Eiropas Savienības
Padome

Briselē, 2018. gada 14. septembrī
(OR. en)

12104/18

Starpiestāžu lieta:
2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

PAVADVĒSTULE

Sūtītājs:	Direktors *Jordi AYET PUIGARNAU* kungs, Eiropas Komisijas ģenerālsekretāra vārdā
Saņemšanas datums:	2018. gada 12. septembris
Saņēmējs:	Eiropas Savienības Padomes ģenerālsekretārs *Jeppe TRANHOLM-MIKKELSEN* kungs
K-jas dok. Nr.:	COM(2018) 630 final
Temats:	Priekšlikums - EIROPAS PARLAMENTA UN PADOMES REGULA, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu

Pielikumā ir pievienots dokuments COM(2018) 630 *final*.

Pielikumā: COM(2018) 630 *final*

EIROPAS
KOMISIJA

Briselē, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA,

ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu

Eiropas Komisijas ieguldījums vadītāju sanāksmē
Zalcburgā, 2018. gada 19.–20. septembrī

{SEC(2018) 396 final} - {SWD(2018) 403 final} - {SWD(2018) 404 final}

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

• Priekšlikuma pamatojums un mērķi

Ikdienas dzīve un ekonomika kļūst arvien vairāk atkarīga no digitālajām tehnoloģijām, un līdz ar to iedzīvotāji arvien vairāk ir pakļauti nopietniem kiberincidentiem. Gan civilā infrastruktūra, gan militārās spējas ir atkarīgas no drošām digitālajām sistēmām, tāpēc nākotnē drošības līmeni noteiks spēja uzlabot Savienības aizsargātību pret kiberdraudiem.

Lai risinātu arvien pieaugošās problēmas, Savienība ir pastāvīgi izvērsusi savu darbību šajā jomā, pamatojoties uz 2013. gada kiberdrošības stratēģiju,[1] tās mērķiem un principiem, kas paredz veicināt uzticamu, drošu un atvērtu kiberdrošības ekosistēmu. 2016. gadā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/1148[2] par tīklu un informācijas sistēmu drošību Savienība pieņēma pirmos pasākumus kiberdrošības jomā.

Ņemot vērā kiberdrošības jomas straujo attīstību, 2017. gada septembrī Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos iesniedza kopīgu paziņojumu[3] "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", lai vēl vairāk stiprinātu Savienības noturības, novēršanas un reaģēšanas spējas, kas ļautu stāties pretī kiberuzbrukumiem. Kopīgajā paziņojumā, kura pamatā ir arī iepriekš izvirzītas iniciatīvas, izklāstīts ierosināto darbību kopums, cita starpā iekļaujot Eiropas Savienības Tīklu un informācijas drošības aģentūras (*ENISA*) stiprināšanu, Savienības mēroga kiberdrošības brīvprātīgas sertifikācijas sistēmas izveidošanu, kas ļautu palielināt digitālās pasaules produktu un pakalpojumu kiberdrošību, kā arī plānu ātrai un koordinētai reaģēšanai uz liela mēroga kiberdrošības incidentiem un krīzēm.

Šajā kopīgajā paziņojumā tika atzīts, ka savu stratēģisko interešu nolūkā Savienībai arī jānodrošina būtisku kiberdrošības tehnoloģisko spēju saglabāšana un attīstīšana, lai aizsargātu savu digitālo vienoto tirgu un jo īpaši kritiskos tīklus un informācijas sistēmas, kā arī sniegtu svarīgākos kiberdrošības pakalpojumus. Savienībai jābūt spējīgai patstāvīgi nodrošināt savu digitālo aktīvu aizsardzību un konkurēt pasaules kiberdrošības tirgū.

Šobrīd Savienība ir kiberdrošības produktu un risinājumu neto importētāja un lielā mērā ir atkarīga no pakalpojumu sniedzējiem ārpus Eiropas[4]. Pasaules mērogā kiberdrošības tirgū, kura vērtība ir 600 miljardi eiro, nākamo piecu gadu laikā paredzams pieaugums vidēji par aptuveni 17 % pārdošanas, uzņēmumu skaita un nodarbinātības ziņā. Taču, raugoties no tirgus viedokļa, 20 vadošo kiberdrošības valstu vidū ir tikai 6 dalībvalstis[5].

Tajā pat laikā Savienībā ir uzkrāta ievērojama lietpratība un pieredze kiberdrošības jomā — Komisija, nesen apzinot kiberdrošības lietpratības centrus, reģistrējusi vairāk nekā

---

1 KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI "Eiropas Savienības kiberdrošības stratēģija — atvērta un droša kibertelpa", JOIN(2013) 1 *final*.

2 Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

3 KOPĪGS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", JOIN(2017) 450 *final*.

4 Galīgā ziņojuma projekts – kiberdrošības tirgus pētījumi, 2018. gads.

5 Galīgā ziņojuma projekts – kiberdrošības tirgus pētījumi, 2018. gads.

660 organizācijas no visas ES[6]. Šī lietpratība, ja tiktu izmantota tirgū pieprasītu produktu un risinājumu izstrādē, varētu sniegt Savienībai iespēju aptvert visu kiberdrošības vērtību ķēdi. Tomēr pētniecības un industriju kopienu centieni ir sadrumstaloti, tām trūkst savstarpējas saskaņotības un kopīga pamatuzdevuma, un tādējādi tiek kavēta ES konkurētspēja šajā jomā, kā arī mazināta tās spēja nodrošināt savu digitālo resursu drošību. Pašlaik attiecīgajām kiberdrošības nozarēm (piemēram, enerģētikai, kosmosam, aizsardzībai, transportam) un apakšnozarēm netiek sniegts pietiekami liels atbalsts[7]. Tāpat arī Eiropa pilnībā neizmanto sinerģijas starp civilajām un aizsardzības kiberdrošības nozarēm.

Savienības publiskā un privātā sektora partnerības kiberdrošības jomā (*cPPP*) izveide 2016. gadā bija stabils pirmais solis pētniecības, industrijas un publiskā sektora kopienu apvienošanā, lai veicinātu pētniecību un inovāciju kiberdrošības jomā, un 2014.–2020. gada finanšu shēmas robežās tai jāsniedz labi, koncentrētāki pētniecības un inovācijas rezultāti. Savienības kiberdrošības publiskā un privātā sektora partnerības izveide deva iespēju industrijas partneriem paust apņemšanos par saviem individuālajiem izdevumiem jomās, kas noteiktas partnerības stratēģiskā pētniecības un inovācijas programmā.

Tomēr Savienība var īstenot daudz lielāka mēroga investīcijas, un tai ir nepieciešams efektīvāks mehānisms, kas ļautu ilgstoši nostiprināt savas spējas, apvienot centienus un kompetences, stimulēt novatorisku risinājumu izstrādi, lai risinātu ar kiberdrošību saistītās industriālās problēmas jauno daudzfunkcionālo tehnoloģiju (piemēram, mākslīgā intelekta, kvantu skaitļošanas, blokķēžu un drošu digitālo identitāšu) jomā, kā arī kritiski svarīgos sektoros (piemēram, transporta, enerģētikas, veselības, finanšu, vispārējās valdības, telesakaru, ražošanas, aizsardzības un kosmosa sektorā).

Kopīgajā paziņojumā ir apsvērta iespēja pastiprināt Savienības kiberdrošības spējas, izveidojot kiberdrošības kompetenču centru tīklu, kura pamatā būtu Eiropas Kiberdrošības kompetenču centrs. Tas palīdzētu pastiprināt pašreizējos spēju veidošanas centienus šajā jomā Savienības un valstu līmenī. Kopīgajā paziņojumā ir izteikts Komisijas nodoms 2018. gadā uzsākt ietekmes novērtējumu, lai struktūras izveides nolūkā izskatītu pieejamos risinājumus. Sperot pirmo soli un domājot par turpmāko attīstību, Komisija uzsāka izmēģinājuma posmu programmas "Apvārsnis 2020" ietvaros, lai palīdzētu apvienot nacionālos centrus vienotā tīklā un radītu jaunu impulsu kiberdrošības kompetenču jomā un tehnoloģiju attīstībā.

Valstu un valdību vadītāji Tallinas digitālajā samitā 2017. gada septembrī aicināja Savienību "līdz 2025. gadam kļūt par pasaules līderi kiberdrošības jomā, lai nodrošinātu mūsu pilsoņu, patērētāju un uzņēmumu uzticēšanos, pārliecību un aizsardzību tiešsaistē, kā arī nodrošinātu likumā reglamentētu bezmaksas internetu".

2017. gada novembrī pieņemtie Padomes secinājumi[8] aicināja Komisiju ātri nodrošināt ietekmes novērtējumu par iespējamajiem risinājumiem un līdz 2018. gada vidum nākt klajā ar priekšlikumu par attiecīgo juridisko instrumentu iniciatīvas īstenošanai.

Digitālās Eiropas programma, ko Komisija ierosināja 2018. gada jūnijā[9]*,* sagatavota ar mērķi paplašināt un maksimāli izmantot digitalizācijas priekšrocības Eiropas pilsoņu un uzņēmumu

---

6 2018. gada Kopīgā pētniecības centra tehniskie ziņojumi: Eiropas kiberdrošības lietpratības centri.

7 Kopīgā pētniecības centra tehniskais ziņojums: apzināšanas projekta rezultāti (vairāk informācijas skatīt 4. un 5. pielikumā).

8 Padomes secinājumi par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", ko Vispārējo lietu padome pieņēma 2017. gada 20. novembrī.

labā visās attiecīgajās ES politikas jomās, stiprinot politikas un atbalstot digitālā vienotā tirgus mērķus. Programmā ir ierosināta saskanīga un visaptveroša pieeja, lai nodrošinātu efektīvāko jaunāko tehnoloģiju izmantošanas veidu, kā arī tehnisko spēju un cilvēku kompetenču pareizu kombināciju digitalizācijas procesam — ne tikai kiberdrošības jomā, bet arī attiecībā uz viedo datu infrastruktūru, mākslīgo intelektu, augstāka līmeņa prasmēm un to pielietošanu industrijā un sabiedriskas nozīmes jomās. Šie elementi ir savstarpēji atkarīgi, viens otru pastiprinoši, un, tos vienlaicīgi veicinot, ir iespējams sasniegt nepieciešamo līmeni datu ekonomikas uzplaukumam[10]. Arī nākamajā ES pētniecības un inovācijas pamatprogrammā – *"Apvārsnis Eiropa"* [11]– kiberdrošība ir izvirzīta kā viena no tās prioritātēm.

Šādā kontekstā šajā regulā tiek ierosināts izveidot Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu. Lai sekmētu Eiropas kiberdrošības tehnoloģisko un industriālo ekosistēmu, šim mērķim izveidotajam sadarbības modelim jāfunkcionē šādi: Kompetenču centrs sekmēs Tīkla darbību un palīdzēs to koordinēt, kā arī sniegs atbalstu kiberdrošības kompetenču kopienai, tādējādi veicinot kiberdrošības tehnoloģiskās darba kārtības virzību un atvieglojot iespējas izmantot šādi iegūtu lietpratību. Konkrēti, Kompetenču centrs, piešķirot dotācijas un rīkojot iepirkumus, īstenos Digitālās Eiropas programmas un pamatprogrammas "Apvārsnis Eiropa" attiecīgās daļas. Ņemot vērā citur pasaulē veiktās ievērojamās investīcijas kiberdrošības jomā un vajadzību koordinēt un apvienot attiecīgos resursus Eiropā, Kompetenču centru ierosināts veidot kā Eiropas partnerību[12], kas tādējādi ļaus vienkāršāk Savienībai, dalībvalstīm un/vai industrijai veikt kopīgas investīcijas. Tādēļ priekšlikumā noteikts, ka Kompetenču centra un Tīkla darbībās dalībvalstīm jāsniedz proporcionāli atbilstošs ieguldījums. Galvenā lēmumu pieņemšanas struktūra ir Valde, kurā pārstāvētas visas dalībvalstis, taču balsošanas tiesības tajā būs tikai tām dalībvalstīm, kuras piedalās ar savu finansiālo ieguldījumu. Balsošanas mehānisms Valdē veidots pēc divkāršā vairākuma principa, kas paredz, ka jābūt nodrošinātiem 75 % finansiālā ieguldījuma un 75 % balsu. Atbilstīgi Komisijas atbildības līmenim Savienības budžeta veidošanā Komisijai pieder 50 % balsu. Darbojoties Valdē, Komisija vajadzības gadījumā izmantos Eiropas Ārējās darbības dienestā gūto lietpratību. Lai uzturētu regulāru dialogu ar privāto sektoru, patērētāju organizācijām un citām ieinteresētajām personām, Valdei palīdz Industriālā un zinātniskā konsultatīvā padome.

Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs ciešā sadarbībā ar šīs regulas izveidoto Nacionālo koordinācijas centru tīklu un kiberdrošības kompetenču kopienu (tostarp kiberdrošības tehnoloģiju izstrādē iesaistīto apjomīgu un daudzveidīgu dalībnieku kopumu, piemēram, pētniecības subjektiem, piedāvājuma un pieprasījuma puses industrijām, kā arī publiskā sektora pārstāvjiem) būtu galvenā īstenošanas struktūra attiecībā uz ES finanšu līdzekļiem, kas atvēlēti kiberdrošībai saskaņā ar ierosināto *Digitālās Eiropas programmu* un *pamatprogrammu "Apvārsnis Eiropa"*.

Šāda visaptveroša pieeja ļautu atbalstīt kiberdrošību visā vērtību ķēdē, sākot ar pētniecību un beidzot ar atbalstu svarīgāko tehnoloģiju ieviešanai un izmantošanai. Dalībvalstu finansiālajai

---

9 Priekšlikums Eiropas Parlamenta un Padomes regulai, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu, COM(2018) 434.

10 Skatīt SWD(2018) 305.

11 Priekšlikums Eiropas Parlamenta un Padomes regulai par pētniecības un inovācijas pamatprogrammas "Apvārsnis Eiropa" izveidi un dalības un rezultātu izplatīšanas noteikumiem, COM(2018) 435.

12 Kā definēts priekšlikumā Eiropas Parlamenta un Padomes regulai par pētniecības un inovācijas pamatprogrammas "Apvārsnis Eiropa" izveidi un dalības un rezultātu izplatīšanas noteikumiem, COM(2018) 435, un kā minēts priekšlikumā Eiropas Parlamenta un Padomes regulai, ar ko laikposmam no 2021. līdz 2027. gadam izveido Digitālās Eiropas programmu, COM(2018) 434.

līdzdalībai šajā iniciatīvā jābūt samērīgai ar ES finansiālo ieguldījumu — tā ir neaizstājams iniciatīvas panākumu elements.

