanu un analīzi parasti nodrošina publisko un privāto vienību DOC apvienojumā ar *CSIRT*. Turklāt saskaņā ar Direktīvu (ES) 2022/2555 *CSIRT* apmainās ar informāciju *CSIRT* tīklā. Pārrobežu DOC jābūt jaunai spējai, kas papildinātu *CSIRT* tīklu, sakopojot un kopīgojot publisku un privātu vienību datus par kiberdrošības apdraudējumu, tādu datu vērtību paaugstinot ar

[24] 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 (TID2 direktīva) (OV L 333, 27.12.2022., 80. lpp.).

ekspertīzēm un kopīgi iegādātām infrastruktūrām un pašiem modernākajiem rīkiem, un veicinot Savienības spēju un tehnoloģiskās suverenitātes attīstību.

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

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

(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 lietās. Pieņemot vienotu taksonomiju un izstrādājot stāvokļa ziņojuma veidni kiberincidentu tehnisko cēloņu un ietekmes aprakstīšanai, jāņem vērā pašreizējais darbs, kas skar kiberincidentu izziņošanu Direktīvas (ES) 2022/2555 īstenošanas sakarā.

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

(20) Vācot un kopīgojot datus un ar tiem apmainoties, Eiropas kibervairogam jāstiprina Savienības tehnoloģiskā suverenitāte. Kvalitatīvu kūrētu datu sakopošanai arī jāveicina progresīvu mākslīgā intelekta un datu analīzes tehnoloģiju attīstība. Tā

jāsekmē, Eiropas kibervairogu savienojot ar Eiropas augstas veiktspējas datošanas infrastruktūru, kas izveidota ar Padomes Regulu (ES) 2021/1173[25].

(21) Lai gan Eiropas kibervairogs ir civils projekts, kiberaizsardzības kopienai varētu būt labums no spēcīgākām civilpersonu spējām atklāt apdraudējumu un apzināties stāvokli, 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 protokoli un standarti, kas ļautu sadarboties ar kiberaizsardzības kopienu, ietverot drošības pārbaudes un drošības nosacījumus. Eiropas kibervairoga attīstība ciešā sadarbībā ar Augsto pārstāvi jāpapildina ar atziņām, kas turpmāk ļautu sadarboties ar tīkliem un platformām, kuras kiberaizsardzības kopienā atbild par informācijas koplietošanu.

(22) Informācijas koplietošanai Eiropas kibervairoga dalībnieku starpā jāatbilst spēkā esošajām juridiskajām prasībām, it sevišķi Savienības un valstu datu aizsardzības tiesību aktiem, kā arī Savienības konkurences noteikumiem, kas reglamentē informācijas apmaiņu. Tādā mērā, kādā nepieciešama persondatu 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 noteikumiem, 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 kiberincidentu briesmu un skaita pieaugumu, kas skar dalībvalstis, ir jāizveido krīzes atbalsta instruments, kas uzlabotu Savienības noturību pret ievērojamiem un plašiem kiberincidentiem un dalībvalstu darbības papildinātu ar ārkārtēju finansiālu atbalstu būtiskāko dienestu gatavībai, reaģēšanai un tūlītējai atkopšanai. Minētajam instrumentam jānodrošina ātra palīdzība noteiktos apstākļos un ar skaidriem nosacījumiem un jādod iespēja rūpīgi uzraudzīt un izvērtēt, kā resursi izmantoti. Lai gan pienākums kiberincidentus un kiberkrīzes novērst, tām sagatavoties un uz tām reaģēt pirmām kārtām ir dalībvalstīm, kiberavārijas mehānisms veicina solidaritāti starp dalībvalstīm saskaņā ar Līguma par Eiropas Savienību (LES) 3. panta 3. punktu.

(25) Kiberavārijas mehānismam jāparedz atbalsts dalībvalstīm, papildinot to pasākumus un resursus, un citas pastāvošas atbalsta iespējas, kad jāreaģē uz ievērojamiem un plašiem kiberincidentiem un nekavējoties jāatkopjas no tiem, piemēram, pakalpojumi, ko sniedz Eiropas Savienības Kiberdrošības aģentūra ("*ENISA*") saskaņā ar tās pilnvarām, koordinēta reaģēšana un *CSIRT* tīkla palīdzība, *EU-CyCLONe* sniegtais seku mazināšanas atbalsts, kā arī dalībvalstu savstarpējā palīdzība, arī LES 42. panta 7.

[25] Padomes Regula (ES) 2021/1173 (2021. gada 13. jūlijs) par Eiropas Augstas veiktspējas datošanas kopuzņēmuma izveidi un ar ko atceļ Regulu (ES) 2018/1488 (OV L 256, 19.7.2021., 3. lpp.).

punkta kontekstā, *PESCO* ātrās kiberreaģēšanas vienībām[26] un ātrās hibrīdreaģēšanas vienībām. Tam jāapmierina vajadzība nodrošināt, ka ir pieejami specializēti līdzekļi, kas atbalsta gatavību kiberincidentiem un reaģēšanu uz tiem visā Savienībā un trešās valstīs.

(26) Šis instruments neskar procedūras un regulējumu, kuru mērķis ir koordinēt Savienības līmeņa reaģēšanu krīzēs, it īpaši *UCPM*[27], *IPCR*[28,] un Direktīvu (ES) 2022/2555. Tas var veicināt vai papildināt darbības, kuras tiek īstenotas LES 42. panta 7. punkta sakarā vai LESD 222. pantā noteiktajos apstākļos. Attiecīgā gadījumā šā instrumenta izmantošana jākoordinē arī ar kiberdiplomātijas rīkkopas pasākumu īstenošanu.

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

(28) Direktīvā (ES) 2022/2555 ir noteikts, ka dalībvalstīm jāizraugās vai jāizveido viena vai vairākas kiberkrīzes pārvaldības iestādes un jānodrošina, ka tām ir pietiekami resursi savu uzdevumu efektīvai un lietderīgai pildīšanai. Tajā arī noteikts, ka dalībvalstīm ir jāapzina spējas, līdzekļi un procedūras, ko var izmantot krīzes gadījumā, kā arī jāpieņem valsts plāns reaģēšanai uz plašiem kiberincidentiem un kiberkrīzēm, kurā ir noteikti plašu kiberincidentu un kiberkrīžu pārvaldības mērķi un kārtība. Dalībvalstīm arī jāizveido viena vai vairākas *CSIRT*, kurām uzticēti kiberincidentu risināšanas pienākumi saskaņā ar skaidri definētu procesu un aptverot vismaz nozares, apakšnozares un vienību veidus, kas ir minētās direktīvas darbības jomā, un sev jānodrošina pietiekami resursi savu uzdevumu faktiskai izpildei. Šī regula neskar Komisijas funkciju nodrošināt, ka dalībvalstis pilda Direktīvā (ES) 2022/2555 noteiktos pienākumus. Kiberavārijas mehānismam jāpalīdz veikt darbības, kuru mērķis ir stiprināt gatavību, kā arī reaģēšanas darbības kiberincidentā, lai mazinātu ievērojamu un plašu kiberincidentu ietekmi, atbalstītu tūlītēju atkopšanos un/vai atjaunotu būtiskāko dienestu darbību.

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

---

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

[27] Eiropas Parlamenta un Padomes Lēmums Nr. 1313/2013/ES (2013. gada 17. decembris) par Savienības civilās aizsardzības mehānismu (OV L 347, 20.12.2013., 924. lpp.).

[28] Integrētus krīzes situāciju politiskās reaģēšanas mehānismus (*IPCR*), un saskaņā ar Komisijas Ieteikumu (ES) 2017/1584 (2017. gada 13. septembris) par koordinētu reaģēšanu uz plašapmēra kiberdrošības incidentiem un krīzēm.

riska scenāriji, kurus izmantot aicināts Padomes secinājumos par Eiropas Savienības pozīcijas izstrādi kiberlietās, kas jāveic Komisijai, Augstajam pārstāvim un TID sadarbības grupai, koordinējoties ar attiecīgām civilām un militārām struktūrām un aģentūrām un izveidotiem tīkliem, to vidū *EU-CyCLONe*, kā arī sakaru tīklu un infrastruktūru riska novērtējums, kas pieprasīts Nevēras kopīgajā ministru aicinājumā un ko veic TID sadarbības grupa ar Komisijas un *ENISA* atbalstu un sadarbībā ar Eiropas Elektronisko sakaru regulatoru iestādi (*BEREC*), koordinētā riska novērtēšana, kas veicama saskaņā ar Direktīvas (ES) 2022/2555 22. pantu, un digitālās darbības noturības pārbaude, kas paredzēta Eiropas Parlamenta un Padomes Regulā (ES) 2022/2554[29]. Nozaru atlasē jāņem vērā arī Padomes ieteikums par koordinētu Savienības mēroga pieeju kritiskās infrastruktūras noturības stiprināšanai.