Ņemot vērā tās lietpratību, kā arī plašo un nozīmīgo ieinteresēto personu pārstāvību, Eiropas Kiberdrošības organizācija, kas saskaņā ar pamatprogrammu "Apvārsnis 2020" kiberdrošības jomā izveidotajā līgumiskajā publiskā un privātā sektora partnerībā pilda tādas pašas funkcijas kā Komisija, jāpieaicina sniegt ieguldījumu Kompetenču centra un Tīkla darbībā.

Turklāt Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram jācenšas arī uzlabot sinerģijas starp kiberdrošības civilajām un aizsardzības dimensijām. Tam jānodrošina atbalsts dalībvalstīm un citiem iesaistītajiem dalībniekiem, sniedzot padomus, daloties lietpratībā un veicinot sadarbību attiecībā uz projektiem un darbībām. Pēc dalībvalstu lūguma tas varētu pildīt arī projektu vadītāja funkcijas, jo īpaši saistībā ar Eiropas Aizsardzības fondu. Šīs iniciatīvas mērķis ir sniegt ieguldījumu tālāk izklāstīto problēmu risināšanā.

- **Nepietiekama sadarbība starp kiberdrošības pieprasījuma un piedāvājuma puses industrijām.** Problēmas, ar ko saskaras Eiropas uzņēmumi, ir saistītas gan ar savas drošības nodrošināšanu, gan drošu produktu un pakalpojumu piedāvāšanu saviem klientiem. Tomēr bieži vien tie nespēj pienācīgi aizsargāt savus jau pastāvošos produktus, pakalpojumus un aktīvus vai izstrādāt drošus, inovatīvus produktus un pakalpojumus. Galvenie kiberdrošības aktīvi bieži vien ir pārāk dārgi, lai tos izstrādātu un ieviestu atsevišķi uzņēmēji, kuru pamatdarbība nav saistīta ar kiberdrošību. Tajā pat laikā saikne starp kiberdrošības tirgus pieprasījumu un piedāvājumu nav pietiekami labi attīstīta, kā rezultātā netiek nodrošināta dažādu nozaru vajadzībām pielāgotu Eiropas produktu un risinājumu pietiekami optimāla piegāde, turklāt tirgus dalībnieku starpā nevalda pietiekami augsta uzticība.
- **Dalībvalstu efektīvas sadarbības mehānisma trūkums industriālo spēju veidošanai.** Pašlaik trūkst efektīva sadarbības mehānisma, kas ļautu dalībvalstīm kopīgi strādāt, lai veidotu nepieciešamās spējas kiberdrošības inovācijas atbalstam industrijas nozarēs un plašāk ieviestu progresīvus Eiropas kiberdrošības risinājumus. Pašreizējie dalībvalstu sadarbības mehānismi kiberdrošības jomā saskaņā ar Direktīvu (ES) 2016/1148 savās pilnvarās neparedz šāda veida pasākumus.
- **Nepietiekama sadarbība pētniecības un industrijas kopienu ietvaros un starp tām.** Neskatoties uz Eiropas teorētiskajām iespējām pilnībā aptvert kiberdrošības vērtību ķēdi, pastāv būtiskas kiberdrošības nozares (piemēram, enerģētika, kosmoss, aizsardzība, transports) un apakšnozares, kam nav pietiekama pētniecības kopienas atbalsta vai ko atbalsta tikai ierobežots skaits pētniecības centru (piemēram, pēckvantu un kvantu kriptogrāfija, mākslīgā intelekta uzticamība un kiberdrošība). Lai arī šāda sadarbība acīmredzami pastāv, tā ļoti bieži tiek īstenota īstermiņā konsultatīvā veidā, neļaujot iesaistīties ilgtermiņa pētniecības plānos kiberdrošības industriālo problēmu risināšanai.
- **Nepietiekama sadarbība starp civilajām un aizsardzības kiberdrošības pētniecības un inovācijas kopienām.** Nepietiekamas sadarbības problēma attiecas arī uz civilajām un aizsardzības kopienām. Esošās sinerģijas netiek pilnībā izmantotas, jo trūkst efektīvu mehānismu, kas ļautu šīm kopienām produktīvi sadarboties un veicinātu uzticēšanos, kas šeit pat vairāk nekā citās jomās ir sekmīgas sadarbības priekšnosacījums. Jārēķinās arī ar ierobežotajām finanšu spējām ES kiberdrošības tirgū, tostarp nepietiekamiem līdzekļiem inovācijas atbalstam.
- **Saskanība ar pašreizējiem noteikumiem konkrētajā politikas jomā**

Kiberdrošības kompetenču tīkls un Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs darbosies kā papildu atbalsts esošajiem kiberdrošības politikas noteikumiem un dalībniekiem. Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra pilnvarojums papildinās *ENISA* centienus, taču centra darbībai ir cita ievirze un tam vajadzīgs citādu prasmju kopums. *ENISA* pilnvarās ir paredzēta konsultatīva loma ES kiberdrošības pētniecības un inovācijas jomā, taču tagad ierosinātās pilnvaras galvenokārt vērstas uz citiem būtiskiem uzdevumiem ES kiberdrošības noturības stiprināšanai. Turklāt *ENISA* pilnvarās nav atrunāti pasākumu veidi, kas ietilptu Kiberdrošības centra un Tīkla galvenajos uzdevumos — tehnoloģiju izstrādes un plašākas ieviešanas stimulēšana kiberdrošības jomā, kā arī šīs jomas spēju veidošanas centienu papildināšana ES un valstu līmenī.

Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs kopā ar Kiberdrošības kompetenču tīklu strādās arī pētniecības atbalsta nolūkā, lai atvieglotu un paātrinātu standartizācijas un sertifikācijas procesus, jo īpaši tos, kas saistīti ar kiberdrošības sertifikācijas shēmām ierosinātā Kiberdrošības akta izpratnē[13][14].

Šī iniciatīva *de facto* stiprina publiskā un privātā sektora partnerības kiberdrošības jomā (*cPPP*) potenciālu; tas bija pirmais ES mēroga mēģinājums apvienot kiberdrošības industriju, pieprasījuma pusi (kiberdrošības produktu un risinājumu pircējus, tostarp publiskās pārvaldes pārstāvjus un kritiski svarīgu nozaru, piemēram, transporta, veselības, enerģētikas, finanšu nozares, pārstāvjus) un pētniecības kopienu, lai izveidotu platformu ilgtspējīgam dialogam un radītu apstākļus brīvprātīgām līdzinvestīcijām. Šī publiskā un privātā sektora partnerība kiberdrošības jomā tika izveidota 2016. gadā, un līdz 2020. gadam tā radītu investīcijas 1,8 miljardu EUR apmērā. Tomēr investīciju apjoms citās pasaules daļās (piemēram, ASV 2017. gadā vien kiberdrošības nozarē investēja 19 miljardus USD) liecina, ka ES jādara vairāk, lai nodrošinātu investīciju kritisko masu un pārvarētu spēju sadrumstalotību visā ES.

- **Saskanība ar citām ES politikas jomām**

Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs darbosies kā vienota īstenošanas struktūra dažādām Savienības programmām, kas atbalsta kiberdrošību, piemēram Digitālās Eiropas programmai un pamatprogrammai "Apvārsnis Eiropa", kā arī uzlabos saskaņotību un sinerģiju.

Šī iniciatīva arī ļaus papildināt dalībvalstu centienus, jo sniegs atbilstošu ieguldījumu izglītības politikas veidošanā, lai uzlabotu kiberdrošības prasmes (piemēram, izstrādājot kiberdrošības mācību programmas civilajās un militārajās izglītības sistēmās) un palīdzētu veidot kvalificētu darbaspēku ES kiberdrošības jomā — tas būtu būtisks ieguvums ne vien kiberdrošības uzņēmumiem, bet arī citām ar kiberdrošību saistītām industrijām. Attiecībā uz izglītību un apmācību kiberaizsardzības jomā šī iniciatīva veidota atbilstīgi darbam, kas patlaban notiek saistībā ar Eiropas Drošības un aizsardzības koledžā izveidoto kiberaizsardzības izglītības, apmācības un mācību platformu.

---

13 Priekšlikums EIROPAS PARLAMENTA UN PADOMES REGULAI par *ENISA* – ES Kiberdrošības aģentūru – un Regulas (ES) Nr. 526/2013 atcelšanu un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akts", COM(2017) 477 *final*/3).

14 Tas neskar sertifikācijas mehānismus saskaņā ar Vispārīgo datu aizsardzības regulu, kurā datu aizsardzības iestāžu darbībai jānorit saskaņā ar Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulu (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK ("Vispārīgā datu aizsardzības regula").

Šī iniciatīva papildinās un atbalstīs digitālās inovācijas centru centienus saskaņā ar Digitālās Eiropas programmu. Digitālās inovācijas centri ir bezpeļņas organizācijas, kas uzņēmumiem, jo īpaši jaunuzņēmumiem, MVU, un uzņēmumiem ar vidēji lielu kapitālu palīdz kļūt konkurētspējīgākiem, uzlabojot viņu uzņēmējdarbības/ražošanas procesus, kā arī to produktus un pakalpojumus, kuros, pateicoties digitālo tehnoloģiju sniegtajām iespējām, izmantotas viedas inovācijas. Digitālās inovācijas centri nodrošina uz uzņēmējdarbību vērstus inovācijas pakalpojumus, piemēram, tirgus izpēti, finanšu konsultācijas, piekļuvi attiecīgajam testēšanas un eksperimentālajam tehniskajam nodrošinājumam, apmācības un prasmju attīstīšanu, lai palīdzētu jauniem produktiem vai pakalpojumiem sekmīgi sasniegt tirgu vai ieviestu labākus ražošanas procesus. Atsevišķi digitālās inovācijas centri, kas attīstījuši lietpratību specifiskos kiberdrošības jautājumos, varētu tieši iesaistīties ar šo iniciatīvu izveidotajā kiberdrošības kompetenču kopienā. Tomēr vairumā gadījumu digitālās inovācijas centri, kuriem nav konkrētas kiberdrošības specializācijas, sekmētu savas mērķauditorijas iespējas piekļūt lietpratībai, zināšanām un spējām kiberdrošības jomā, kas pieejamas ar kiberdrošības kompetenču kopienas starpniecību, un tas notiktu ciešā sadarbībā ar Nacionālo koordinācijas centru tīklu un Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru. Digitālās inovācijas centri arī atbalstītu novatorisku kiberdrošības produktu un risinājumu plašāku ieviešanu atbilstoši uzņēmumu un citu galalietotāju, kurus tie apkalpo, vajadzībām. Visbeidzot, konkrētu nozaru digitālās inovācijas centri varētu dalīties savās zināšanās par nozaru reālajām vajadzībām ar Tīklu un Kiberdrošības centru, lai tādējādi sniegtu ieguldījumu pārdomu procesā par pētniecības un inovācijas programmu, kurā ņemtas vērā industriju prasības.

Tiks meklētas sinerģijas ar attiecīgajām Eiropas Inovāciju un tehnoloģiju institūta zināšanu un inovāciju kopienām, jo īpaši ar *EIT Digital*.

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

• Juridiskais pamats

Tā būtības un konkrēto mērķu dēļ Kompetenču centram jābūt balstītam uz divkārša juridiskā pamata. LESD 187. pants, ar kuru nosaka Savienības pētniecības un tehnoloģiju attīstības pamatprogrammu izpildei nepieciešamās struktūras, ļauj Kompetenču centram radīt sinerģijas un apvienot resursus, lai dalībvalstu līmenī ieguldītu attiecīgajās spējās, kā arī attīstītu Eiropas kopīgos aktīvus (piemēram, kopīgi iegādājoties nepieciešamo kiberdrošības testēšanas un eksperimentālo infrastruktūru). LESD 188. panta pirmā daļa paredz šādu pasākumu pieņemšanu. Neskatoties uz to, 188. panta pirmā daļa kā vienīgais juridiskais pamats neļautu šiem pasākumiem pārsniegt pētniecības un izstrādes jomas robežas, kas būtu nepieciešams, lai sasniegtu visus šajā regulā noteiktos Kompetenču centra mērķus, atbalstot kiberdrošības produktu un risinājumu plašāku ieviešanu tirgū, palīdzot Eiropas kiberdrošības industrijai kļūt konkurētspējīgākai un palielināt savu tirgus daļu, kā arī sniedzot pievienoto vērtību valstu centieniem kiberdrošības prasmju trūkuma novēršanā. Tādēļ, lai sasniegtu šos mērķus, juridiskais pamats jāpapildina ar 173. panta 3. punktu, kas Savienībai ļautu paredzēt pasākumus industrijas konkurētspējas atbalstīšanai.

• Priekšlikuma pamatojums attiecībā uz subsidiaritātes un proporcionalitātes principiem

Kiberdrošība ir jautājums, kas skar Savienības kopējās intereses, kā to apstiprina iepriekšminētie Padomes secinājumi. Tam vērā ņemams piemērs ir tādu kiberincidentu kā *WannaCry* vai *NonPetya* mērogs un to pārrobežu raksturs. Kiberdrošības tehnoloģisko problēmu raksturs un mērogs, kā arī nepietiekami koordinēti centieni industrijas, publiskā

sektora un pētniecības kopienu ietvaros un starp tām rada nepieciešamību ES turpināt koordinācijas pasākumu atbalstīšanu, lai apvienotu resursu kritisko masu un nodrošinātu labāku zināšanu, kā arī aktīvu pārvaldību. Tas ir nepieciešams, jo jāņem vērā resursu prasības, kas saistītas ar noteiktām kiberdrošības izpētes, izstrādes un plašākas ieviešanas spējām; vajadzība nodrošināt piekļuvi starpdisciplinārai zinātībai kiberdrošības jautājumos dažādās jomās (kas bieži vien valsts līmenī ir tikai daļēji pieejama); industriālo vērtību ķēžu globālais raksturs, kā arī globālo konkurentu darbība visos tirgos.

Tam ir nepieciešami resursi un lietpratība tādā apjomā, ko tikai ar grūtībām spētu nodrošināt kādas dalībvalsts atsevišķa rīcība. Piemēram, Eiropas mēroga kvantu sakaru tīkls varētu prasīt ES investīcijas aptuveni 900 miljonu EUR apmērā atkarībā no dalībvalstu investīcijām (kas būtu savstarpēji saistītas/papildinošas) un tā, cik lielā mērā šo tehnoloģiju būtu iespējams izmantot esošo infrastruktūru ietvaros. Šī iniciatīva būs svarīga finansiālo resursu apkopošanā, kā arī turpmākai šāda veida investīciju veicināšanai Savienībā.

Šīs iniciatīvas mērķi nav pilnībā sasniedzami dalībvalstīm atsevišķi. Kā norādīts iepriekš, tie ir labāk sasniedzami Savienības līmenī, apvienojot centienus un izvairoties no to nevajadzīgas dublēšanās, palīdzot sasniegt investīciju kritisko masu un nodrošinot optimālu valstu finansējuma izmantošanu. Tai pat laikā saskaņā ar proporcionalitātes principu šī regula paredz tikai to, kas vajadzīgs minētā mērķa sasniegšanai. Tāpēc ES rīcība ir pamatota ar subsidiaritātes principu un proporcionalitātes principu.

Šis instruments neparedz nekādus jaunus reglamentējošus pienākumus uzņēmumiem. Vienlaikus uzņēmumi un jo īpaši MVU, visticamāk, samazinās izmaksas, kas saistītas ar viņu centieniem izstrādāt novatoriskus kiberdrošus produktus, jo iniciatīva ļauj apvienot resursus, lai dalībvalstu līmenī ieguldītu attiecīgajās spējās, kā arī attīstītu Eiropas kopīgos aktīvus (piemēram, kopīgi iegādājoties nepieciešamo kiberdrošības testēšanas un eksperimentālo infrastruktūru). Šos aktīvus industrijas un MVU varētu izmantot dažādās nozarēs, lai nodrošinātu savu produktu kiberdrošību, kā arī padarītu kiberdrošību par vienu no savām konkurences priekšrocībām.

- **Juridiskā instrumenta izvēle**

Ar ierosināto instrumentu tiek izveidota struktūra, kuras pienākums ir īstenot kiberdrošības darbības saskaņā ar Digitālās Eiropas programmu un pamatprogrammu "Apvārsnis Eiropa". Tajā ir izklāstītas tās pilnvaras, uzdevumi, kā arī pārvaldības mehānisms. Lai izveidotu šādu Savienības struktūru, jāpieņem regula.

3. APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMI

Priekšlikums izveidot Kiberdrošības kompetenču tīklu ar Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru ir jauna iniciatīva. Tā turpina un izvērš 2016. gadā izveidoto publiskā un privātā sektora partnerību kiberdrošības jomā.

- **Apspriešanās ar ieinteresētajām personām**

Kiberdrošība ir plašs starpnozaru temats. Komisija ir izmantojusi dažādas apspriešanās metodes, lai pārliecinātos, ka šajā iniciatīvā ir pienācīgi atspoguļotas Savienības sabiedrības vispārējās intereses, nevis tikai šaura loka ieinteresēto personu grupu īpašas intereses. Šī metode nodrošina Komisijas darba pārredzamību un pārskatatbildību. Lai arī konkrēti šai iniciatīvai netika veikta atklāta sabiedriskā apspriešana, ņemot vērā tās mērķauditoriju

(industrijas un pētniecības kopienas un dalībvalstis), tās tematika jau ir tikusi aptverta vairāku citu atklātu sabiedrisko apspriežu ietvaros:

- 2018. gadā veiktā vispārējā atklātā sabiedriskā apspriešana par investīcijām, pētniecību un inovāciju, MVU un vienoto tirgu.
- 2017. gadā uzsāktā 12 nedēļu ilgā sabiedriskā apspriešana tiešsaistē, lai noskaidrotu plašākas sabiedrības (aptuveni 90 respondentu) viedokli saistībā ar *ENISA* darba izvērtēšanu un pārskatīšanu.
- 2016. gadā veiktā 12 nedēļu ilgā sabiedriskā apspriešana tiešsaistē attiecībā uz līgumiskās publiskā un privātā sektora partnerības uzsākšanu kiberdrošības jomā (aptuveni 240 respondentu).

Tāpat arī Komisija ir organizējusi mērķtiecīgas apspriešanās saistībā ar šo iniciatīvu, tostarp darbsemināru, sanāksmes un mērķtiecīgus pieprasījumus pēc ieguldījuma (no *ENISA* un Eiropas Aizsardzības aģentūras). Apspriešanās periods ilga 6 mēnešus, no 2017. gada novembra līdz 2018. gada martam. Tāpat arī Komisija apzinājusi lietpratības centrus, un tas ir ļāvis apkopot informāciju no 665 kiberdrošības jomas lietpratības centriem par viņu zinātību, darbību, darbības jomām un starptautisko sadarbību. Apsekojums tika uzsākts janvārī, un līdz 2018. gada 8. martam iesniegtie apsekojuma rezultāti tika ņemti vērā ziņojuma analīzei.

Industrijas un pētniecības kopienu ieinteresētās personas uzskata, ka Kompetenču centrs un Tīkls varētu sniegt pievienoto vērtību pašreizējiem centieniem valstu līmenī, palīdzot visā Eiropā izveidot kiberdrošības ekosistēmu, kas ļautu uzlabot sadarbību starp pētniecības un industrijas kopienām. Viņi tāpat arī uzskatīja par nepieciešamu, lai ES un dalībvalstis veidotu kiberdrošības industriālās politikas proaktīvu, ilgtermiņa un stratēģisku perspektīvu, kas pārsniedz pētniecības un inovācijas jomu. Ieinteresētās personas uzsvēra nepieciešamību piekļūt svarīgiem resursiem, piemēram, testēšanas un eksperimentālajam tehniskajam nodrošinājumam, kā arī kļūt ambiciozākiem, lai novērstu prasmju trūkumu kiberdrošības jomā, piemēram, īstenojot liela mēroga projektus, kuros varētu piesaistīt talantīgākos speciālistus. Viss iepriekš minētais arī tika uzskatīts par nepieciešamu, lai Savienība tiktu atzīta par pasaules līderi kiberdrošības jomā.

Dalībvalstis, ņemot vērā apspriešanās pasākumus, kas tika veikti kopš pagājušā gada septembra,[15] kā arī īpašos Padomes secinājumus,[16] pauda gandarījumu par nodomu izveidot Kiberdrošības kompetenču tīklu, lai stimulētu kiberdrošības tehnoloģiju izstrādi un plašāku ieviešanu, uzsverot vajadzību būt iekļaujošiem attiecībā uz visām dalībvalstīm un to esošajiem izcilības un kompetenču centriem, kā arī pievērst īpašu uzmanību papildināmībai. Konkrēti attiecībā uz nākamo Kompetenču centru dalībvalstis uzsvēra tā svarīgo lomu Tīkla atbalsta koordinēšanā. Dalībvalstu kiberaizsardzības vajadzību apzināšanas projekts, ko 2018. gada martā īstenoja Eiropas Ārējās darbības dienests, jo īpaši attiecībā uz valstu pasākumus un kiberaizsardzības vajadzībām apliecināja, ka vairums dalībvalstu par pievienoto vērtību uzskata ES atbalstu kiberaizsardzības apmācības un izglītības jomā, kā arī pētniecības un izstrādes sniegto atbalstu industrijai[17]. Šī iniciatīva tiešām ir īstenojama kopā ar dalībvalstīm vai to atbalstītajiem subjektiem. Sadarbība starp industrijas, pētniecības un/vai publiskā sektora kopienām apvienotu un stiprinātu esošos subjektus un to centienus, nevis radītu

15 Piemēram, Apaļā galda augsta līmeņa diskusija ar dalībvalstīm, priekšsēdētāja vietnieku Andrusu Ansipu, komisāri Mariju Gabrielu 2017. gada 5. decembrī.

16 Vispārējo lietu padome: Padomes 2017. gada 20. novembra secinājumi par kopīgo paziņojumu Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību".

17 EĀDD, 2018. gada marts.

jaunas. Dalībvalstis būtu arī jāiesaista tādu konkrētu darbību noteikšanā, kas vērstas uz publisko sektoru kā tiešo kiberdrošības tehnoloģiju un zinātības izmantotāju.

- **Ietekmes novērtējums**

Šo iniciatīvu papildinošais ietekmes novērtējums 2017. gada 11. aprīlī tika iesniegts Regulējuma kontroles padomei, kas par to sniedza pozitīvu atzinumu ar atrunām. Ietekmes novērtējums pēc tam tika pārskatīts, ņemot vērā šīs padomes piezīmes. Regulējuma kontroles padomes atzinums un pielikums, kur paskaidrots, kā analizētas minētās piezīmes, publicēts kopā ar šo priekšlikumu.

Ietekmes novērtējumā ir apsvērti vairāki leģislatīvi un neleģislatīvi politikas risinājumi. Par tālāk minētajiem risinājumiem tika veikts padziļināts novērtējums.

- Pamatscenārijā — sadarbības risinājumā — tiek pieņemta pašreizējās pieejas turpināšana, lai ES veidotu kiberdrošības industriālās un tehnoloģiskās spējas, atbalstot pētniecību un inovāciju, kā arī saistītos sadarbības mehānismus saskaņā ar 9. pamatprogrammu.
- 1. risinājums: Kiberdrošības kompetenču tīkls ar Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru, kam ir divkāršas pilnvaras veikt pasākumus, lai atbalstītu industriālās tehnoloģijas, kā arī pasākumus pētniecības un inovācijas jomā.
- 2. risinājums: Kiberdrošības kompetenču tīkls ar Eiropas Kiberdrošības pētniecības un kompetenču centru ir vērsts uz pētniecības un inovācijas pasākumiem.

Agrīnā posmā tika noraidīti sekojoši risinājumi: 1) risinājums neveikt nekādas darbības, 2) risinājums izveidot tikai Kiberdrošības kompetenču tīklu, 3) risinājums izveidot tikai centralizētu struktūru, kā arī 4) risinājums izmantot jau pastāvošu aģentūru (Eiropas Savienības Tīklu un informācijas drošības aģentūru (*ENISA*), Pētniecības izpildaģentūru (*REA*) vai Inovācijas un tīklu izpildaģentūru (*INEA*)).

Analīzē tika secināts, ka 1. risinājums ir vispiemērotākais, lai sasniegtu iniciatīvas mērķus, vienlaikus piedāvājot visaugstāko ekonomisko, sociālo un vides ietekmi un aizsargājot Savienības intereses. Galvenie argumenti par labu šim risinājumam bija iespēja izveidot reālu kiberdrošības industriālo politiku, atbalstot pasākumus, kas saistīti ne tikai ar pētniecību un izstrādi, bet arī plašāku ieviešanu tirgū, elastīgums, kas ļautu pielietot dažādus modeļus sadarbībai ar Kompetenču centru tīklu, lai optimizētu jau apgūto zināšanu un resursu izmantošanu, iespēja strukturēt sadarbību, kā arī no visām attiecīgajām nozarēm, tai skaitā aizsardzības nozares, nākošo publisko un privāto ieinteresēto personu kopējās saistības. Visbeidzot, 1. risinājums ļauj arī veicināt sinerģijas un var strādāt kā divu dažādu ES kiberdrošības finansējuma plūsmu īstenošanas mehānisms nākamās daudzgadu finanšu shēmas ietvaros (Digitālās Eiropas programma, "Apvārsnis Eiropa").

- **Pamattiesības**

Šī iniciatīva ļaus dalībvalstu publiskajām iestādēm un industrijām efektīvāk novērst kiberdraudus un uz tiem reaģēt, apgādājot sevi ar drošākiem produktiem un risinājumiem. Tas ir jo īpaši svarīgi, lai aizsargātu piekļuvi būtiskiem pakalpojumiem (piemēram, transporta, veselības, banku un finanšu pakalpojumiem).

Lielākas Eiropas Savienības spējas patstāvīgi garantēt savu produktu un pakalpojumu drošību var arī palīdzēt pilsoņiem izmantot viņu demokrātiskās tiesības un vērtības (piemēram, labāk aizsargājot viņu ar informāciju saistītās tiesības, kas ietvertas Pamattiesību hartā, jo īpaši tiesības uz personas datu un privātās dzīves aizsardzību) un tādējādi palielināt uzticību digitālajai sabiedrībai un ekonomikai.

4. IETEKME UZ BUDŽETU

Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs sadarbībā ar Kiberdrošības kompetenču tīklu būs galvenā īstenošanas struktūra attiecībā uz ES finanšu līdzekļiem, kas atvēlēti kiberdrošībai saskaņā ar Digitālās Eiropas programmu un pamatprogrammu "Apvārsnis Eiropa".

Ietekme uz budžetu, kas saistīta ar Digitālās Eiropas programmas ieviešanu, ir detalizēti izklāstīta šim priekšlikumam pievienotajā tiesību akta priekšlikuma finanšu pārskatā. Ieguldījuma apmēru no 21. panta 1. punkta b) apakšpunktā minētās "Apvārsnis Eiropa" pamatprogrammas otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma Komisija ierosinās likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas. Priekšlikuma pamatā būs stratēģiskās plānošanas procesa rezultāts, kā noteikts Regulas XXX [pamatprogramma "Apvārsnis Eiropa"] 6. panta 6. punktā.

5. CITI ELEMENTI

- **Īstenošanas plāni un uzraudzīšanas, izvērtēšanas un ziņošanas kārtība**

Šajā priekšlikumā ir iekļauta arī skaidri formulēta izvērtēšanas klauzula, saskaņā ar kuru Komisija veiks neatkarīgu izvērtējumu (38. pants). Pēc tam Komisija par veikto izvērtējumu ziņos Eiropas Parlamentam un Padomei, vajadzības gadījumā pievienojot priekšlikumu to pārskatīt, kas ļautu noteikt, cik liela ir instrumenta ietekme un pievienotā vērtība. Izvērtējumā tiks izmantota Komisijas labāka regulējuma metodika.

Izpilddirektoram reizi divos gados jāiesniedz Valdei Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra un Tīkla paveiktā izvērtējums, kā noteikts šā priekšlikuma 17. pantā. Izpilddirektoram arī jāsagatavo turpmākas rīcības plāns atbilstīgi retrospektīvu izvērtējumu secinājumiem un reizi divos gados par īstenošanas gaitu jāziņo Komisijai. Kā noteikts šā priekšlikuma 16. pantā, Valdei jābūt atbildīgai par tādas turpmākas rīcības pienācīgu uzraudzību, kas balstīta uz šādiem secinājumiem.