(30) Turklāt kiberavārijas mehānismam jāsniedz atbalsts citām sagatavotības darbībām un jāatbalsta sagatavotība citās nozarēs, uz kurām neattiecas tādu vienību koordinēta pārbaude, kuras darbojas ļoti kritiskās nozarēs. Minētajās darbībās var ietilpt dažādi valstu gatavības pasākumi.

(31) Kiberavārijas mehānismam arī jāsniedz atbalsts reaģēšanas darbībām kiberincidentos, lai mazinātu ievērojamu un plašu kiberincidentu ietekmi, atbalstītu tūlītēju atkopšanos vai atjaunotu būtiskāko dienestu darbību. Attiecīgā gadījumā tam jāpapildina *UCPM*, lai nodrošinātu visaptverošu pieeju reaģēšanai uz kiberincidentu ietekmi uz pilsoņiem.

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

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

(34) Lai izvēlētos privātos pakalpojumu sniedzējus pakalpojumu sniegšanai ES kiberdrošības rezervju sakarā, ir jānosaka minimālo kritēriju kopums, kas iekļaujams uzaicinājumā iesniegt piedāvājumus, lai atlasītu šos pakalpojumu sniedzējus, tādējādi nodrošinot, ka tiek apmierinātas to dalībvalstu iestāžu un vienību vajadzības, kuras darbojas kritiskās vai ļoti kritiskās nozarēs.

---

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

(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 kiberavārijas mehānisms.

(36) Lai tuvinātu šīs regulas mērķus veicināt kopīgu stāvokļa apzināšanos, uzlabot Savienības noturību un sagādāt iespēju efektīvi reaģēt uz ievērojamiem un plašiem kiberincidentiem, *EU-CyCLONe*, *CSIRT* tīklam vai Komisijai jāvar lūgt *ENISA* izskatīt un novērtēt briesmas, vājās vietas un seku mazināšanas darbības konkrēta ievērojama vai plaša kiberincidenta sakarā. Pēc incidenta izskatīšanas un novērtēšanas *ENISA* sadarbībā ar attiecīgajām ieinteresētajām personām, ieskaitot privātā sektora, dalībvalstu, Komisijas un citu attiecīgo ES iestāžu, struktūru un aģentūru pārstāvjus, jāsagatavo incidenta pārskata ziņojums. Attiecībā uz privāto sektoru *ENISA* veido kanālus informācijas apmaiņai ar specializētiem pakalpojumu sniedzējiem, arī pārvaldītu drošības risinājumu pagādātājiem un pārdevējiem, lai palīdzētu izpildīt *ENISA* uzdevumu visā Savienībā panākt vienādi augstu kiberdrošību. Pamatojoties uz sadarbību ar ieinteresētajām personām, ieskaitot privāto sektoru, pārskata ziņojumam par konkrētiem incidentiem jābūt mērķim pēc incidenta novērtēt tā cēloņus, ietekmi un seku mazinājumu. Īpaša uzmanība jāpievērš to pārvaldīto drošības pakalpojumu sniedzēju ieguldījumam un pieredzei, kuri atbilst šīs regulas noteiktajiem visaugstākās profesionālās godprātības, objektivitātes un nepieciešamo tehnisko zināšanu nosacījumiem. Ziņojums jāiesniedz *EU-CyCLONe*, *CSIRT* tīklam un Komisijai un jāizmanto to darbā. Ja incidents ir saistīts ar trešu valsti, Komisijai par to jāinformē arī Augstais pārstāvis.

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

(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 plašos kiberincidentos, 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.

(39) Šīs regulas mērķi Savienība var sasniegt labāk nekā dalībvalstis. Tātad Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteiktajiem

subsidiaritātes un proporcionalitātes principiem. Šī regula nosaka vienīgi pasākumus, kuri nepieciešami 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 kiberapdraudējumu un kiberincidentus, tiem sagatavoties un uz tiem reaģēt, sevišķi ar šādām darbībām:

a) drošības operāciju centru Eiropas mēroga infrastruktūras ("Eiropas kibervairoga") ierīkošana, lai izveidotu un uzlabotu kopīgas atklāšanas un stāvokļa apzināšanās spējas;

b) kiberavārijas mehānisma izveide, kas palīdzētu dalībvalstīm sagatavoties ievērojamiem un plašiem kiberincidentiem, uz tiem reaģēt un pēc tiem tūdaļ atkopties;

c) Eiropas kiberincidentu izskatīšanas mehānisma izveide ievērojamu vai plašu incidentu izskatīšanai un novērtēšanai.

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

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

b) visā Savienībā stiprināt to vienību gatavību, kuras darbojas kritiskās un ļoti kritiskās nozarēs, un stiprināt solidaritāti, attīstot spējas vienoti reaģēt ievērojama vai plaša kiberincidenta gadījumā, arī darot pieejamu Savienības atbalstu ar programmu "Digitālā Eiropa" ("PDE") asociētajām trešajām valstīm reaģēšanai uz kiberincidentiem;

c) uzlabot Savienības noturību un veicināt efektīvu reaģēšanu, izskatot un novērtējot ievērojamus vai plašus incidentus, arī gūstot labu mācību un attiecīgos gadījumos izstrādājot ieteikumus.

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:

(1) **"pārrobežu drošības operāciju centrs" ("pārrobežu DOC")** ir daudzvalstu platforma, kas koordinētā tīkla struktūrā apvieno DOC no vismaz trim dalībvalstīm, kuras veido mitināšanas konsorciju, un ir izstrādāta, lai novērstu kiberapdraudējumu un kiberincidentus un atbalstītu kvalitatīvu izlūkdatu sagatavošanu, galvenokārt – mainoties ar datiem no dažādiem publiskiem un privātiem avotiem, kā arī daloties modernos rīkos un uzticamā vidē kopīgi attīstot kiberapdraudējuma atklāšanas, analīzes un novēršanas un aizsardzības spējas;

(2) **"publiska struktūra"** ir publisko tiesību subjekts, kas definēts Eiropas Parlamenta un Padomes Direktīvas 2014/24/ES[30] 2. panta 1. punkta 4) apakšpunktā;

3) **"mitināšanas konsorcijs"** ir konsorcijs, kas sastāv no piedalīgajām valstīm, kuras pārstāv valstu DOC un kuras ir piekritušas izveidot un veicināt rīku un infrastruktūras iegādi pārrobežu DOC vajadzībām un darbībai;

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

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

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

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

(8) **"plašs kiberincidents"** ir Direktīvas (ES) 2022/2555 6. panta 7. punktā definēts incidents;

(9) **"gatavība"** ir gatavība un spēja nodrošināt efektīvu un ātru reaģēšanu uz ievērojamu vai plašu kiberincidentu, kas panāktas iepriekšējas riska novērtēšanas un novērošanas rezultātā;

(10) **"reaģēšana"** ir rīcība ievērojama vai plaša kiberincidenta gadījumā vai tā laikā, vai pēc tā, lai pārvarētu tā tūlītējās un īslaicīgās negatīvās sekas;

[30] 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.).

(11) **“uzticami pakalpojumu sniedzēji”** ir Direktīvas (ES) 2022/2555 6. panta 40. punktā definētie pārvaldīto drošības pakalpojumu sniedzēji, kas atlasīti saskaņā ar šīs regulas 16. pantu.

II nodaļa

EIROPAS KIBERVAIROGS

3. pants

Eiropas kibervairoga izveide

1. Lai attīstītu progresīvas Savienības spējas atklāt, analizēt un apstrādāt datus par kiberdraudiem un incidentiem Savienībā, tiek izveidota savstarpēji savienota drošības operāciju centru Eiropas mēroga infrastruktūra (“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 sakopo un kopīgo dažādu avotu datus par kiberapdraudējumu un incidentiem;

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;

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. Dalībai Eiropas kibervairogā katra dalībvalsts norīko vismaz vienu savu DOC. Valsts DOC ir publiskā sektora struktūra.

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

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

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.