Ja ir aizdomas par administratīvām kļūdām tiesību subjekta darbībā, Eiropas Ombuds var veikt izmeklēšanu saskaņā ar Līguma 228. panta noteikumiem.

2018/0328 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA,

ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru un Nacionālo koordinācijas centru tīklu

Eiropas Komisijas ieguldījums vadītāju sanāksmē
Zalcburgā, 2018. gada 19.–20. septembrī

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 173. panta 3. punktu un 188. panta pirmo daļu,

ņemot vērā Eiropas Komisijas priekšlikumu,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[18],

ņemot vērā Reģionu komitejas atzinumu[19],

saskaņā ar parasto likumdošanas procedūru,

tā kā:

1) Mūsu ikdienas dzīvi un ekonomiku arvien vairāk nosaka digitālās tehnoloģijas, un iedzīvotāji arvien vairāk ir pakļauti nopietniem kiberincidentiem. Gan civilā infrastruktūra, gan militārās spējas ir atkarīgas no drošām digitālajām sistēmām, tāpēc nākotnē drošības līmeni cita starpā noteiks tehnoloģiju un industrijas nodrošinātā spēja uzlabot Savienības aizsargātību pret kiberdraudiem.

2) Savienība ir pastāvīgi izvērsusi savu darbību, lai risinātu pieaugošās kiberdrošības problēmas saskaņā ar 2013. gada kiberdrošības stratēģiju,[20] kuras mērķis ir veicināt uzticamu, drošu un atvērtu kiberdrošības ekosistēmu. 2016. gadā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/1148[21] par tīklu un informācijas sistēmu drošību Savienība pieņēma pirmos pasākumus kiberdrošības jomā.

3) 2017. gada septembrī Komisija un Savienības Augstā pārstāve ārlietās un drošības politikas jautājumos iesniedza kopīgu paziņojumu[22] "Noturība, novēršana un

18 OV C […], […], […]. lpp.

19 OV C [...], [...], [...]. lpp.

20 Kopīgs paziņojums Eiropas Parlamentam un Padomei: Eiropas Savienības kiberdrošības stratēģija — atvērta un droša kibertelpa", JOIN(2013) 1 *final*.

21 Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

22 Kopīgs paziņojums Eiropas Parlamentam un Padomei "Noturība, novēršana un aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", JOIN(2017) 450 *final*.

aizsardzība, veidojot Eiropas Savienībai stipru kiberdrošību", lai vēl vairāk stiprinātu Savienības noturības, novēršanas un reaģēšanas spējas, kas ļautu stāties pretī kiberuzbrukumiem.

4) Valstu un valdību vadītāji Tallinas digitālajā samitā 2017. gada septembrī aicināja Savienību "līdz 2025. gadam kļūt par pasaules līderi kiberdrošības jomā, lai nodrošinātu mūsu pilsoņu, patērētāju un uzņēmumu uzticēšanos, pārliecību un aizsardzību tiešsaistē, kā arī nodrošinātu likumā reglamentētu bezmaksas internetu".

5) Būtiski tīklu un informācijas sistēmu traucējumi var ietekmēt atsevišķas dalībvalstis un Savienību kopumā. Tādējādi iekšējā tirgus vienmērīgai darbībai tīklu un informācijas sistēmu drošība ir ārkārtīgi svarīga. Patlaban Savienība ir atkarīga no kiberdrošības pakalpojumu sniedzējiem ārpus Eiropas. Tomēr savu stratēģisko interešu nolūkā Savienībai jānodrošina būtisku kiberdrošības tehnoloģisko spēju saglabāšana un attīstīšana, lai aizsargātu savu digitālo vienoto tirgu un jo īpaši lai aizsargātu kritiskos tīklus un informācijas sistēmas, kā arī sniegtu svarīgākos kiberdrošības pakalpojumus.

6) Savienībā ir uzkrāta ievērojama lietpratība un pieredze kiberdrošības jomā saistībā ar pētniecību, tehnoloģijām un industriālo attīstību, taču industrijas un pētniecības kopienu centieni ir sadrumstaloti, turklāt tām trūkst saskaņotības un kopīga pamatuzdevuma, un tādējādi šajā nozarē tiek kavēta konkurētspēja. Šie centieni un lietpratība jāapkopo, jāapvieno tīklā un efektīvi jāizmanto, lai pastiprinātu un papildinātu jau esošus pētījumus, tehnoloģiskās un industriālās spējas Savienības un valstu līmenī.

7) 2017. gada novembrī pieņemtie Padomes secinājumi aicināja Komisiju ātri nodrošināt ietekmes novērtējumu par iespējamajiem risinājumiem, kā izveidot kiberdrošības kompetenču tīklu ar Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru, un līdz 2018. gada vidum nākt klajā ar priekšlikumu par attiecīgo juridisko instrumentu.

8) Kompetenču centram vajadzētu būt Savienības galvenajam instrumentam, kas izmantojams, lai apvienotu investīcijas kiberdrošības pētniecībā, tehnoloģijās un industriālajā attīstībā un īstenotu attiecīgos projektus un iniciatīvas kopā ar Kiberdrošības kompetenču tīklu. Tam būtu jāsniedz ar kiberdrošību saistīts finansiāls atbalsts no Digitālās Eiropas programmas un pamatprogrammas "Apvārsnis Eiropa", turklāt vajadzētu būt pieejamam Eiropas Reģionālās attīstības fondam un vajadzības gadījumā citām programmām. Šādai pieejai būtu jāpalīdz veidot sinerģijas un koordinēt finansiālo atbalstu, kas saistīts ar kiberdrošības pētniecību, inovācijām, tehnoloģijām un industriālo attīstību, tādējādi ļaujot izvairīties no nevajadzīgas centienu dublēšanās.

9) Ņemot vērā, ka šīs iniciatīvas mērķi vislabāk ir sasniedzami, tajā piedaloties visām dalībvalstīm vai pēc iespējas lielākai dalībvalstu daļai, un tā kā dalībvalstu dalības stimulēšanas nolūkā balsstiesības būtu jāparedz tikai tām dalībvalstīm, kuras sniedz finansiālu ieguldījumu Kompetenču centra administratīvo un darbības izmaksu segšanai.

10) Iesaistīto dalībvalstu finansiālajai līdzdalībai šajā iniciatīvā vajadzētu būt samērīgai ar Savienības finansiālo ieguldījumu.

11) Kompetenču centram būtu jāsekmē Kiberdrošības kompetenču tīkla (turpmāk "Tīkls"), ko katrā dalībvalstī veido nacionālie koordinācijas centri, darbība un jāpalīdz tā koordinēt. Nacionālajiem koordinācijas centriem būtu jāsaņem tiešs

Savienības finansiālais atbalsts ar šo regulu saistītu pasākumu veikšanai, tostarp dotācijas, kas piešķirtas bez uzaicinājuma iesniegt priekšlikumus.

12) Nacionālie koordinācijas centri būtu jāizvēlas dalībvalstīm. Papildus nepieciešamajām administratīvajām spējām šajos centros vajadzētu būt attīstītai vai arī tieši pieejamai tehnoloģiskai lietpratībai kiberdrošības jomā, jo īpaši tādās sfērās kā kriptogrāfija, IKT drošības pakalpojumi, ielaušanās atklāšana, sistēmu drošība, tīklu drošība, programmatūras un lietojumprogrammu drošība, vai drošības un privātuma cilvēciskie un sabiedriskie aspekti. Centriem būtu jāspēj arī efektīvi iesaistīties un nodrošināt koordināciju ar industriju, publisko sektoru, tostarp saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/1148[23] izraudzītām iestādēm, un pētniecības kopienu.

13) Ja nacionālajiem koordinācijas centriem tiek sniegts finansiāls atbalsts, lai atbalstītu trešās personas valstu līmenī, tas, noslēdzot otrā līmeņa dotāciju nolīgumus, tālāk piešķirams attiecīgajām ieinteresētajām personām.

14) Jaunās tehnoloģijas, piemēram, mākslīgais intelekts, lietu internets, augstas veiktspējas datošana (*HPC*) un kvantu skaitļošana, blokķēde un tāds jēdziens kā droša digitālā identitāte vienlaikus rada jaunas kiberdrošības problēmas un piedāvā to risinājumus. Lai novērtētu un apliecinātu pašreizējo vai nākotnes IKT sistēmu noturību, būs jāveic drošības risinājumu testēšana attiecībā uz *HPC* un kvantu mehānismu uzbrukumiem. Kompetenču centram, Tīklam un kiberdrošības kompetenču kopienai būtu jāpalīdz attīstīt un izplatīt jaunākos kiberdrošības risinājumus. Tajā pat laikā vajadzētu būt iespējai, ka Kompetenču centru un Tīklu var izmantot izstrādātāji un operatori, kuri darbojas kritiskajās nozarēs, piemēram, transporta, enerģētikas, veselības, finanšu, vispārējās valdības, telesakaru, ražošanas, aizsardzības un kosmosa sektorā, jo tas viņiem palīdzētu risināt kiberdrošības problēmas.

15) Kompetenču centram būtu jāpilda vairākas galvenās funkcijas. Pirmkārt, Kompetenču centram būtu jāsekmē Eiropas Kiberdrošības kompetenču tīkla darbība un jāpalīdz tās koordinēšanā, kā arī jāsniedz atbalsts kiberdrošības kompetenču kopienai. Kompetenču centram būtu jāuzņemas kiberdrošības tehnoloģiskās programmas vadība un jāsekmē Tīklā un kiberdrošības kompetenču kopienā apkopotās lietpratības pieejamība. Otrkārt, tam būtu jāīsteno Digitālās Eiropas programmas un pamatprogrammas "Apvārsnis Eiropa" attiecīgās daļas, piešķirot dotācijas, parasti pēc uzaicinājumiem iesniegt priekšlikumus konkursa kārtībā. Treškārt, Kompetenču centram būtu jāveicina Savienības, dalībvalstu un/vai industrijas kopīgas investīcijas.

16) Kompetenču centram būtu jāveicina un jāatbalsta kiberdrošības kompetenču kopienas sadarbība un pasākumu koordinācija, kas aptvertu kiberdrošības tehnoloģiju izstrādē iesaistīto apjomīgu, atvērtu un daudzveidīgu dalībnieku kopumu. Šajā kopienā jo īpaši būtu jāietver pētniecības subjekti, piedāvājuma un pieprasījuma puses industrijas, kā arī publiskā sektora pārstāvji. Kiberdrošības kompetenču kopienai būtu jāsniedz ieguldījums Kompetenču centra pasākumos un darba plānā, kā arī tai būtu jāgūst labums no Kompetenču centra un Tīkla kopienas veidošanas pasākumiem, taču tai nevajadzētu būt kā citādi privileģētai attiecībā uz uzaicinājumiem iesniegt priekšlikumus vai uzaicinājumiem iesniegt piedāvājumus.

[23] Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

17) Lai apmierinātu gan pieprasījuma, gan piedāvājuma puses industriju vajadzības, Kompetenču centra uzdevumam sniegt industrijām zināšanas un tehnisko palīdzību kiberdrošības jomā būtu jāattiecas gan uz IKT produktiem un pakalpojumiem, gan uz visiem citiem industriālajiem un tehnoloģiskajiem produktiem un risinājumiem, kuros jābūt integrētam kiberdrošības aspektam.

18) Tā kā Kompetenču centram un Tīklam būtu jācenšas panākt sinerģijas starp kiberdrošības civilo un aizsardzības jomu, pamatprogrammas "Apvārsnis Eiropa" finansētie projekti tiks īstenoti saskaņā ar Regulu XXX [turpmāk "Apvārsnis Eiropa" regula], kurā noteikts, ka pētniecības un inovācijas pasākumi "Apvārsnis Eiropa" ietvaros ir vērsti uz civilajām vajadzībām.

19) Lai nodrošinātu strukturētu un ilgtspējīgu sadarbību, Kompetenču centra un nacionālo koordinācijas centru attiecības būtu jānosaka saskaņā ar līgumisku vienošanos.

20) Būtu jāizstrādā attiecīgi noteikumi, kas garantētu Kompetenču centra atbildību un pārredzamību.

21) Komisijas Kopīgajam pētniecības centram un Eiropas Savienības Tīklu un informācijas drošības aģentūrai (*ENISA*), ņemot vērā viņu attiecīgo lietpratību kiberdrošības jomā, būtu aktīvi jāiesaistās kiberdrošības kompetenču kopienas, kā arī Industriālās un zinātniskās konsultatīvās padomes darbībā.

22) Gadījumos, kad nacionālie koordinācijas centri un kiberdrošības kompetenču kopienas subjekti saņem finansiālu ieguldījumu no Savienības vispārējā budžeta, tiem būtu jāpublisko fakts, ka attiecīgie pasākumi tiek veikti šīs iniciatīvas kontekstā.

23) No Savienības finansiālā ieguldījuma Kompetenču centrā būtu jāsedz puse no izmaksām, ko radījusi Kompetenču centra izveide, administrēšanas un koordinēšanas pasākumi. Lai izvairītos no finansējuma dublēšanās, minētajiem pasākumiem nevajadzētu vienlaikus saņemt ieguldījumu no citām Savienības programmām.

24) Kompetenču centra Valdei, kas sastāv no dalībvalstīm un Komisijas, būtu jānosaka Kompetenču centra darbības vispārējais virziens un jānodrošina, ka Kompetenču centrs pilda savus uzdevumus saskaņā ar šo regulu. Valde būtu jāpilnvaro izstrādāt budžetu, pārbaudīt tā izpildi, pieņemt atbilstošus finansiālos noteikumus, noteikt pārredzamas darba procedūras Kompetenču centra lēmumu pieņemšanai, pieņemt Kompetenču centra darba plānu un daudzgadu stratēģisko plānu, kurā izklāstītas prioritātes Kompetenču centra mērķu un uzdevumu sasniegšanā, pieņemt savu reglamentu, iecelt izpilddirektoru un lemt par izpilddirektora pilnvaru termiņa pagarināšanu un izbeigšanu.

25) Lai Kompetenču centrs darbotos pienācīgi un rezultatīvi, Komisijai un dalībvalstīm būtu jānodrošina, ka Valdē ieceļamajām personām ir atbilstoša profesionālā lietpratība un pieredze funkcionālajās jomās. Lai nodrošinātu Valdes darba nepārtrauktību, Komisijai un dalībvalstīm būtu arī jācenšas ierobežot savu attiecīgo pārstāvju mainību Valdē.

26) Lai Kompetenču centra darbība būtu sekmīga, tās izpilddirektors jāieceļ, ņemot vērā nopelnus un ar dokumentiem apliecinātas administratīvās un vadības prasmes, kā arī kompetenci un pieredzi kiberdrošības jomā, turklāt izpilddirektora pienākumi jāpilda pilnīgi neatkarīgi.

27) Lai uzturētu regulāru dialogu ar privāto sektoru, patērētāju organizācijām un citām ieinteresētajām personām, Kompetenču centrā vajadzētu būt izveidotai padomdevēja struktūrai — Industriālajai un zinātniskajai konsultatīvajai padomei. Industriālajai un

zinātniskajai konsultatīvajai padomei būtu jākoncentrējas uz jautājumiem, kas ir svarīgi ieinteresētajām personām, un par tiem jāinformē Kompetenču centra Valde. Industriālās un zinātniskās konsultatīvās padomes sastāvam un tai uzticētajiem uzdevumiem, piemēram, konsultācijām saistībā ar darba plānu, būtu jānodrošina pietiekama ieinteresēto personu pārstāvība Kompetenču centra darbā.

28) Kompetenču centram ar Industriālās un zinātniskās konsultatīvās padomes starpniecību būtu jāgūst labums no īpašās lietpratības, kā arī plašās un nozīmīgās ieinteresēto personu pārstāvības, kuras pamatā ir līgumiskā publiskā un privātā sektora partnerība kiberdrošības jomā programmas "Apvārsnis 2020" ietvaros.

29) Kompetenču centrā vajadzētu būt ieviestiem noteikumiem par interešu konfliktu novēršanu un risināšanu. Kompetenču centram būtu arī jāievēro atbilstīgi Savienības noteikumi par publisku piekļuvi dokumentiem, kā noteikts Eiropas Parlamenta un Padomes Regulā (EK) Nr. 1049/2001[24]. Uz Kompetenču centra veikto personas datu apstrādi attieksies Eiropas Parlamenta un Padomes Regula (ES) Nr. XXX/2018. Kompetenču centram būtu jāievēro Savienības iestādēm piemērojamie noteikumi un valstu tiesību akti, kas attiecas uz rīkošanos ar datiem, jo īpaši sensitīvu, bet neklasificētu informāciju un ES klasificētu informāciju.

30) Visā izdevumu ciklā Savienības un dalībvalstu finansiālās intereses būtu jāaizsargā ar samērīgiem pasākumiem, tostarp pārkāpumu novēršanu, atklāšanu un izmeklēšanu, zaudēto, nepamatoti izmaksāto vai nepareizi izlietoto līdzekļu atgūšanu un attiecīgos gadījumos administratīvo un finansiālo sodu piemērošanu saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES, *Euratom*) Nr. XXX[25] [turpmāk "Finanšu regula"].

31) Kompetenču centram būtu jādarbojas atklāti un pārredzami, savlaicīgi sniedzot visu atbilstīgo informāciju, kā arī popularizējot savus pasākumus, tostarp informēšanas un izplatīšanas pasākumus, plašākai sabiedrībai. Kompetenču centra struktūru reglaments būtu jādara publiski pieejams.

32) Komisijas iekšējam revidentam Kompetenču centrā vajadzētu būt tādām pašām pilnvarām, kādas tam ir Komisijā.

33) Komisijai, Kompetenču centram, Revīzijas palātai un Eiropas Birojam krāpšanas apkarošanai būtu jāsaņem piekļuve visai nepieciešamajai informācijai un telpām, lai varētu veikt Kompetenču centra dotāciju, līgumu un parakstīto nolīgumu revīzijas un izmeklēšanas.

34) Ņemot vērā, ka šīs regulas mērķus – saglabāt un attīstīt Savienības kiberdrošības tehnoloģiskās un industriālās spējas, palielināt Savienības kiberdrošības industrijas konkurētspēju un padarīt kiberdrošību par citu Savienības industriju konkurētspējīgu priekšrocību – nevar pietiekami labi sasniegt atsevišķās dalībvalstīs ierobežoto resursu izkliedētības, kā arī nepieciešamā investīciju apjoma dēļ, taču, izvairoties no nevajadzīgas šo centienu dublēšanās, var labāk sasniegt Savienības līmenī, palīdzot sasniegt investīciju apjoma kritisko masu un nodrošinot publiskā finansējuma optimālu izmantošanu, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā

---

[24] Eiropas Parlamenta un Padomes 2001. gada 30. maija Regula (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (OV L 145, 31.5.2001., 43. lpp.).

[25] [pievienot virsrakstu un OV atsauci].

noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai,

IR PIEŅĒMUŠI ŠO REGULU.

I NODAĻA

KOMPETENČU CENTRA UN TĪKLA VISPĀRĪGIE NOTEIKUMI UN PRINCIPI

1. pants

Priekšmets

1. Ar šo regulu izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru (turpmāk "Kompetenču centrs") un Nacionālo koordinācijas centru tīklu, kā arī paredz noteikumus nacionālo koordinācijas centru izvirzīšanai un kiberdrošības kompetenču kopienas izveidei.

2. Kompetenču centrs palīdz īstenot kiberdrošības darbības, kas paredzētas ar Regulu Nr. XXX izveidotajā Digitālās Eiropas programmā un jo īpaši minētās regulas 6. pantā, kā arī ar Regulu Nr. XXX izveidotajā pamatprogrammā "Apvārsnis Eiropa" un jo īpaši I pielikuma 2. pīlāra 2.2.6. iedaļā Lēmumā Nr. XXX, ar ko izveido īpašo programmu, ar kuru īsteno pētniecības un inovācijas pamatprogrammu "Apvārsnis Eiropa" [īpašās programmas atsauces numurs].

3. Kompetenču centrs atrodas [Briselē, Beļģijā].

4. Kompetenču centrs ir juridiska persona. Katrā dalībvalstī tam ir visplašākā tiesībspēja un rīcībspēja, kas šīs dalībvalsts tiesību aktos paredzēta juridiskajām personām. Tas var iegādāties vai atsavināt kustamu un nekustamu mantu un būt par pusi tiesas procesā.

2. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

(1) "kiberdrošība" ir tīklu un informācijas sistēmu, to lietotāju un citu personu aizsardzība pret kiberdraudiem;

(2) "kiberdrošības produkti un risinājumi" ir IKT produkti, pakalpojumi vai procesi ar īpašu mērķi tīklus un informācijas sistēmas, to lietotājus un iesaistītās personas aizsargāt pret kiberdraudiem;

(3) "publiskā iestāde" ir jebkura valdība vai cita publiskās pārvaldes iestāde, tostarp publiska padomdevēja struktūra, valsts, reģionu vai vietējā līmenī vai jebkura fiziska vai juridiska persona, kas saskaņā ar attiecīgās valsts tiesību aktiem pilda publiskās pārvaldes funkcijas, tostarp veicot konkrētus pienākumus;

(4) "iesaistītā dalībvalsts" ir dalībvalsts, kas brīvprātīgi sniedz finansiālu ieguldījumu Kompetenču centra administratīvo un darbības izmaksu segšanai.

3. pants

Kompetenču centra un Tīkla pamatuzdevums

1. Kompetenču centrs un Tīkls palīdz Savienībai:

   (a) saglabāt un attīstīt kiberdrošības tehnoloģiskās un industriālās spējas, kas nepieciešamas digitālā vienotā tirgus drošībai;

   (b) palielināt Savienības kiberdrošības industrijas konkurētspēju un padarīt kiberdrošību par citu Savienības industriju konkurētspējīgu priekšrocību.

2. Kompetenču centrs vajadzības gadījumā veic savus uzdevumus sadarbībā ar Nacionālo koordinācijas centru tīklu un kiberdrošības kompetenču kopienu.

4. pants

Kompetenču centra mērķi un uzdevumi

Kompetenču centram ir šādi mērķi un saistītie uzdevumi:

1. sekmēt 6. pantā minētā Nacionālo koordinācijas centru tīkla (turpmāk "Tīkls") un 8. pantā minētās kiberdrošības kompetenču kopienas darbu un palīdzēt to koordinēt;

2. palīdzēt īstenot kiberdrošības darbības, kas paredzētas ar Regulu Nr. XXX[26] izveidotajā Digitālās Eiropas programmā un jo īpaši minētās regulas 6. pantā, ar Regulu Nr. XXX [27]izveidotajā pamatprogrammā "Apvārsnis Eiropa" un jo īpaši I pielikuma 2. pīlāra 2.2.6. iedaļā Lēmumā Nr. XXX, ar ko izveido īpašo programmu, ar kuru īsteno pētniecības un inovācijas pamatprogrammu "Apvārsnis Eiropa" [īpašās programmas atsauces numurs], kā arī citās Savienības programmās, ja tas paredzēts Savienības tiesību aktos;

3. uzlabot industriju, publiskā sektora un pētniecības kopienu rīcībā esošās kiberdrošības spējas, zināšanas un infrastruktūru, veicot šādus uzdevumus:

   (a) attiecībā uz industrijas un pētniecības modernajām infrastruktūrām kiberdrošības jomā un saistītajiem pakalpojumiem – iegūt, uzlabot, ekspluatēt šādas infrastruktūras un pakalpojumus un padarīt pieejamus plašam industrijas lietotāju lokam visā Savienībā, tostarp MVU, publiskajam sektoram, kā arī pētniecības un zinātnes kopienām;

   (b) attiecībā uz industrijas un pētniecības modernajām infrastruktūrām kiberdrošības jomā un saistītajiem pakalpojumiem – sniegt atbalstu, tostarp finansiālu, citiem subjektiem, lai tās varētu iegūt, uzlabot, ekspluatēt šādas infrastruktūras un pakalpojumus un padarīt pieejamus plašam industrijas lietotāju lokam visā Savienībā, tostarp MVU, publiskajam sektoram, kā arī pētniecības un zinātnes kopienām;

   (c) kiberdrošības jautājumos sniegt zināšanas un tehnisko palīdzību industrijai un publiskajām iestādēm, jo īpaši atbalstot darbības, kuru mērķis ir atvieglot piekļuvi Tīklā un kiberdrošības kompetenču kopienā pieejamajai lietpratībai;

---

[26] [pievienot pilnu virsrakstu un OV atsauci].

[27] [pievienot pilnu virsrakstu un OV atsauci].

4. sekmēt modernāko kiberdrošības produktu un risinājumu plašu ieviešanu visā ekonomikā, veicot šādus uzdevumus:

   (a) stimulēt pētniecību un izstrādi kiberdrošības jomā un Savienības kiberdrošības produktu un risinājumu izmantošanu publiskajās iestādēs un lietotāju industrijās;

   (b) palīdzēt publiskajām iestādēm, pieprasījuma puses industrijām un citiem lietotājiem pieņemt un integrēt jaunākos kiberdrošības risinājumus;

   (c) jo īpaši palīdzēt publiskajām iestādēm organizēt publisko iepirkumu vai publisko iestāžu uzdevumā rīkot modernāko kiberdrošības produktu un risinājumu iepirkumus;

   (d) sniegt finansiālu atbalstu un tehnisku palīdzību kiberdrošības jomas jaunuzņēmumiem un MVU, lai veidotu saikni ar potenciālajiem tirgiem un piesaistītu investīcijas;

5. uzlabot izpratni par kiberdrošību un palīdzēt mazināt prasmju trūkumu Savienībā saistībā ar kiberdrošību, veicot šādus uzdevumus:

   (a) atbalstīt kiberdrošības prasmju turpmāku attīstīšanu, vajadzības gadījumā sadarbībā ar attiecīgajām ES aģentūrām un struktūrām, tostarp *ENISA*;

6. veicināt kiberdrošības pētniecību un izstrādi Savienībā šādi:

   (a) sniegt finansiālu atbalstu centieniem kiberdrošības pētniecības jomā, pamatojoties uz kopīgu, pastāvīgi izvērtētu un uzlabotu daudzgadu stratēģisko, industriālo, tehnoloģisko un pētniecisko programmu;

   (b) sadarbībā ar industriju un Tīklu atbalstīt plaša mēroga pētījumu un demonstrējumu projektus nākamās paaudzes kiberdrošības tehnoloģisko spēju jomā;

   (c) atbalstīt pētniecību un inovāciju kiberdrošības tehnoloģiju standartizācijā;

7. uzlabot sadarbību starp civilo un aizsardzības jomu attiecībā uz divējāda lietojuma tehnoloģijām un to pielietošanu kiberdrošības jomā, veicot šādus uzdevumus:

   (a) sniegt atbalstu dalībvalstīm, kā arī industrijas un pētniecības ieinteresētajām personām saistībā ar pētniecību, izstrādi un plašāku ieviešanu;

   (b) veicināt sadarbību starp dalībvalstīm, sniedzot atbalstu izglītības, apmācības un mācību jomā;

   (c) apvienot ieinteresētās personas, lai veicinātu sinerģijas starp kiberdrošības pētniecību un tirgiem civilajā un aizsardzības jomā;

8. veicināt sinerģijas starp kiberdrošības civilajām un aizsardzības jomām saistībā ar Eiropas Aizsardzības fondu, veicot šādus uzdevumus:

   (a) sniegt padomus, dalīties lietpratībā un veicināt sadarbību starp attiecīgajām ieinteresētajām personām;

   (b) pārvaldīt daudznacionālus kiberaizsardzības projektus pēc dalībvalstu pieprasījuma un tādējādi uzņemties projektu vadītāja lomu Regulas XXX [Regula, ar ko izveido Eiropas Aizsardzības fondu] izpratnē.

5. pants

Investēšana infrastruktūrās, spējās, produktos vai risinājumos un to izmantošana

1. Ja Kompetenču centrs nodrošina finansējumu infrastruktūrām, spējām, produktiem vai risinājumiem saskaņā ar 4. panta 3. un 4. punktu dotāciju vai godalgu veidā, Kompetenču centra darba plānā var konkrēti precizēt:

   (a) noteikumus, kas reglamentē darbību saistībā ar infrastruktūru vai spēju, tostarp attiecīgā gadījumā šādas darbības īstenošanu uzticot mitinātājam, pamatojoties uz Kompetenču centra noteiktajiem kritērijiem;

   (b) noteikumus, kas reglamentē piekļuvi infrastruktūrai vai spējai un to izmantošanu.