2. Pēc uzaicinājuma izteikt ieinteresētību *ECCC* atlasa mitināšanas konsorciju dalībai ar *ECCC* kopīgā rīku un infrastruktūru iepirkumā. *ECCC* var mitināšanas konsorcijam piešķirt dotāciju rīku un infrastruktūru darbības finansēšanai. Savienības finansiālās iemaksas sedz līdz 75 % rīku un infrastruktūras iegādes izmaksu un līdz 50 % darbības izmaksu, bet mitināšanas konsorcijs sedz atlikušās izmaksas. Pirms rīku un infrastruktūras iegādes procedūras *ECCC* un mitināšanas konsorcijs noslēdz mitināšanas un izmantošanas līgumu, kurā reglamentē rīku un infrastruktūras izmantošanu.

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) ir domāta tam, lai novērstu un atklātu incidentus, uz tiem reaģētu vai pēc tiem atkoptos, vai mazinātu to ietekmi;

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 ievērojamu 1. punktā minēto datu apjomu un nosacījumus, ar kuriem 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, pārrobežu DOC nodrošina augstu savstarpēju sadarbspēju. Lai veicinātu pārrobežu DOC sadarbspēju, Komisija var ar īstenošanas aktiem, konsultējusies ar *ECCC*, detalizēti noteikt sadarbspējas nosacījumus. Minētos īstenošanas aktus pieņem saskaņā ar šīs regulas 21. panta 2. punktā minēto pārbaudes procedūru.

4. Pārrobežu DOC cits ar citu noslēdz sadarbības nolīgumus, nosakot pārrobežu platformu informācijas kopīgošanas principus.

7. pants

Sadarbība un dalīšanās informācijā ar Savienības struktūrām

1. Ja pārrobežu DOC iegūst informāciju par potenciālu vai notiekošu plaša mēroga kiberincidentu, tie bez liekas kavēšanās sniedz attiecīgu informāciju *EU-CyCLONe*, *CSIRT* tīklam un Komisijai, ņemot vērā to attiecīgās krīzes pārvarēšanas funkcijas saskaņā ar Direktīvu (ES) 2022/2555.

2. Komisija var ar īstenošanas aktiem noteikt 1. punktā noteiktās informācijas kopīgošanas kārtību. Minētos īstenošanas aktus pieņem saskaņā ar šīs regulas 21. panta 2. punktā minēto pārbaudes procedūru.

8. pants

Drošība

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

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. Šajā darbībā Komisija ar Augstā pārstāvja atbalstu ievēro attiecīgā aizsardzības līmeņa drošības standartus, lai veicinātu sadarbību ar militārām iestādēm.

III nodaļa

KIBERAVĀRIJAS MEHĀNISMS

9. pants

Kiberavārijas mehānisma izveide

1. Lai uzlabotu Savienības noturību pret ievērojamu kiberdrošības apdraudējumu un solidāri sagatavotos ievērojamu un plašu kiberincidentu īslaicīgai ietekmei un to mazinātu, tiek izveidots kiberavārijas mehānisms (“mehānisms”).

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

10. pants

Darbību veidi

1. Mehānisms atbalsta šādas darbības:

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

b) reaģēšanas darbības, kas atbalsta reaģēšanu uz ievērojamiem un plašiem kiberincidentiem un tūlītēju atkopšanos pēc tiem un kas jāveic uzticamiem 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.

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 ļoti kritiskajām nozarēm, no kurām vienības var pakļaut koordinētai gatavības pārbaudei, ņemot vērā iegūtos un plānotos koordinētos riska novērtējumus un noturības pārbaudes Savienības līmenī.

2. TID sadarbības grupa sadarbībā ar Komisiju, *ENISA* un Augsto pārstāvi izstrādā kopīgus riska scenārijus un metodiku koordinētajiem pārbaudes pasākumiem.

12. pants

ES kiberdrošības rezervju izveide

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

2. ES kiberdrošības rezerves veido reaģēšanas uz incidentiem pakalpojumi no uzticamiem pakalpojumu sniedzējiem, kas atlasīti pēc 16. pantā noteiktajiem kritērijiem. Rezervēs ietilpst pakalpojumi, par kuriem iepriekš uzņemtas saistības. Pakalpojumi ir izvietojami visās dalībvalstīs.

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.

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

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

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

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

8. Komisija var ar īstenošanas aktiem noteikt ES kiberdrošības rezervēm nepieciešamo reaģēšanas pakalpojumu veidus un skaitu. Minētos īstenošanas aktus pieņem saskaņā ar 21. panta 2. punktā minēto pārbaudes procedūru.

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 ievērojamiem vai plašiem kiberincidentiem 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 var ar īstenošanas aktiem sīkāk noteikt ES kiberdrošības rezervju atbalsta pakalpojumu piešķiršanas kārtību. Minētos īstenošanas aktus pieņem saskaņā ar 21. panta 2. punktā minēto pārbaudes procedūru.

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 nekavējoties nosūta 12. panta 3. punktā minētajiem lietotājiem.

2. Pieprasījumu prioritarizēšanai vairāku vienlaicīgu pieprasījumu gadījumā attiecīgi ņemami vērā šādi kritēriji:

a) kiberincidenta smagums;

b) skartās vienības veids, augstāk prioritarizējot incidentus, kuri skar Direktīvas (ES) 2022/2555 3. panta 1. punktā definētās būtiskās vienības;

c) iespējamā ietekme uz skartajām dalībvalstīm vai lietotājiem;

d) incidenta iespējamais pārrobežu raksturs un briesmas, ka tas pārmetīsies uz citām dalībvalstīm vai lietotājiem;

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.

4. Šā panta 3. punktā minētie nolīgumi var būt pēc parauga, ko sagatavojusi *ENISA* pēc apspriešanās ar dalībvalstīm.

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

6. Viena mēneša laikā pēc atbalsta darbības beigām lietotāji iesniedz Komisijai un *ENISA* 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.

7. Komisija regulāri ziņo TID sadarbības grupai par atbalsta izmantošanu un rezultātiem.

15. pants

Koordinācija ar krīzes pārvarēšanas mehānismiem

1. Gadījumos, kad ievērojamu vai plašu kiberincidentu cēlonis vai sekas ir katastrofa, kas definēta Lēmumā Nr. 1313/2013/ES[31], šajā regulā paredzētais atbalsts reaģēšanai uz tādiem incidentiem papildina Lēmuma Nr. 1313/2013/ES darbības, to neskarot.

2. Plaša pārrobežu kiberincidenta 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, kiberavārijas mehānisma atbalsts var papildināt palīdzību, ko sniedz kopīgajā ārpolitikā un drošības politikā un kopīgajā drošības un aizsardzības politikā, arī caur kiberdrošības ātrās reaģēšanas vienībām. Tas var arī papildināt vai veicināt palīdzību, ko dalībvalsts sniedz citai dalībvalstij uz Līguma par Eiropas Savienību 42. panta 7. punkta pamata.

4. Kiberavārijas mehānisma atbalsts var ietilpt Savienības un dalībvalstu kopīgajā reaģēšanā Līguma par Eiropas Savienības darbību 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, veicinot arī kiberdrošības prasmju attīstību ES.

[31] 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 jutīgu informāciju, kas saistīta ar pakalpojumu, sevišķi pierādījumus, konstatējumus un ziņojumus, un atbilst Savienības drošības noteikumiem 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 aparatūru un programmatūras tehnisko aprīkojumu;

g) pakalpojumu sniedzējs spēj pierādīt, ka tam ir pieredze līdzīgu pakalpojumu sniegšanā attiecīgām valsts iestādēm vai vienībām, kas darbojas kritiskās vai ļoti 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, kurās tas spēj pakalpojumu īstenot;

j) kad ir ieviesta ES sertifikācijas shēma pārvaldīto drošības pakalpojumu Regulai (ES) 2019/881, pakalpojumu sniedzējs tiek sertificēts pēc minētās shēmas.

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 ievērojamiem vai plašiem kiberincidentiem, 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 ar Augsto pārstāvi koordinē darbību ar saņemtajiem pieprasījumiem un no ES kiberdrošības rezervēm trešām valstīm piešķirtā atbalsta īstenošanu.

IV nodaļa

KIBERINCIDENTU IZSKATĪŠANAS MEHĀNISMS

18. pants

Kiberincidentu izskatīšanas mehānisms

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

2. Lai sagatavotu 1. punktā minēto incidentu pārskata ziņojumu, *ENISA* sadarbojas ar visām attiecīgajām ieinteresētajām personām, ieskaitot dalībvalstu, Komisijas, citu attiecīgo ES iestāžu, struktūru un aģentūru pārstāvjus, pārvaldīto drošības pakalpojumu sniedzējus un kiberdrošības pakalpojumu lietotājus. Attiecīgā gadījumā *ENISA* sadarbojas arī ar ievērojamu vai plašu kiberincidentu 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 ievērojamā vai plašā kiberincidenta 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.

4. Attiecīgā gadījumā ziņojumā sniedz ieteikumus 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:

(1) 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";

(2) pievieno šādu g) apakšpunktu:

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

a) 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[32], izņemot ES kiberdrošības rezervju īstenošanas darbības, ko īsteno Komisija un *ENISA*.";

2) regulas 9. pantu groza šādi:

[32] 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.–31. lpp.).

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

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

c) | 1 629 566 000 EUR konkrētajam mērķim Nr. 3 – Kiberdrošība un uzticamība;

d) | 482 347 000 EUR konkrētajam mērķim Nr. 4 – Padziļinātas digitālās prasmes";

b) pievieno šādu 8. punktu:

"8. Atkāpjoties no Regulas (ES, Euratom) 2018/1046 12. panta 4. punkta, neizmantotās saistību un maksājumu apropriācijas darbībām, 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.";

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

"2. Finansējumu no Programmas var sniegt jebkurā Finanšu regulā 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/XX 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) XXX/XXXX [Finanšu regulas pārstrādnes] 169. panta 3. punkta, vienas trešās valsts pieprasījums ir pietiekams, lai pilnvarotu Komisiju vai *ENISA* rīkoties.

Īstenojot ar Regulas (ES) 2023/XX 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) XXX/XXXX [Finanšu regulas pārstrādnes] 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:

“Darbībām, kuras īsteno ar Regulas (ES) 2023/XX 3. pantu izveidoto Eiropas kibervairogu, piemērojamie noteikumi ir Regulas (ES) 2023/XX 4. un 5. panta noteikumi. Gadījumā, kad šīs regulas noteikumi runā pretī Regulas (ES) 2023/XX 4. un 5. pantam, pārāki ir otrie un tos piemēro minētajām konkrētajām darbībām.”;

(5) regulas 19. pantu aizstāj ar šādu:

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

Regulas XXXX 4. pantā minētajiem valstu DOC un Regulas XXXX 5. pantā minētajam mitināšanas konsorcijam atbalstu dotāciju veidā *ECCC* var saskaņā ar Finanšu regulas 195. panta 1. punkta d) apakšpunktu tieši piešķirt bez uzaicinājuma iesniegt priekšlikumus.

Atbalstu dotāciju veidā kiberavārijas mehānismam, kas noteikts Regulas XXXX 10. pantā, *ECCC* var saskaņā ar Finanšu regulas 195. panta 1. punkta d) apakšpunktu tieši piešķirt dalībvalstīm bez uzaicinājuma iesniegt priekšlikumus.

Sakarā ar Regulas 202X/XXXX 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 ievērojamu vai plašu kiberincidentu, kas definēts Regulas XXXX 10. panta c) punktā, un saskaņā ar Finanšu regulas 193. panta 2. punkta otrās daļas a) apakšpunktu pienācīgi pamatotos gadījumos par attiecināmām var uzskatīt arī izmaksas, kas radušās pirms dotācijas pieteikuma iesniegšanas.”;

(6) I un II pielikumu groza saskaņā ar šīs regulas pielikumu.

20. pants

Izvērtēšana

[Četrus gadus pēc šīs regulas piemērošanas sākuma]Komisija iesniedz Eiropas Parlamentam un Padomei šīs regulas izvērtējumu un pārskatu.

21. pants

Komiteju procedūra

1. Komisijai palīdz ar Regulu (ES) 2021/694 izveidotā Programmas "Digitālā Eiropa" koordinācijas komiteja. 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 –	*Padomes vārdā –*
priekšsēdētāja	*priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

1.2. Attiecīgā politikas joma

1.3. Priekšlikums/iniciatīva attiecas uz:

1.4. Mērķi

1.4.1. Vispārīgie mērķi

1.4.2. Konkrētie mērķi

1.4.3. Paredzamie rezultāti un ietekme

1.4.4. Snieguma rādītāji

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, tostarp sīki izstrādāts iniciatīvas izvēršanas grafiks

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

1.7. Plānotās budžeta izpildes metodes

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

2.2. Pārvaldības un kontroles sistēma

2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums

2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu

2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

3.2.3.1. Aplēstās cilvēkresursu vajadzības

3.2.4. Saderība ar pašreizējo daudzgadu finanšu shēmu

3.2.5. Trešo personu iemaksas

3.3. Aplēstā ietekme uz ieņēmumiem

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Eiropas Parlamenta un Padomes Regula, ar ko nosaka pasākumus ar mērķi Savienībā stiprināt solidaritāti un spējas atklāt kiberdrošības apdraudējumus un incidentus, sagatavoties tiem un reaģēt uz tiem

1.2. Attiecīgā politikas joma

Digitālajam laikmetam gatava Eiropa

Eiropas stratēģiskās investīcijas

Darbība: Eiropas digitālās nākotnes veidošana

1.3. Priekšlikums/iniciatīva attiecas uz:

☒ **jaunu darbību**

☐ **jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību**[33]

☐ **esošas darbības pagarināšanu**

☐ **vienas vai vairāku darbību apvienošanu vai pārorientēšanu uz citu/jaunu darbību**

1.4. Mērķi

1.4.1. Vispārīgie mērķi

Kibersolidaritātes akts stiprinās solidaritāti Savienības līmenī, lai labāk atklātu kiberdrošības apdraudējumus un incidentus, sagatavotos tiem un reaģētu uz tiem. Tā mērķi ir šādi:

a) stiprināt kiberdraudu un kiberincidentu kopīgu atklāšanu un situācijas apzināšanos ES;

b) pastiprināt kritisko vienību gatavību visā ES un stiprināt solidaritāti, attīstot kopīgās spējas reaģēt uz ievērojamiem vai liela mēroga kiberdrošības incidentiem, tostarp darīt pieejamu atbalstu reaģēšanai uz incidentiem PDE asociētajām trešām valstīm;

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

[33] Kā paredzēts Finanšu regulas 58. panta 2. punkta a) vai b) apakšpunktā.

1.4.2. Konkrētie mērķi

Kibersolidaritātes akta mērķu kopums tiks sasniegts ar šādām darbībām:

a) izvērst drošības operāciju centru Eiropas mēroga infrastruktūru (Eiropas kibervairogs), lai veidotu un uzlabotu kopīgas atklāšanas un situācijas apzināšanās spējas;

b) izveidot kiberavārijas mehānismu, lai palīdzētu dalībvalstīm sagatavoties ievērojamiem un liela mēroga kiberdrošības incidentiem, reaģēt uz tiem un nekavējoties atgūties no tiem. Atbalstu reaģēšanai uz incidentiem dara pieejamu arī Eiropas Savienības iestādēm, struktūrām, birojiem un aģentūrām (ISBA).

Šīs darbības tiks atbalstītas ar finansējumu no PDE, kas ar šo leģislatīvo instrumentu tiks grozīta, lai tajā iekļautu iepriekš minētās darbības, paredzētu finansiālu atbalstu to attīstīšanai un precizētu finansiālā atbalsta saņemšanas nosacījumus;

c) izveidot Eiropas kiberdrošības incidentu pārskatīšanas mehānismu ievērojamu vai liela mēroga incidentu pārskatīšanai un novērtēšanai.

1.4.3. Paredzamie rezultāti un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz labuma guvējiem / mērķgrupām.

Priekšlikums sniegs ievērojamu labumu dažādām ieinteresētajām personām. Eiropas kibervairogs uzlabos dalībvalstu spējas atklāt kiberdraudus. Kiberavārijas mehānisms papildinās dalībvalstu darbības, sniedzot ārkārtas atbalstu, kas palīdzēs sagatavoties draudiem, reaģēt uz tiem un nekavējoties no tiem atgūties / atjaunot pamatpakalpojumu darbību. Šīs darbības stiprinās rūpniecības un uzņēmumu konkurētspēju Eiropā visā digitalizētajā ekonomikā un veicinās to digitālo pārveidi, paaugstinot kiberdrošības līmeni digitālajā vienotajā tirgū. Galvenais priekšlikuma mērķis ir palielināt kritiskās vai sevišķi kritiskās nozarēs darbojošos iedzīvotāju, uzņēmumu un vienību noturību pret augošajiem kiberdrošības apdraudējumiem, kuriem var būt postoša ietekme uz sabiedrību un ekonomiku. Tas tiks darīts, ieguldot rīkos, kas palīdzēs ātrāk atklāt kiberdrošības apdraudējumus un incidentus un reaģēt uz tiem un palīdzēs dalībvalstīm labāk sagatavoties ievērojamiem un liela mēroga kiberdrošības incidentiem, kā arī reaģēt uz tiem. Tam būtu arī jāpalīdz nodrošināt Eiropai lielākas spējas šajās jomās, jo īpaši spējas vākt un analizēt datus par kiberdrošības apdraudējumiem un incidentiem.