2. Tīkla locekļu, kiberdrošības kompetenču kopienas locekļu vai citu trešo personu, kas pārstāv kiberdrošības produktu un risinājumu lietotājus, uzdevumā Kompetenču centrs var būt atbildīgs par attiecīgu kopējā iepirkuma darbību vispārējo izpildi, ieskaitot pirmskomercializācijas iepirkumus. Šajā nolūkā Kompetenču centram var palīdzēt viens vai vairāki nacionālie koordinācijas centri vai kiberdrošības kompetenču kopienas locekļi.

6. pants

Nacionālo koordinācijas centru izvirzīšana

1. Līdz [datums] katra dalībvalsts izvirza subjektu, kas šīs regulas izpratnē darbosies kā nacionālais koordinācijas centrs, un par to paziņo Komisijai.

2. Pamatojoties uz novērtējumu par šī subjekta atbilstību 4. punktā noteiktajiem kritērijiem, 6 mēnešu laikā pēc tam, kad dalībvalsts pārsūtījusi informāciju par izvirzīšanu, Komisija pieņem lēmumu par subjekta akreditēšanu par nacionālo koordinācijas centru vai šādu izvirzīšanu noraida. Komisija publicē nacionālo koordinācijas centru sarakstu.

3. Dalībvalstis jebkurā laikā var izvirzīt jaunu subjektu par nacionālo koordinācijas centru šīs regulas izpratnē. Uz jebkura jauna subjekta izvirzīšanu attiecas 1. un 2. punkts.

4. Izvirzītie nacionālie koordinācijas centri, pildot savu pamatuzdevumu saskaņā ar šīs regulas 3. pantu, ir spējīgi atbalstīt Kompetenču centru un Tīklu. Tiem ir attīstīta vai arī tieši pieejama tehnoloģiskā lietpratība kiberdrošības jomā, turklāt tie spēj efektīvi iesaistīties un nodrošināt koordināciju ar industriju, publisko sektoru un pētniecības kopienu.

5. Kompetenču centra un nacionālo koordinācijas centru attiecības nosaka saskaņā ar līgumisku vienošanos, ko slēdz starp Kompetenču centru un katru nacionālo koordinācijas centru. Vienošanās paredz noteikumus, kas reglamentē savstarpējās attiecības, kā arī uzdevumu sadalījumu starp Kompetenču centru un katru nacionālo koordinācijas centru.

6. Nacionālo koordinācijas centru tīkls aptver visu dalībvalstu izvirzīto nacionālo koordinācijas centru kopums.

7. pants

Nacionālo koordinācijas centru uzdevumi

1. Nacionālajiem koordinācijas centriem ir šādi uzdevumi:

(a) atbalstīt Kompetenču centru tā mērķu sasniegšanā un jo īpaši kiberdrošības kompetenču kopienas koordinēšanā;

(b) veicināt industrijas un citu dalībnieku līdzdalību dalībvalstu līmenī pārrobežu projektu ietvaros;

(c) sadarbībā ar Kompetenču centru veicināt konkrētās nozarēs pastāvošo industriālo problēmu identificēšanu un risināšanu kiberdrošības jomā;

(d) valsts līmenī darboties kā kiberdrošības kompetenču kopienas un Kompetenču centra kontaktpunktam;

(e) veicināt sinerģiju veidošanu ar attiecīgajiem pasākumiem valsts un reģionu līmenī;

(f) īstenot konkrētas darbības, kurām Kompetenču centrs ir piešķīris dotācijas, tostarp sniedzot finansiālu atbalstu trešajām personām saskaņā ar Regulas Nr. XXX [jaunā Finanšu regula] 204. pantu atbilstoši nosacījumiem, kas ietverti attiecīgajos dotāciju nolīgumos;

(g) valsts vai reģionu līmenī popularizēt un izplatīt Tīkla, kiberdrošības kompetenču kopienas un Kompetenču centra attiecīgos paveiktā darba rezultātus;

(h) novērtēt to subjektu pieteikumus kļūt par kiberdrošības kompetenču kopienas daļu, kas iedibināti tajā pašā dalībvalstī, kur koordinācijas centrs.

2. Finansiālu atbalstu trešajām personām f) apakšpunkta izpratnē var piešķirt jebkurā no Regulas XXX [jaunā Finanšu regula] 125. pantā norādītajiem veidiem, tai skaitā fiksētas summas veidā.

3. Saistībā ar šajā pantā noteikto uzdevumu izpildi nacionālie koordinācijas centri var saņemt Savienības dotācijas saskaņā ar Regulas XXX [jaunā Finanšu regula] 195. panta d) apakšpunktu.

4. Vajadzības gadījumā nacionālie koordinācijas centri sadarbojas ar Tīkla starpniecību, lai veiktu 1. punkta a), b), c), e) un g) apakšpunktos minētos uzdevumus.

8. pants

Kiberdrošības kompetenču kopiena

1. Kiberdrošības kompetenču kopiena sekmē 3. pantā minētā Kompetenču centra pamatuzdevuma izpildi, kā arī uzlabo un izplata lietpratību kiberdrošības jomā visā Savienībā.

2. Kiberdrošības kompetenču kopienu veido industrija, akadēmiskās un bezpeļņas pētniecības organizācijas un asociācijas, kā arī publiskie subjekti un citi subjekti, kas nodarbojas ar tehniskiem un ar darbību saistītiem jautājumiem. Tā apvieno galvenās ieinteresētās personas attiecībā uz kiberdrošības tehnoloģiskajām un industriālajām spējām Savienībā. Kopienai savā darbībā jāiesaista nacionālie koordinācijas centri, kā arī Savienības iestādes un struktūras ar atbilstošu lietpratību.

3. Tikai Savienībā iedibināti subjekti var tikt akreditēti kā kiberdrošības kompetenču kopienas locekļi. Tām jāapliecina sava lietpratība kiberdrošības jautājumos vismaz vienā no šīm jomām:

(a) pētniecība;

(b) industriālā attīstība;

(c) apmācība un izglītība.

4. Kompetenču centrs akreditē subjektus, kas saskaņā ar valsts tiesību aktiem ir iedibināti kā kiberdrošības kompetenču kopienas locekļi, balstoties uz 3. punktā noteikto atbilstības kritēriju novērtējumu, ko veic tās dalībvalsts nacionālais koordinācijas centrs, kurā attiecīgais subjekts ir iedibināts. Akreditācija ir beztermiņa, taču Kompetenču centrs to jebkurā laikā var atsaukt, ja tas vai attiecīgais nacionālais koordinācijas centrs uzskata, ka subjekts neatbilst 3. punktā noteiktajiem kritērijiem, vai gadījumos, kad šāda rīcība atbilst attiecīgajiem noteikumiem, kas izklāstīti Regulas XXX [jaunā Finanšu regula] 136. pantā.

5. Kompetenču centrs akreditē attiecīgās Savienības struktūras, aģentūras un birojus kā kiberdrošības kompetenču kopienas locekļus pēc tam, kad ir veikts novērtējums par šo subjektu atbilstību 3. punktā noteiktajiem kritērijiem. Akreditācija ir beztermiņa, taču Kompetenču centrs to jebkurā laikā var atsaukt, ja tas uzskata, ka subjekts neatbilst 3. punktā noteiktajiem kritērijiem, vai gadījumos, kad šāda rīcība atbilst attiecīgajiem noteikumiem, kas izklāstīti Regulas XXX [jaunā Finanšu regula] 136. pantā.

6. Komisijas pārstāvji var piedalīties kopienas darbā.

9. pants

Kiberdrošības kompetenču kopienas locekļu uzdevumi

Kiberdrošības kompetenču kopienas locekļiem ir šādi uzdevumi:

(1) sniegt atbalstu 3. un 4. pantā noteiktās Kompetenču centra pamatuzdevuma un mērķu izpildei, kā arī šajā nolūkā cieši sadarboties ar Kompetenču centru un attiecīgajiem nacionālajiem koordinācijas centriem;

(2) piedalīties Kompetenču centra un nacionālo koordinācijas centru veicinātajos pasākumos;

(3) attiecīgā gadījumā piedalīties Kompetenču centra Valdes izveidotajās darba grupās, lai veiktu konkrētus pasākumus, kuri paredzēti Kompetenču centra darba plānā;

(4) attiecīgā gadījumā atbalstīt Kompetenču centru un nacionālos koordinācijas centrus konkrētu projektu veicināšanā;

(5) veicināt un izplatīt kopienas ietvaros veikto pasākumu un projektu attiecīgos rezultātus.

10. pants

Kompetenču centra sadarbība ar Savienības iestādēm, struktūrām, birojiem un aģentūrām

1. Kompetenču centrs sadarbojas ar attiecīgajām Savienības iestādēm, struktūrām, birojiem un aģentūrām, tostarp Eiropas Savienības Tīklu un informācijas drošības aģentūru, ES iestāžu un aģentūru datorapdraudējumu reaģēšanas vienību (*CERT-EU*), Eiropas Ārējās darbības dienestu, Komisijas Kopīgo pētniecības centru,

Pētniecības izpildaģentūru, Inovācijas un tīklu izpildaģentūru, Eiropola Eiropas Kibernoziedzības apkarošanas centru, kā arī Eiropas Aizsardzības aģentūru.

2. Šāda sadarbība notiek saskaņā ar darba vienošanos. Minēto vienošanos iesniedz Komisijai iepriekšējai apstiprināšanai.

II NODAĻA

KOMPETENČU CENTRA ORGANIZĀCIJA

11. pants

Dalība un struktūra

1. Kompetenču centra locekļi ir Savienība, ko pārstāv Komisija, un dalībvalstis.

2. Kompetenču centra struktūra veidota šādi:

(a) Valde, kas pilda 13. pantā noteiktos uzdevumus;

(b) izpilddirektors, kurš pilda 16. pantā noteiktos uzdevumus;

(c) Industriālā un zinātniskā konsultatīvā padome, kas pilda 20. pantā noteiktos uzdevumus.

I IEDAĻA

VALDE

12. pants

Valdes sastāvs

1. Valdē ir viens pārstāvis no katras dalībvalsts un pieci Komisijas pārstāvji, kuri rīkojas Savienības vārdā.

2. Katram Valdes loceklim ir aizstājējs, kurš attiecīgo personu pārstāv tās prombūtnes gadījumā.

3. Valdes locekļus un viņu aizstājējus ieceļ, pamatojoties uz viņu zināšanām tehnoloģiju jomā, kā arī viņu attiecīgajām vadības, administratīvajām un budžeta veidošanas prasmēm. Komisija un dalībvalstis cenšas ierobežot savu pārstāvju mainību Valdē, lai nodrošinātu Valdes darba nepārtrauktību. Komisija un dalībvalstis tiecas panākt vīriešu un sieviešu līdzsvarotu pārstāvību Valdē.

4. Valdes locekļu un viņu aizstājēju pilnvaru termiņš ir četri gadi. Minēto pilnvaru termiņu var pagarināt.

5. Valdes locekļi darbojas Kompetenču centra interesēs, neatkarīgi un pārredzami ievērojot tā mērķus un pamatuzdevumu, identitāti, autonomiju un saskanību.

6. Komisija var pieaicināt novērotājus, arī attiecīgo Savienības struktūru, biroju un aģentūru pārstāvjus, kuri attiecīgā gadījumā var piedalīties Valdes sēdēs.

7. Eiropas Tīklu un informācijas drošības aģentūra (*ENISA*) ir pastāvīgs novērotājs Valdē.

13. pants

Valdes uzdevumi

1. Valdei ir vispārēja atbildība par Kompetenču centra stratēģisko virzību un darbību, un Valde uzrauga tā pasākumu īstenošanu.

2. Valde pieņem savu reglamentu. Šie noteikumi ietver īpašas procedūras, lai identificētu interešu konfliktus un izvairītos no tiem, kā arī nodrošinātu sensitīvas informācijas konfidencialitāti.

3. Valde pieņem vajadzīgos stratēģiskos lēmumus, jo īpaši:

   (a) pieņem daudzgadu stratēģisko plānu, kurā ietverts paziņojums par Kompetenču centra galvenajām prioritātēm un plānotajām iniciatīvām, ieskaitot aplēses par finansējuma vajadzībām un avotiem;

   (b) pamatojoties uz izpilddirektora priekšlikumu, pieņem Kompetenču centra darba plānu, gada pārskatus un bilanci, kā arī gada darbības pārskatu;

   (c) pieņem Kompetenču centra īpašos finanšu noteikumus saskaņā ar [Finanšu regulas 70. pantu];

   (d) pieņem izpilddirektora iecelšanas procedūru;

   (e) pieņem kritērijus un procedūras, lai novērtētu un akreditētu subjektus kā kiberdrošības kompetenču kopienas locekļus;

   (f) ieceļ un atbrīvo no amata izpilddirektoru, pagarina viņa pilnvaru laiku, dod viņam norādījumus un uzrauga viņa darbības rezultātus, kā arī ieceļ amatā grāmatvedi;

   (g) pieņem Kompetenču centra gada budžetu, tostarp attiecīgo štatu sarakstu, kurā norādīts katras funkciju grupas un pakāpes pagaidu amata vietu skaits, kā arī līgumdarbinieku un norīkoto valsts ekspertu skaits, kas izteikts pilnslodzes ekvivalentos;

   (h) pieņem noteikumus attiecībā uz interešu konfliktiem;

   (i) kopā ar kiberdrošības kompetenču kopienas locekļiem izveido darba grupas;

   (j) ieceļ Industriālās un zinātniskās konsultatīvās padomes locekļus;

   (k) izveido iekšējās revīzijas struktūru saskaņā ar Komisijas Deleģēto regulu (ES) Nr. 1271/2013[28];

   (l) veicina Kompetenču centra atpazīstamību visā pasaulē, lai palielinātu tā pievilcību un padarītu to par struktūru, kurai kiberdrošības jomā izdevies sasniegt pasaules līmeņa izcilību;

   (m) pēc izpilddirektora ieteikuma nosaka Kompetenču centra komunikācijas politiku;

   (n) atbild par atbilstīgiem turpmākiem pasākumiem pēc retrospektīvu izvērtējumu secinājumiem;

[28] Komisijas 2013. gada 30. septembra Deleģētā regula (ES) Nr. 1271/2013 par finanšu pamatregulu struktūrām, kas minētas Eiropas Parlamenta un Padomes Regulas (ES, *Euratom*) Nr. 966/2012 208. pantā (OV L 328, 7.12.2013., 42. lpp.).

(o) ja nepieciešams, pieņem Civildienesta noteikumu un Nodarbināšanas kārtības īstenošanas noteikumus saskaņā ar 31. panta 3. punktu;

(p) vajadzības gadījumā paredz noteikumus par valsts ekspertu norīkošanu Kompetenču centrā, kā arī par stažieru izmantošanu saskaņā ar 32. panta 2. punktu;

(q) pieņem Kompetenču centra drošības noteikumus;

(r) pieņem krāpšanas apkarošanas stratēģiju, kas ir proporcionāla krāpšanas riskiem, ņemot vērā veicamo pasākumu izmaksu un ieguvumu analīzi;

(s) pieņem metodiku dalībvalstu finansiālā ieguldījuma aprēķināšanai;

(t) atbild par jebkuru uzdevumu, kas nav īpaši iedalīts konkrētai Kompetenču centra struktūrai; tā var uzticēt šādu uzdevumu izpildi jebkurai Kompetenču centra struktūrai.

14. pants

Valdes priekšsēdētājs un tās sēdes

1. Valde ievēl Valdes priekšsēdētāju un Valdes priekšsēdētāja vietnieku no balsstiesīgo locekļu vidus uz diviem gadiem. Valdes priekšsēdētāja un Valdes priekšsēdētāja vietnieka pilnvaru termiņu pēc Valdes lēmuma pieņemšanas var pagarināt vienu reizi. Savukārt, ja Valdes priekšsēdētāja vai Valdes priekšsēdētāja vietnieka dalība Valdē beidzas viņu amata pilnvaru termiņa laikā, tajā pašā dienā automātiski beidzas viņu amata pilnvaru termiņš. Valdes priekšsēdētāja vietnieks *ex officio* aizstāj Valdes priekšsēdētāju, ja Valdes priekšsēdētājs nespēj pildīt savus pienākumus. Valdes priekšsēdētājs piedalās balsošanā.
2. Valde rīko kārtējās sēdes vismaz trīsreiz gadā. Valde var rīkot ārkārtas sēdes pēc Komisijas, pēc trešdaļas visu Valdes locekļu, pēc Valdes priekšsēdētāja vai – savu uzdevumu izpildes ietvaros – pēc izpilddirektora pieprasījuma.
3. Izpilddirektors piedalās apspriedēs, ja vien Valde nav nolēmusi citādi, taču izpilddirektoram nav balsstiesību. Valde atsevišķos gadījumos var uzaicināt citas personas piedalīties tās sēdēs novērotāja statusā.
4. Industriālās un zinātniskās konsultatīvās padomes locekļi pēc Valdes priekšsēdētāja uzaicinājuma var piedalīties Valdes sēdēs, taču tiem nav balsstiesību.
5. Atbilstīgi Valdes reglamentam tās locekļiem un viņu aizstājējiem sēdēs var palīdzēt padomdevēji vai eksperti.
6. Kompetenču centrs nodrošina Valdes sekretariātu.

15. pants

Valdes balsošanas kārtība

1. Savienībai ir 50 % balsstiesību. Savienības balsstiesības nav dalāmas.
2. Katrai iesaistītajai dalībvalstij ir viena balss.
3. Valde pieņem lēmumus ar vismaz 75 % balsu vairākumu, ieskaitot klāt neesošo locekļu balsis; šis vairākums pārstāv vismaz 75 % no kopējām finansiālajām iemaksām Kompetenču centrā. Finansiālais ieguldījums tiek aprēķināts, pamatojoties uz 17. panta 2. punkta c) apakšpunktā minētajiem aprēķinātajiem izdevumiem, kurus

ierosinājušas dalībvalstis, un pamatojoties uz ziņojumu par iesaistīto dalībvalstu ieguldījuma vērtību, atbilstoši 22. panta 5. punktam.

4. Balsstiesības ir vienīgi Komisijas un iesaistīto dalībvalstu pārstāvjiem.

5. Valdes priekšsēdētājs piedalās balsošanā.

II IEDAĻA

IZPILDDIREKTORS

16. pants

Izpilddirektora iecelšana amatā, atlaišana vai pilnvaru termiņa pagarināšana

1. Izpilddirektors ir persona, kam ir lietpratība un augsta reputācija Kompetenču centra darbības jomās.

2. Izpilddirektoru pieņem darbā kā Kompetenču centra pagaidu darbinieku saskaņā ar Pārējo darbinieku nodarbināšanas kārtības 2. panta a) apakšpunktu.

3. Izpilddirektoru ieceļ Valde no Komisijas ierosināto kandidātu saraksta pēc atklātas un pārredzamas atlases procedūras.

4. Lai noslēgtu līgumu ar izpilddirektoru, Kompetenču centru pārstāv Valdes priekšsēdētājs.

5. Izpilddirektora amata pilnvaru termiņš ir četri gadi. Līdz minētā laikposma beigām Komisija veic novērtējumu, kurā ņem vērā izpilddirektora snieguma izvērtējumu un Kompetenču centra turpmākos uzdevumus un problēmjautājumus.

6. Valde, rīkojoties pēc Komisijas priekšlikuma, kurā ņemts vērā 5. punktā minētais novērtējums, izpilddirektora amata pilnvaru laiku var vienu reizi pagarināt uz laiku, kas nepārsniedz četrus gadus.

7. Izpilddirektors, kura pilnvaru termiņš ir ticis pagarināts, nevar piedalīties citā atlases procedūrā uz to pašu amata vietu.

8. Izpilddirektoru no amata atceļ tikai ar Valdes lēmumu, kas pieņemts pēc Komisijas priekšlikuma.

17. pants

Izpilddirektora uzdevumi

1. Izpilddirektors ir atbildīgs par Kompetenču centra darbību un ikdienas pārvaldību, kā arī ir tā likumīgais pārstāvis. Izpilddirektors atskaitās Valdei un veic savus pienākumus pilnīgi neatkarīgi saskaņā ar viņam piešķirtajām pilnvarām.

2. Izpilddirektors neatkarīgi veic jo īpaši šādus uzdevumus:

   (a) īsteno Valdes pieņemtos lēmumus;

   (b) palīdz Valdei tās darbā, nodrošina sēžu sekretariātu un sniedz visu informāciju, kas nepieciešama viņu pienākumu pildīšanai;

   (c) pēc apspriešanās ar Valdi un Komisiju, sagatavo un iesniedz pieņemšanai Valdē daudzgadu stratēģiskā plāna projektu un Kompetenču centra ikgadējā darba plāna projektu, ietverot darba plāna īstenošanai nepieciešamo uzaicinājumu iesniegt priekšlikumus, uzaicinājumu izteikt ieinteresētību un uzaicinājumu iesniegt piedāvājumus tvērumu, kā arī attiecīgo Komisijas un dalībvalstu ierosināto izdevumu aplēses;

(d) sagatavo un iesniedz pieņemšanai Valdē gada budžeta projektu, tai skaitā attiecīgo štatu sarakstu, kurā norādīts katras funkciju grupas un pakāpes pagaidu amata vietu skaits, kā arī līgumdarbinieku un norīkoto valsts ekspertu skaits, kas izteikts pilnslodzes ekvivalentos;

(e) īsteno darba plānu un ziņo par to Valdei;

(f) sagatavo Kompetenču centra gada darbības pārskatu, ieskaitot informāciju par attiecīgajiem izdevumiem;

(g) nodrošina efektīvu uzraudzības un izvērtēšanas procedūru ieviešanu saistībā ar Kompetenču centra darbību;

(h) sagatavo turpmākas rīcības plānu atbilstīgi retrospektīvu novērtējumu secinājumiem un divreiz gadā par īstenošanas gaitu ziņo Komisijai;

(i) sagatavo, apspriež un slēdz līgumus ar nacionālajiem koordinācijas centriem;

(j) atbild par administratīviem, finanšu un personāla jautājumiem, tostarp par Kompetenču centra budžeta izpildi, pienācīgi ņemot vērā padomus, kas saņemti no iekšējās revīzijas struktūras, Valdes deleģēto pienākumu ietvaros;

(k) apstiprina un pārvalda uzaicinājumu izteikt priekšlikumus izsludināšanu saskaņā ar darba plānu, kā arī administrē dotāciju nolīgumus un lēmumus;

(l) apstiprina finansējumam atlasīto darbību sarakstu, balstoties uz neatkarīgu ekspertu grupas izveidotu sarindojuma sarakstu;

(m) apstiprina un pārvalda uzaicinājumu izteikt piedāvājumus izsludināšanu saskaņā ar darba plānu un administrē līgumus;

(n) apstiprina finansēšanai atlasītos piedāvājumus;

(o) iesniedz gada pārskatu projektu un bilanci iekšējai revīzijas struktūrai un pēc tam arī Valdei;

(p) nodrošina riska novērtējuma un riska pārvaldības veikšanu;

(q) paraksta individuālus dotāciju nolīgumus, lēmumus un līgumus;

(r) paraksta iepirkuma līgumus;

(s) sagatavo turpmākas rīcības plānu atbilstīgi secinājumiem, kas izriet no iekšējās vai ārējās revīzijas ziņojumiem, kā arī no izmeklēšanas, kuru veicis Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un divreiz gadā par plāna īstenošanas gaitu ziņo Komisijai un regulāri — Valdei;

(t) sagatavo Kompetenču centram piemērojamos finanšu noteikumus;

(u) izveido efektīvu un lietderīgu iekšējās kontroles sistēmu un nodrošina tās darbību, kā arī ziņo Valdei par jebkādām būtiskām pārmaiņām šādā sistēmā;

(v) nodrošina efektīvu saziņu ar Savienības iestādēm;

(w) veic citus pasākumus, kas nepieciešami, lai novērtētu Kompetenču centra virzību tā pamatuzdevuma un mērķu izpildes virzienā saskaņā ar šīs regulas 3. un 4. pantu;

(x) veic visus citus uzdevumus, ko viņam vai viņai uzticējusi vai deleģējusi Valde.

III IEDAĻA

INDUSTRIĀLĀ UN ZINĀTNISKĀ KONSULTATĪVĀ PADOME

18. pants

Industriālās un zinātniskās konsultatīvās padomes sastāvs

1. Industriālā un zinātniskā konsultatīvā padome sastāv no ne vairāk kā 16 locekļiem. Locekļus no kiberdrošības kompetenču kopienas subjektu pārstāvju vidus ieceļ Valde.

2. Industriālās un zinātniskās konsultatīvās padomes locekļiem ir lietpratība vai nu attiecībā uz kiberdrošības pētniecību, industriālo attīstību, profesionālajiem pakalpojumiem vai to plašāku ieviešanu. Prasības attiecībā uz šādu lietpratību sīkāk precizē Valde.

3. Valdes procedūras konsultatīvās padomes locekļu iecelšanai, kā arī konsultatīvās padomes darbības procedūras nosaka Kompetenču centra reglamentā un publisko.

4. Industriālās un zinātniskās konsultatīvās padomes locekļu pilnvaru termiņš ir trīs gadi. Minēto pilnvaru termiņu var pagarināt.

5. Komisijas un Eiropas Savienības Tīklu un informācijas drošības aģentūras pārstāvji var piedalīties Industriālās un zinātniskās konsultatīvās padomes darbībā un atbalstīt to.

19. pants

Industriālās un zinātniskās konsultatīvās padomes darbība

1. Industriālā un zinātniskā konsultatīvā padome tiekas sanāksmēs vismaz divreiz gadā.

2. Industriālā un zinātniskā konsultatīvā padome var ieteikt Valdei izveidot darba grupas, kuru kompetencē būtu īpaši ar Kompetenču centra darbību saistīti jautājumi un, ja tas nepieciešams, kuru vispārējo koordināciju veic viens vai vairāki Industriālās un zinātniskās konsultatīvās padomes locekļi.

3. Industriālā un zinātniskā konsultatīvā padome ievēl tās priekšsēdētāju.

4. Industriālā un zinātniskā konsultatīvā padome pieņem savu reglamentu, ieskaitot to pārstāvju izvirzīšanu, kuri vajadzības gadījumā pārstāv konsultatīvo padomi, kā arī nosaka viņu pārstāvības ilgumu.

20. pants

Industriālās un zinātniskās konsultatīvās padomes uzdevumi

Industriālā un zinātniskā konsultatīvā padome konsultē Kompetenču centru attiecībā uz tā pasākumu īstenošanu, kā arī:

(1) sniedz stratēģiskas konsultācijas izpilddirektoram un Valdei, kā arī ieguldījumu darba plāna un daudzgadu stratēģiskā plāna izstrādē Valdes noteiktajos termiņos;

(2) lai apkopotu 1. punktā minētajām stratēģiskajām konsultācijām nepieciešamo informāciju, organizē sabiedriskās apspriešanas, kurās var piedalīties visas ieinteresētās personas no publiskā un privātā sektora kiberdrošības jomā;

(3) veicina un apkopo atsauksmes par Kompetenču centra darba plānu un daudzgadu stratēģisko plānu.

III NODAĻA

FINANŠU NOTEIKUMI

21. pants

Savienības finansiālais ieguldījums

1. Savienības ieguldījums Kompetenču centrā administratīvo un darbības izmaksu segšanai ietver:

   (a) 1 981 668 000 EUR no Digitālās Eiropas programmas, ieskaitot līdz 23 746 000 EUR administratīvajām izmaksām;

   (b) ieguldījuma summu no pamatprogrammas "Apvārsnis Eiropa", arī administratīvo izmaksu segšanai, kas nosakāma, ņemot vērā stratēģiskās plānošanas procesu, kas jāveic saskaņā ar Regulas XXX ["Apvārsnis Eiropa" regula] 6. panta 6. punktu.

2. Savienības maksimālo ieguldījumu izmaksā no Savienības vispārējā budžeta apropriācijām, kas piešķirtas [Digitālās Eiropas programmai] un īpašajai programmai, kura izveidota ar Lēmumu XXX un ar kuru īsteno pamatprogrammu "Apvārsnis Eiropa".

3. Kompetenču centrs īsteno [Digitālās Eiropas programmas] un [pamatprogrammas "Apvārsnis Eiropa"] kiberdrošības darbības saskaņā ar Regulas (ES, *Euratom*) XXX[29] [Finanšu regula] 62. panta c) punkta iv) apakšpunktu.

4. Savienības finansiālais ieguldījums nesedz ar 4. panta 8. punkta b) apakšpunktā minētajiem uzdevumiem saistītās izmaksas.