1.4.4. Snieguma rādītāji

Norādīt, pēc kādiem rādītājiem seko līdzi progresam un sasniegumiem.

Attiecībā uz solidaritātes veicināšanu Savienības līmenī varētu ņemt vērā vairākus rādītājus:

1) kopējā iepirkuma rezultātā iegūto kiberdrošības infrastruktūru vai rīku, vai gan infrastruktūru, gan rīku skaits;

2) to darbību skaits, ar kurām Ārkārtējas reaģēšanas mehānisma kiberdrošības jomā ietvaros atbalsta gatavību kiberdrošības incidentiem un reaģēšanu uz tiem.

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņā vai ilgtermiņā izpildāmās vajadzības, tostarp sīki izstrādāts iniciatīvas izvēršanas grafiks

Regulai vajadzētu būt pilnībā piemērojamai drīz pēc tās pieņemšanas, t. i., divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

1.5.2. Savienības iesaistīšanās pievienotā vērtība (tās pamatā var būt dažādi faktori, piemēram, koordinēšanas radītie ieguvumi, juridiskā noteiktība, lielāka rezultativitāte vai komplementaritāte). Šā punkta izpratnē "Savienības iesaistīšanās pievienotā vērtība" ir vērtība, kas veidojas Savienības iesaistīšanās rezultātā un kas papildina vērtību, kura veidotos, ja dalībvalstis rīkotos atsevišķi.

Tā kā kiberdrošības apdraudējumiem kopumā ir spēcīgs pārrobežu raksturs un aug to risku un incidentu skaits, kuru sekas sniedzas pāri valstu un nozaru robežām un papildus tieši skartajam produktam ietekmē vēl citus produktus, dalībvalstis vienas pašas nevar ar labiem rezultātiem sasniegt šīs intervences mērķus un ir vajadzīga kopīga rīcība un solidaritāte Savienības līmenī. Pieredze cīņā pret kiberdraudiem, kas izriet no kara pret Ukrainu, kā arī atziņas, kas gūtas Francijas prezidentūras laikā īstenotajās kiberdrošības mācībās (*EU CyCLES*), liecina: lai panāktu solidaritāti ES līmenī, būtu jāizstrādā konkrēti savstarpējā atbalsta mehānismi, jo īpaši sadarbība ar privāto sektoru. Ņemot to vērā, Padomes 2022. gada 23. maija secinājumos par Eiropas Savienības kiberdrošības statusa uzlabošanu Komisija tika aicināta iesniegt priekšlikumu par jaunu ārkārtas reaģēšanas fondu kiberdrošības jomā. Savienības līmenī sniegtais atbalsts un īstenotās darbības, kuru mērķis ir uzlabot kiberdrošības apdraudējumu atklāšanu un palielināt gatavību un reaģēšanas spējas, sniegtu pievienoto vērtību, jo tādējādi tiktu novērsta centienu dublēšanās Savienībā un dalībvalstīs. Tas ļautu labāk izmantot pastāvošos resursus un uzlabot koordināciju un informācijas apmaiņu par gūtajām atziņām.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Eiropas kibervairoga ietvaros īstenotās situācijas apzināšanās un draudu atklāšanas jomā PDE kiberdrošības darba programmas 2021.–2022. gadam ietvaros tika izsludināts uzaicinājums paust ieinteresētību par rīku un infrastruktūras kopīgu iepirkšanu ar mērķi izveidot pārrobežu drošības operāciju centrus un uzaicinājums pieteikties dotācijām, kas paredzētas tādu DOC spēju veidošanai, kuri strādā publiskā un privātā sektora organizāciju labā.

Attiecībā uz gatavību incidentiem un reaģēšanu uz tiem Komisija ir izveidojusi īstermiņa programmu dalībvalstu atbalstam, izmantojot papildu finansējumu, kas piešķirts Eiropas Savienības Kiberdrošības aģentūrai, lai nekavējoties palielinātu gatavību smagiem kiberincidentiem un spējas reaģēt uz tiem. Aptvertie pakalpojumi ietver gatavības nodrošināšanas darbības, piemēram, ielaušanās testēšanu kritiskajās vienībās, lai noteiktu to ievainojamību. Tā arī vairo iespējas palīdzēt dalībvalstīm tādu smagu incidentu gadījumā, kas skar kritiskās vienības. *ENISA* jau īsteno šo īstermiņa programmu un ir jau sniegusi attiecīgas vērtīgas atziņas, kas ir ņemtas vērā, gatavojot šo regulu.

1.5.4. Saderība ar daudzgadu finanšu shēmu un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

Kibersolidaritātes akts balstīsies uz darbībām, kuras pašlaik atbalsta Savienība un dalībvalstis un kuru mērķis ir uzlabot situācijas apzināšanos un kiberdraudu atklāšanu un reaģēt uz liela mēroga un pārrobežu kiberdrošības incidentiem. Šis instruments arī saskan ar citiem krīžu pārvarēšanas satvariem, ieskaitot *IPCR*, kopējo drošības un aizsardzības politiku, tostarp kiberdrošības ātrās reaģēšanas vienībām, un palīdzību, ko viena dalībvalsts sniedz citai dalībvalstij saskaņā ar Līguma par Eiropas Savienību 42. panta 7. punktu. Jaunais priekšlikums arī papildinātu un atbalstītu struktūras, kas izveidotas saskaņā ar citiem kiberdrošības instrumentiem, piemēram, Direktīvu (ES) 2022/2555 (“TID2 direktīva”) vai Regulu (ES) 2019/881 (“Kiberdrošības akts”).

1.5.5. Dažādo pieejamo finansēšanas iespēju, tostarp pārdales iespējas, novērtējums

ENISA uzticēto darbības jomu pārvaldība atbilst tās pašreizējām pilnvarām un vispārējiem uzdevumiem. Šīm darbības jomām varētu būt nepieciešami konkrēti profili vai jauni darba uzdevumi, bet tos var nodrošināt, izmantojot jau pastāvošos *ENISA* resursus un pārdalot vai sasaistot dažādus uzdevumus. *ENISA* pašlaik īsteno īstermiņa programmu, ko Komisija izveidoja 2022. gadā, lai nekavējoties palielinātu gatavību un spējas reaģēt uz smagiem kiberincidentiem. Tajā ietvertie pakalpojumi paredz iespējas palīdzēt dalībvalstīm tādu smagu incidentu gadījumā, kas skar kritiskās vienības. *ENISA* jau īsteno šo īstermiņa programmu un ir jau sniegusi attiecīgas vērtīgas atziņas, kas ir ņemtas vērā, gatavojot šo regulu. Īstermiņa programmai piešķirtos resursus varētu izmantot arī šīs regulas kontekstā.

1.6. Priekšlikuma/iniciatīvas ilgums un finansiālā ietekme

☒ **Ierobežots ilgums**

– ☒ Priekšlikuma/iniciatīvas darbības laiks: no dienas, kad pieņemts priekšlikums Eiropas Parlamenta un Padomes regulai ar mērķi Savienībā stiprināt solidaritāti un spējas atklāt kiberdrošības apdraudējumus un incidentus, sagatavoties tiem un reaģēt uz tiem ("Kibersolidaritātes akts").

– ☒ Finansiālā ietekme uz saistību apropriācijām – no 2023. līdz 2027. gadam, uz maksājumu apropriācijām – no 2023. līdz 2031. gadam[34].

☐ **Beztermiņa**

– Īstenošana ar uzsākšanas periodu no GGGG. līdz GGGG. gadam,

– pēc kura turpinās normāla darbība.

1.7. Plānotās budžeta izpildes metodes[35]

☒ Komisijas īstenota **tieša pārvaldība**:

– ☒ ko veic tās struktūrvienības, tostarp personāls Savienības delegācijās;

– ☐ ko veic izpildaģentūras.

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☒ **Netieša pārvaldība**, kurā budžeta izpildes uzdevumi uzticēti:

– ☐ trešām valstīm vai to izraudzītām struktūrām;

– ☐ starptautiskām organizācijām un to aģentūrām (precizēt);

– ☐ EIB un Eiropas Investīciju fondam;

– ☒ Finanšu regulas 70. un 71. pantā minētajām struktūrām;

– ☐ publisko tiesību subjektiem;

– ☐ privāttiesību subjektiem, kas veic sabiedrisko pakalpojumu sniedzēju uzdevumus, tādā mērā, kādā tiem ir pienācīgas finanšu garantijas;

– ☐ dalībvalstu privāttiesību subjektiem, kuriem ir uzticēta publiskā un privātā sektora partnerības īstenošana un ir pienācīgas finanšu garantijas;

---

34 Aktā paredzētajām darbībām būtu jāpiešķir atbalsts no nākamās daudzgadu finanšu shēmas.

35 Sīkāku informāciju par budžeta izpildes veidiem un atsauces uz Finanšu regulu sk. *BUDGpedia* tīmekļa vietnē: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

– ☐ subjektiem vai personām, kurām, ievērojot LESD V sadaļu, uzticēts īstenot konkrētas KĀDP darbības un kuras ir noteiktas attiecīgajā pamataktā.

– *Ja norādīti vairāki pārvaldības veidi, sniedziet papildu informāciju iedaļā "Piezīmes"!*

Piezīmes

Ar Eiropas kibervairogu saistītās darbības īstenos *ECCC*. Līdz brīdim, kad *ECCC* spēs izpildīt savu budžetu, šīs darbības *ECCC* vārdā īstenos Eiropas Komisija tiešās pārvaldības režīmā. *ECCC* var atlasīt vienības, pamatojoties uz uzaicinājumiem paust ieinteresētību piedalīties kopīgā rīku iepirkumā. *ECCC* var piešķirt dotācijas šo rīku ekspluatācijai. *ECCC* var piešķirt dotācijas arī gatavības nodrošināšanas darbībām kiberavārijas mehānisma ietvaros. Komisijai ir vispārēja atbildība par ES kiberdrošības rezerves īstenošanu. Komisija, izmantojot iemaksu nolīgumus, var pilnībā vai daļēji uzticēt ES kiberdrošības rezerves darbības nodrošināšanu un pārvaldību Eiropas Savienības Kiberdrošības aģentūrai. Šajā regulā paredzētās darbības, kas uzticētas *ENISA*, ir saskaņā ar tās pašreizējām pilnvarām. Minētās darbības ir šādas: i) atbalsts TID sadarbības grupai gatavības nodrošināšanas darbību izstrādē, kas tiek veikta saskaņā ar riska novērtējumiem; ii) atbalsts Komisijai ES kiberdrošības rezerves izveidē un īstenošanas uzraudzībā, arī atbalsta pieprasījumu saņemšanā un apstrādē; iii) veidņu izstrāde, lai atvieglotu atbalsta pieprasījumu iesniegšanu, un to konkrēto nolīgumu izstrāde, kas noslēdzami starp pakalpojumu sniedzēju un lietotāju, kuram tiek sniegts atbalsts no ES kiberdrošības rezerves; iv) ar konkrētiem ievērojamiem vai liela mēroga kiberdrošības incidentiem saistītu apdraudējumu, ievainojamības un ietekmes mazināšanas pasākumu pārskatīšana un novērtēšana un ziņojumu sagatavošana par to. Tiek lēsts, ka visi šie uzdevumi aizņems aptuveni septiņus pilnslodzes ekvivalentus no pastāvošajiem *ENISA* resursiem, un tie tiks pildīti, pamatojoties uz jau iegūtajām speciālajām zināšanām un sagatavošanās darbu, ko *ENISA* pašlaik veic izmēģinājuma projektā, kurš attiecas uz ārkārtas atbalstu gatavības nodrošināšanai un reaģēšanai uz incidentiem.

2. PĀRVALDĪBAS PASĀKUMI

2.1. Pārraudzības un ziņošanas noteikumi

Norādīt biežumu un nosacījumus.

Lai novērtētu jauno noteikumu iedarbīgumu, Komisija uzraudzīs to īstenošanu, piemērošanu un atbilstību tiem. Komisija četru gadu laikā pēc šīs regulas piemērošanas sākuma dienas iesniedz Eiropas Parlamentam un Padomei ziņojumu par šīs regulas izvērtēšanu un pārskatīšanu.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Ierosināto pārvaldības veidu, finansējuma apgūšanas mehānismu, maksāšanas kārtības un kontroles stratēģijas pamatojums

Ar regulu tiek ieviests satvars ES finansējuma īstenošanai ar mērķi palielināt kiberdrošības noturību, veicot darbības, kas uzlabo spējas atklāt ievērojamus un liela mēroga kiberdrošības incidentus, reaģēt uz tiem un atgūties no tiem. Komunikācijas tīklu, satura un tehnoloģiju (*CNECT*) ĢD struktūrvienības, kas atbild par attiecīgo politikas jomu, pārvaldīs regulas īstenošanu.

Lai veiktu jaunos uzdevumus, Komisijas dienestiem ir nepieciešami atbilstīgi resursi. Tiek lēsts, ka jaunās regulas izpildes panākšanai būs vajadzīgi 6 *FTE* (3 *AD* un 3 *CA*), lai nodrošinātu šādu uzdevumu veikšanu:

- noteikt gatavības nodrošināšanas darbības saskaņā ar riska novērtējumiem;
- nodrošināt pārrobežu DOC platformu sadarbspēju;
- izstrādāt potenciālos īstenošanas aktus (divus drošības operāciju centriem un divus kiberavārijas mehānismam);
- pārvaldīt DOC mitināšanas un lietošanas nolīgumus;
- izveidot un pārvaldīt ES kiberdrošības rezervi – tieši vai izmantojot iemaksu nolīgumu ar *ENISA*. Ja tiek noslēgts iemaksu nolīgums ar *ENISA* – izstrādāt un uzraudzīt iemaksu nolīguma īstenošanu attiecībā uz *ENISA* uzticētajiem uzdevumiem;
- piedalīties *ENISA* sasauktajās konsultatīvajās grupās, lai pārskatītu un novērtētu ievērojamus un liela mēroga kiberdrošības incidentus, un sagatavot attiecīgos ziņojumus.

2.2.2. Informācija par apzinātajiem riskiem un risku mazināšanai izveidoto iekšējās kontroles sistēmu

Attiecībā uz Eiropas kibervairogu apzinātais risks ir tāds, ka dalībvalstis pārrobežu DOC platformās vai starp pārrobežu platformām un citām attiecīgām vienībām ES līmenī nedalās pietiekami plašā būtiskā informācijā par kiberdraudiem. Lai mazinātu

šos riskus, finansējums tiks piešķirts pēc uzaicinājuma paust ieinteresētību, kurā dalībvalstis apņemsies dalīties ar noteiktu informācijas apjomu ES līmenī. Pēc tam šī apņemšanās tiks formalizēta mitināšanas un lietošanas nolīgumā, kas piešķirs *ECCC* pilnvaras veikt revīzijas, lai pārliecinātos, ka kopīgi iepirktie rīki un infrastruktūra tiek izmantoti saskaņā ar nolīgumu. Saistības pārrobežu drošības operāciju centros dalīties ar informāciju augstā līmenī tiks formalizētas konsorcija nolīgumā.

Risks, kas apzināts attiecībā uz kiberavārijas mehānismu, ir tāds, ka lietotāji, kas piedalās mehānismā, neveic pietiekamus pasākumus, lai nodrošinātu gatavību kiberuzbrukumiem. Šā iemesla dēļ, lai lietotāji varētu saņemt atbalstu no ES kiberdrošības rezerves, viņiem ir pienākums veikt šādus gatavības nodrošināšanas pasākumus. Iesniedzot pieprasījumus atbalstam no ES kiberdrošības rezerves, lietotājiem jāpaskaidro, kādi pasākumi jau ir veikti, lai reaģētu uz incidentu, un tie tiks ņemti vērā, novērtējot ES kiberdrošības rezervei iesniegtos pieprasījumus.

2.2.3. Kontroles izmaksefektivitātes (kontroles izmaksu attiecība pret attiecīgo pārvaldīto līdzekļu vērtību) aplēse un pamatojums un gaidāmā kļūdu riska līmeņa novērtējums (maksājumu izdarīšanas brīdī un slēgšanas brīdī)

Tā kā programmas "Digitālā Eiropa" dalības noteikumi, kas piemērojami saskaņā ar Kibersolidaritātes aktu sniegtajam atbalstam, ir līdzīgi tiem, ko Komisija izmantos savās darba programmās, un atbalsta saņēmēju loka riska profils ir līdzīgs kā tieši pārvaldītajās programmās, var gaidīt, ka kļūdas robeža būs līdzīga tai, ko Komisija paredzējusi programmai "Digitālā Eiropa", proti, tāda, kas sniedz pamatotu pārliecību, ka kļūdu risks daudzgadu izdevumu periodā katru gadu būs 2–5 % robežās, paturot prātā, ka galīgais mērķis ir panākt, lai daudzgadu programmu slēgšanas brīdī, pēc tam kad būs ņemta vērā visu veikto revīzijas pasākumu, korekciju un nepamatoti izmaksāto summu atmaksāšanas pasākumu finansiālā ietekme, atlikušais kļūdu īpatsvars būtu pēc iespējas tuvāks 2 %.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus, piemēram, krāpšanas apkarošanas stratēģijā iekļautos pasākumus.

Eiropas Kiberdrošības vairoga gadījumā *ECCC* būs pilnvaras piekļūt informācijai un veikt pārbaudes uz vietas, lai revidētu kopīgi iepirktos rīkus un infrastruktūras saskaņā ar mitināšanas un lietošanas nolīgumu, kas jānoslēdz starp mitinātājkonsorciju un *ECCC*.

Uz šai regulai nepieciešamajām papildu apropriācijām attieksies pašreizējie krāpšanas novēršanas pasākumi, ko piemēro Savienības iestādēm, struktūrām un aģentūrām.

3. PRIEKŠLIKUMA/INICIATĪVAS APLĒSTĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorijas un budžeta izdevumu pozīcijas

- Esošās budžeta pozīcijas

Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Nr.	Dif./nedif. [36]	no EBTA valstīm[37]	no kandidātvalstīm un potenciālajām kandidātvalstīm[38]	no citām trešām valstīm	citi piešķirtie ieņēmumi
1	02 04 01 10 – programma "Digitālā Eiropa" – kiberdrošība	Dif.	JĀ	JĀ	NĒ	NĒ
1	02 04 01 11 – programma "Digitālā Eiropa" – Eiropas Kiberdrošības rūpnieciskais, tehnoloģiju un pētniecības kompetenču centrs	Dif.	JĀ	JĀ	NĒ	NĒ
1	02 04 03 – programma "Digitālā Eiropa" – mākslīgais intelekts	Dif.	JĀ	JĀ	NĒ	NĒ
1	02 04 04 – programma "Digitālā Eiropa" – prasmes	Dif.	JĀ	JĀ	NĒ	NĒ
1	02 01 30 – atbalsta izdevumi programmai "Digitālā Eiropa"	Nedif.	JĀ	JĀ	NĒ	NĒ

[36] Dif. – diferencētās apropriācijas, nedif. – nediferencētās apropriācijas.
[37] EBTA – Eiropas Brīvās tirdzniecības asociācija.
[38] Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis.

3.2. Priekšlikuma aplēstā finansiālā ietekme uz apropriācijām

3.2.1. Kopsavilkums par aplēsto ietekmi uz darbības apropriācijām

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgas darbības apropriācijas

– ☒ Priekšlikumam/iniciatīvai ir vajadzīgas šādas darbības apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

Daudzgadu finanšu shēmas izdevumu kategorija	Nr.	1. **"Vienotais tirgus, inovācija un digitalizācija"**

Priekšlikums nepalielinās kopējo saistību līmeni programmā "Digitālā Eiropa". Ieguldījumu šajā iniciatīvā nodrošina, pārdalot saistības, proti, ar 2. SM un 4. SM saistībām palielinot 3. SM un *ECCC* budžetu. Ja DFS pārskatīšanas rezultātā tiktu palielinātas programmā "Digitālā Eiropa" ietvertās saistības, minēto palielinājumu varētu izmantot šai iniciatīvai.

CNECT ĢD			**2025.** gads	**2026.** gads	**2027.** gads	**2028.+** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
○ Darbības apropriācijas										
Budžeta pozīcija[39] 02.040110 (pārdale no 02.0403 un 02.0404)	Saistības	(1a)	15,000	15,000	6,000	*p.m.*				**36,000**
	Maksājumi	(2a)	15,000	15,000	6,000					**36,000**
Budžeta pozīcija 02.040111.02 (pārdale no 02.0403 un 02.0404)	Saistības	(1b)	13,000	23,000	28,000	*p.m.*				**64,000**
	Maksājumi	(2b)	8,450	18,200	25,250	12,100				**64,000**
Administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem[40]										

[39] Saskaņā ar oficiālo budžeta nomenklatūru.

[40] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

Budžeta pozīcija 02.0130		(3)	0,150	0,150	0,150	*p.m.*				0,450
KOPĀ *CNECT* ĢD apropriācijas	Saistības	=1a+1b +3	**28,150**	**38,150**	**34,150**	***p.m.***				**100,450**
	Maksājumi	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ KOPĀ darbības apropriācijas	Saistības	(4)	28,000	38,000	34,000	*p.m.*				**100,000**
	Maksājumi	(5)	23,450	33,200	31,250	12,100				**100,000**
○ KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem		(6)	0,150	0,150	0,150	*p.m.*				**0,450**
KOPĀ daudzgadu finanšu shēmas 1. IZDEVUMU KATEGORIJAS apropriācijas	Saistības	=4+ 6	**28,150**	**38,150**	**34,150**	***p.m.***				**100,450**
	Maksājumi	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

<u>Ja priekšlikums/iniciatīva ietekmē vairāk nekā vienu darbības izdevumu kategoriju, atkārtot iepriekš minēto iedaļu:</u>

○ KOPĀ darbības apropriācijas (visas darbības izdevumu kategorijas)	Saistības	(4)	28,000	38,000	34,000	*p.m.*				**100,000**
	Maksājumi	(5)	23,450	33,200	31,250	12,100				**100,000**
KOPĀ administratīvās apropriācijas, kas tiek finansētas no konkrētu programmu piešķīrumiem (visas darbības izdevumu kategorijas)		(6)	0,150	0,150	0,150					**0,450**
KOPĀ daudzgadu finanšu shēmas **1.–6. IZDEVUMU KATEGORIJAS apropriācijas** (atsauces summa)	Saistības	=4+ 6	**28,150**	**38,150**	**34,150**	***p.m.***				**100,450**
	Maksājumi	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Daudzgadu finanšu shēmas izdevumu kategorija	**7.**	"Administratīvie izdevumi"

Šī iedaļa būtu jāaizpilda, izmantojot administratīva rakstura budžeta datu izklājlapu, kas vispirms jānoformē tiesību akta finanšu pārskata pielikumā (Komisijas lēmuma par iekšējiem noteikumiem attiecībā uz Eiropas Savienības vispārējā budžeta Komisijas iedaļas izpildi 5. pielikums), kurš starpdienestu konsultāciju vajadzībām tiek augšupielādēts sistēmā *DECIDE*.

miljonos EUR (trīs zīmes aiz komata)

		2025. gads	**2026.** gads	**2027.** gads	**2028.+** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
CNECT ĢD									
○ Cilvēkresursi		0,786	0,786	0,786	*p.m.*				**2,358**
○ Citi administratīvie izdevumi		0,035	0,035	0,035	*p.m.*				**0,105**
KOPĀ *CNECT* ĢD	Apropriācijas	**0,821**	**0,821**	**0,821**					**2,463**

KOPĀ daudzgadu finanšu shēmas **7. IZDEVUMU KATEGORIJAS apropriācijas**	(Saistību summa = maksājumu summa)	**0,821**	**0,821**	**0,821**					**2,463**

miljonos EUR (trīs zīmes aiz komata)

		2025. gads	**2026.** gads	**2027.** gads	**2028.+** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
KOPĀ daudzgadu finanšu shēmas **1.–7. IZDEVUMU KATEGORIJAS**	Saistības	**28,971**	**38,971**	**34,971**	***p.m.***				**102,913**
	Maksājumi	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

apropriācijas										

3.2.2. Aplēstais iznākums, ko dos finansējums no darbības apropriācijām

Saistību apropriācijas miljonos EUR (trīs zīmes aiz komata)

Norādīt mērķus un iznākumus			**N** gads		**N+1** gads		**N+2** gads		**N+3** gads		Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)						**KOPĀ**	
	IZNĀKUMI																	
⇩	Veids [41]	Vidējās izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Daudzums	Izmaksas	Kopējais daudzums	Kopējās izmaksas
KONKRĒTAIS MĒRĶIS Nr. 1[42]…																		
– Iznākums																		
– Iznākums																		
– Iznākums																		
Starpsumma – konkrētais mērķis Nr. 1																		
KONKRĒTAIS MĒRĶIS Nr. 2…																		
– Iznākums																		
Starpsumma – konkrētais mērķis Nr. 2																		

41 Iznākumi ir attiecīgie produkti vai pakalpojumi (piemēram, finansēto studentu apmaiņu skaits, uzbūvēto ceļu garums kilometros utt.).

42 Kā aprakstīts 1.4.2. punktā "Konkrētie mērķi".

KOPSUMMAS																

3.2.3. Kopsavilkums par aplēsto ietekmi uz administratīvajām apropriācijām

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgas administratīvās apropriācijas

– ☒ Priekšlikumam/iniciatīvai ir vajadzīgas šādas administratīvās apropriācijas:

miljonos EUR (trīs zīmes aiz komata)

	2025. gads	2026. gads	2027. gads	N+3 gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			**KOPĀ**
Daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA								
Cilvēkresursi	0,786	0,786	0,786					**2,358**
Citi administratīvie izdevumi	0,035	0,035	0,035					**0,105**
Starpsumma – daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJA	**0,821**	**0,821**	**0,821**					**2,463**
Ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS[43]								
Cilvēkresursi								
Pārējie administratīvie izdevumi	0,150	0,150	0,150					**0,450**
Starpsumma – ārpus daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	**0,150**	**0,150**	**0,150**					**0,450**
KOPĀ	**0,971**	**0,971**	**0,971**					**2,913**

Vajadzīgās cilvēkresursu un citu administratīvu izdevumu apropriācijas tiks nodrošinātas no ĢD apropriācijām, kas jau ir piešķirtas darbības pārvaldībai un/vai ir pārdalītas attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtus papildu resursus un ņemot vērā budžeta ierobežojumus.

[43] Tehniskais un/vai administratīvais atbalsts un ES programmu un/vai darbību īstenošanas atbalsta izdevumi (kādreizējās BA pozīcijas), netiešā pētniecība, tiešā pētniecība.

3.2.3.1. Aplēstās cilvēkresursu vajadzības

– ☐ Priekšlikumam/iniciatīvai nav vajadzīgi cilvēkresursi

– ☒ Priekšlikumam/iniciatīvai ir vajadzīgi šādi cilvēkresursi:

Aplēse izsakāma ar pilnslodzes ekvivalentu

		2025. gads	**2026.** gads	**2027.** gads	**N+3** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
O Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)								
20 01 02 01 (Galvenā mītne un Komisijas pārstāvniecības)		3	3	3				
20 01 02 03 (Delegācijas)								
01 01 01 01 (Netiešā pētniecība)								
01 01 01 11 (Tiešā pētniecība)								
Citas budžeta pozīcijas (norādīt)								
O Ārštata darbinieki (izsakot ar pilnslodzes ekvivalentu *FTE*)[44]								
20 02 01 (*AC*, *END*, *INT*, ko finansē no vispārīgajām apropriācijām)		3	3	3				
20 02 03 (*AC*, *AL*, *END*, *INT* un *JPD* delegācijās)								
XX 01 xx **yy zz**[45]	– galvenajā mītnē							
	– delegācijās							
01 01 01 02 (*AC*, *END*, *INT* – netiešā pētniecība)								
01 01 01 12 (*AC*, *END*, *INT* – tiešā pētniecība)								
Citas budžeta pozīcijas (norādīt)								
KOPĀ		**6**	**6**	**6**				

XX ir attiecīgā politikas joma vai budžeta sadaļa.

Nepieciešamie cilvēkresursi tiks nodrošināti, izmantojot attiecīgā ĢD darbiniekus, kuri jau ir iesaistīti konkrētās darbības pārvaldībā un/vai ir pārgrupēti attiecīgajā ĢD, vajadzības gadījumā izmantojot arī vadošajam ĢD gada budžeta sadales procedūrā piešķirtos papildu resursus un ņemot vērā budžeta ierobežojumus.

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki	- Noteikt gatavības nodrošināšanas darbības saskaņā ar riska novērtējumiem (11. pants), - izstrādāt potenciālos īstenošanas aktus (divus drošības operāciju centriem un divus kiberavārijas mehānismam), - pārvaldīt DOC mitināšanas un lietošanas nolīgumus, - izveidot un pārvaldīt ES kiberdrošības rezervi – tieši vai izmantojot iemaksu nolīgumu ar *ENISA*.
Ārštata darbinieki	Ierēdņa uzraudzībā: - noteikt gatavības nodrošināšanas darbības saskaņā ar riska novērtējumiem (11. pants), - izstrādāt potenciālos īstenošanas aktus (divus drošības operāciju centriem un

44 *AC* – līgumdarbinieki, *AL* – vietējie darbinieki, *END* – valstu norīkotie eksperti, *INT* – aģentūru darbinieki, *JPD* – jaunākie eksperti delegācijās.

45 Ārštata darbiniekiem paredzēto maksimālo summu finansē no darbības apropriācijām (kādreizējām BA pozīcijām).

	divus kiberavārijas mehānismam), - pārvaldīt DOC mitināšanas un lietošanas nolīgumus, - izveidot un pārvaldīt ES kiberdrošības rezervi – tieši vai izmantojot iemaksu nolīgumu ar *ENISA*.

3.2.4. *Saderība ar pašreizējo daudzgadu finanšu shēmu*

Priekšlikuma/iniciatīvas finansēšanai:

– ☒ pilnīgi pietiek ar līdzekļu pārvietošanu daudzgadu finanšu shēmas (DFS) attiecīgajā izdevumu kategorijā

Aprakstiet, kas jāpārplāno, norādot attiecīgās budžeta pozīcijas un summas. Lielas pārplānošanas gadījumā sniedziet *Excel* tabulu.

	23	24	25	26	27	Kopā
1. SM	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
2. SM — sākotnējais	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Kiberiniciatīvai			18 000 000	28 000 000	19 000 000	65 000 000
2. SM — JAUNAIS	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
3. SM — 2024. g. BP	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
No 2. SM–4. SM			15 000 000	15 000 000	6 000 000	36 000 000
3. SM — jaunais	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC — sākotnējais	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
No 2. SM–4. SM			13 000 000	23 000 000	28 000 000	64 000 000
***ECCC* — jaunais**	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
4. SM — sākotnējais	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Kiberiniciatīvai			10 000 000	10 000 000	15 000 000	35 000 000
4. SM — JAUNAIS	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– ☐ jāizmanto no DFS attiecīgās izdevumu kategorijas nepiešķirtās rezerves un/vai īpašie instrumenti, kas noteikti DFS regulā

Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas un budžeta pozīcijas, atbilstošās summas un instrumentus, kurus ierosināts izmantot.

– ☐ jāpārskata DFS

Paskaidrojiet, kas jādara, norādot attiecīgās izdevumu kategorijas, budžeta pozīcijas un atbilstošās summas.

3.2.5. *Trešo personu iemaksas*

Priekšlikums/iniciatīva:

– ☒ neparedz trešo personu līdzfinansējumu

– ☐ paredz trešo personu sniegtu līdzfinansējumu atbilstoši šādai aplēsei:

Apropriācijas miljonos EUR (trīs zīmes aiz komata)

	N gads[46]	**N+1** gads	**N+2** gads	**N+3** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)			Kopā
Norādīt līdzfinansētāju struktūru								
KOPĀ līdzfinansētās apropriācijas								

[46] N gads ir gads, kurā priekšlikumu/iniciatīvu sāk īstenot. Aizstājiet "N" ar paredzēto pirmo īstenošanas gadu (piemēram, 2021.). Tas pats attiecas uz turpmākajiem gadiem.

3.3. Aplēstā ietekme uz ieņēmumiem

– ☒ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus.

– ☐ Priekšlikums/iniciatīva finansiāli ietekmē:

– ☐ pašu resursus

– ☐ citus ieņēmumus

– Atzīmējiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

miljonos EUR (trīs zīmes aiz komata)

Budžeta ieņēmumu pozīcija:	Kārtējā finanšu gadā pieejamās apropriācijas	Priekšlikuma/iniciatīvas ietekme[47]						
		N gads	**N+1** gads	**N+2** gads	**N+3** gads	Norādīt tik gadu, cik nepieciešams ietekmes ilguma atspoguļošanai (sk. 1.6. punktu)		
……. pants								

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgās budžeta izdevumu pozīcijas.

[…]

Citas piezīmes (piemēram, metode/formula, ko izmanto, lai aprēķinātu ietekmi uz ieņēmumiem, vai jebkura cita informācija).

[…]

[47] Norādītajām tradicionālo pašu resursu (muitas nodokļi, cukura nodevas) summām jābūt neto summām, t. i., bruto summām, no kurām atskaitītas iekasēšanas izmaksas 20 % apmērā.