22. pants

Iesaistīto dalībvalstu veicamās iemaksas

1. Iesaistītās dalībvalstis veic kopējās iemaksas Kompetenču centra administratīvo un darbības izmaksu segšanai vismaz tādā pašā apmērā, kāds minēts šīs regulas 21. panta 1. punktā.

2. Lai novērtētu 1. punktā, kā arī 23. panta 3. punkta b) apakšpunkta ii) daļā minētās iemaksas, izmaksas nosaka atbilstīgi attiecīgo dalībvalstu ierastajai izmaksu uzskaites praksei, dalībvalstī piemērojamiem grāmatvedības standartiem un piemērojamiem starptautiskajiem grāmatvedības standartiem, un starptautiskajiem finanšu pārskatu standartiem. Izmaksas apstiprina neatkarīgs ārējs revidents, ko iecēlusi attiecīgā dalībvalsts. Ja apstiprināšanā rodas neskaidrības, Kompetenču centrs pārbauda vērtēšanas metodi.

3. Ja kāda no iesaistītajām dalībvalstīm nav izpildījusi savas finansiālā ieguldījuma saistības, izpilddirektors to fiksē rakstiski un nosaka pieņemamu laikposmu, kurā neizpilde jānovērš. Ja šāds stāvoklis minētajā termiņā netiek novērsts, izpilddirektors sasauc Valdes sēdi, lai lemtu, vai līdz pienākumu izpildei būtu jāatsauc attiecīgās iesaistītās dalībvalsts balsstiesības vai būtu jāveic kādi citi pasākumi. Saistības nepildošās dalībvalsts balsstiesības tiek atņemtas līdz saistību neizpildes novēršanai.

[29] [pievienot pilnu virsrakstu un OV atsauci].

4. Komisija var izbeigt, proporcionāli samazināt vai apturēt Savienības finansiālo ieguldījumu Kompetenču centrā, ja attiecībā uz 1. punktā minētajiem ieguldījumiem iesaistītās dalībvalstis neveic iemaksas, veic tās tikai daļēji vai novēloti.

5. Iesaistītās dalībvalstis līdz katra gada 31. janvārim ziņo Valdei par 1. punktā minēto, katrā iepriekšējā finanšu gadā veikto ieguldījumu vērtību.

23. pants

Kompetenču centra izmaksas un resursi

1. Kompetenču centru kopīgi finansē Savienība un dalībvalstis, veicot finansiālās iemaksas, kuras maksā pa daļām, kā arī iemaksas, kas ietver izmaksas, kuras radušās nacionālajiem koordinācijas centriem un saņēmējiem, īstenojot darbības, kuru izmaksas Kompetenču centrs neatlīdzina.

2. Kompetenču centra administratīvās izmaksas nepārsniedz [skaitlis] EUR, un tās tiek segtas ar finansiālu ieguldījumu, kas katru gadu tiek sadalīts vienādi starp Savienību un iesaistītajām dalībvalstīm. Ja daļa no administratīvo izmaksu segšanai paredzētā ieguldījuma netiek izmantota, to var novirzīt Kompetenču centra darbības izmaksu segšanai.

3. Kompetenču centra darbības izmaksas sedz, izmantojot:

   (a) Savienības finansiālo ieguldījumu;

   (b) iesaistīto dalībvalstu iemaksas šādās formās:

      i) finansiālās iemaksas un

      ii) vajadzības gadījumā iesaistīto dalībvalstu iemaksas natūrā par izmaksām, kas radušās nacionālajiem koordinācijas centriem un saņēmējiem netiešo darbību īstenošanā, atskaitot Kompetenču centra ieguldījumu un jebkuru citu Savienības ieguldījumu šajās izmaksās.

4. Kompetenču centra resursus, kas iekļauti tā budžetā, veido šādas iemaksas:

   (a) iesaistīto dalībvalstu finansiālās iemaksas administratīvo izmaksu segšanai;

   (b) iesaistīto dalībvalstu finansiālās iemaksas darbības izmaksu segšanai;

   (c) visi Kompetenču centra gūtie ieņēmumi;

   (d) jebkādas citas finansiālās iemaksas, līdzekļi un ieņēmumi.

5. Jebkādi iesaistīto dalībvalstu Kompetenču centram veikto iemaksu nestie procenti uzskatāmi par tā ieņēmumiem.

6. Visi Kompetenču centra resursi un tā pasākumi ir vērsti uz 4. pantā izklāstīto mērķu sasniegšanu.

7. Kompetenču centram pieder visi aktīvi, ko tas radījis vai kas tam nodoti tā mērķu sasniegšanai.

8. Izņemot gadījumu, kad Kompetenču centrs tiek likvidēts, jebkuri izdevumus pārsniedzoši ieņēmumi netiek izmaksāti iesaistītajiem Kompetenču centra locekļiem.

24. pants

Finanšu saistības

Kompetenču centra finanšu saistības nepārsniedz tā budžetā pieejamo vai tā locekļu atvēlēto finanšu līdzekļu apjomu.

25. pants

Finanšu gads

Finanšu gads ilgst no 1. janvāra līdz 31. decembrim.

26. pants

Budžeta izveide

1. Katru gadu izpilddirektors izstrādā Kompetenču centra ieņēmumu un izdevumu tāmes projektu nākamajam finanšu gadam un kopā ar štatu saraksta projektu nosūta Valdei. Ieņēmumiem un izdevumiem jābūt līdzsvarā. Kompetenču centra izdevumi ietver personāla, administratīvās, infrastruktūras un darbības izmaksas. Administratīvajiem izdevumiem jābūt pēc iespējas mazākiem.
2. Pamatojoties uz 1. punktā minēto ieņēmumu un izdevumu tāmes projektu, katru gadu Valde sagatavo Kompetenču centra ieņēmumu un izdevumu tāmi nākamajam finanšu gadam.
3. Līdz katra gada 31. janvārim Valde nosūta Komisijai 2. punktā minēto tāmi, kas ir daļa no vienotā programmdokumenta projekta.
4. Pamatojoties uz minēto tāmi, Komisija Savienības budžeta projektā iekļauj aplēses, ko tā uzskata par vajadzīgām attiecībā uz štatu sarakstu un tās iemaksas apjomu, kas maksājama no vispārējā budžeta, un iesniedz tās Eiropas Parlamentam un Padomei saskaņā ar LESD 313. un 314. pantu.
5. Eiropas Parlaments un Padome apstiprina iemaksu apropriācijas Kompetenču centram.
6. Eiropas Parlaments un Padome pieņem Kompetenču centra štatu sarakstu.
7. Valde kopā ar darba plānu pieņem Kompetenču centra budžetu. Tas kļūst par galīgo variantu pēc Savienības vispārējā budžeta pieņemšanas galīgajā redakcijā. Vajadzības gadījumā Valde Kompetenču centra budžetu un darba plānu pielāgo saskaņā ar Savienības vispārējo budžetu.

27. pants

Kompetenču centra pārskatu sniegšana un budžeta izpildes apstiprināšana

Kompetenču centra provizorisko un galīgo pārskatu iesniegšana un budžeta izpildes apstiprināšana jāveic saskaņā ar Finanšu regulu un tās finanšu noteikumiem un grafiku, kas pieņemti saskaņā ar 29. pantu.

28. pants

Darbības un finanšu pārskati

1. Izpilddirektors katru gadu ziņo Valdei par savu pienākumu izpildi saskaņā ar Kompetenču centra finanšu noteikumiem.
2. Divu mēnešu laikā pēc katra finanšu gada beigām izpilddirektors apstiprināšanai iesniedz Valdei gada darbības pārskatu par Kompetenču centra paveikto iepriekšējā

kalendārajā gadā, īpaši saistībā ar konkrētā gada darba plānu. Minētajā pārskatā cita starpā ietver informāciju par šādiem jautājumiem:

(a) paveiktās operatīvās darbības un attiecīgie izdevumi;

(b) iesniegtās darbības, tostarp to sadalījums atbilstīgi dalībnieku veidam, ieskaitot MVU, un dalībvalstīm;

(c) finansējumam atlasītās darbības, tostarp to sadalījums atbilstīgi dalībnieku veidam, tai skaitā MVU, un atbilstīgi dalībvalstīm, norādot Kompetenču centra ieguldījumu saistībā ar individuāliem dalībniekiem un darbībām;

(d) progress 4. pantā noteikto mērķu sasniegšanā un turpmākas darbības priekšlikumi šo mērķu sasniegšanai.

3. Gada darbības pārskatu pēc tam, kad Valde to ir apstiprinājusi, dara publiski pieejamu.

29. pants

Finanšu noteikumi

Kompetenču centrs pieņem savus īpašos finanšu noteikumus saskaņā ar Regulas XXX [jaunā Finanšu regula] 70. pantu.

30. pants

Finansiālo interešu aizsardzība

1. Kompetenču centrs veic piemērotus pasākumus, lai nodrošinātu, ka, īstenojot saskaņā ar šo regulu finansētas darbības, Savienības finansiālās intereses tiek aizsargātas ar krāpšanas, korupcijas un jebkādu citu nelikumīgu darbību novēršanas pasākumiem, efektīvām pārbaudēm un, ja ir atklāti pārkāpumi, atgūstot nepamatoti izmaksātās summas un attiecīgā gadījumā piemērojot iedarbīgus, samērīgus un atturošus administratīvus sodus.

2. Kompetenču centrs piešķir Komisijas personālam un citām Komisijas, kā arī Revīzijas palātas pilnvarotajām personām piekļuvi objektiem un telpām un visai informācijai, tostarp informācijai elektroniskā formātā, kas nepieciešama revīziju veikšanai.

3. Eiropas Birojs krāpšanas apkarošanai (*OLAF*) var veikt izmeklēšanu, tostarp pārbaudes un inspekcijas uz vietas, saskaņā ar noteikumiem un procedūrām, kas noteiktas Padomes Regulā (*Euratom*, EK) Nr. 2185/96[30] un Eiropas Parlamenta un Padomes Regulā (ES, *Euratom*) Nr. 883/2013[31] ar mērķi noteikt, vai ir notikusi krāpšana, korupcija vai kādas citas nelikumīgas darbības, kas ietekmē Savienības finanšu intereses saistībā ar dotācijas nolīgumu vai līgumu, kas tieši vai netieši finansēts saskaņā ar šo regulu.

---

30 Padomes 1996. gada 11. novembra Regula (*Euratom*, EK) Nr. 2185/96 par pārbaudēm un apskatēm uz vietas, ko Komisija veic, lai aizsargātu Eiropas Kopienu finanšu intereses pret krāpšanu un citām nelikumībām (OV L 292, 15.11.1996., 2. lpp.).

31 Eiropas Parlamenta un Padomes 2013. gada 11. septembra Regula (ES, *Euratom*) Nr. 883/2013 par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1073/1999 un Padomes Regulu (*Euratom*) Nr. 1074/1999 (OV L 248, 18.9.2013., 1. lpp.).

4. Neskarot šā panta 1., 2. un 3. punktu, līgumiem un dotāciju nolīgumiem, kas izriet no šīs regulas īstenošanas, jāsatur noteikumi, kas nepārprotami nosaka Komisijas, Kompetenču centra, Revīzijas palātas un *OLAF* pilnvaras atbilstoši to kompetencei veikt šādas revīzijas un izmeklēšanu. Ja darbības īstenošanai pilnā apmērā vai daļēji tiek izmantoti ārpakalpojumi vai tā tiek deleģēta tālāk, vai ir vajadzīgs noslēgt publiskā iepirkuma līgumu vai piešķirt finansiālu atbalstu trešai personai, attiecīgajā līgumā vai dotācijas nolīgumā atbalsta saņēmējam uzliek pienākumu nodrošināt, lai katra iesaistītā trešā persona nepārprotami akceptētu minētās Komisijas, Kompetenču centra, Revīzijas palātas un *OLAF* pilnvaras.

IV NODAĻA
KOMPETENČU CENTRA PERSONĀLS

31. pants

Personāls

1. Kompetenču centra personālam piemēro Eiropas Savienības Civildienesta noteikumus un Savienības pārējo darbinieku nodarbināšanas kārtību, atbilstoši Padomes Regulai (EEK, *Euratom*, EOTK) Nr. 259/68[32] (turpmāk "Civildienesta noteikumi" un "Nodarbināšanas kārtība"), kā arī noteikumus, kurus Savienības iestādes kopīgi pieņēmušas Civildienesta noteikumu un Nodarbināšanas kārtības piemērošanai.

2. Valde attiecībā uz Kompetenču centra personālu īsteno pilnvaras, kas ar Civildienesta noteikumiem piešķirtas iecēlējinstitūcijai, un pilnvaras, kas ar Nodarbināšanas kārtību piešķirtas iestādei, kura pilnvarota slēgt līgumu (turpmāk "iecēlējinstitūcijas pilnvaras").

3. Saskaņā ar Civildienesta noteikumu 110. pantu, pamatojoties uz Civildienesta noteikumu 2. panta 1. punktu un Nodarbināšanas kārtības 6. pantu, Valde pieņem lēmumu, kurā attiecīgās iecēlējinstitūcijas pilnvaras piešķir izpilddirektoram un definē nosacījumus, kādos minēto deleģējumu var apturēt. Izpilddirektors ir pilnvarots minētās pilnvaras deleģēt tālāk.

4. Ārkārtas apstākļu spiesta, Valde var pieņemt lēmumu uz laiku apturēt iecēlējinstitūcijas pilnvaru deleģējumu izpilddirektoram un jebkādu tā pilnvaru tālākdeleģēšanu. Šādā gadījumā Valde pati īsteno iecēlējinstitūcijas pilnvaras vai deleģē tās kādam no tās locekļiem vai Kompetenču centra personāla darbiniekam, kurš nav izpilddirektors.

5. Valde pieņem Civildienesta noteikumu un Nodarbināšanas kārtības īstenošanas noteikumus saskaņā ar Civildienesta noteikumu 110. pantu.

6. Personāla resursus nosaka Kompetenču centra štatu sarakstā, kurā norāda pagaidu darbinieku skaitu atbilstīgi funkciju grupām un pakāpēm, kā arī līgumdarbinieku skaitu, izteiktu pilnslodzes ekvivalentos, atbilstīgi tā gada budžetam.

7. Kompetenču centra personālā ir uz noteiktu laiku pieņemti darbinieki un līgumdarbinieki.

---

[32] Padomes 1968. gada 29. februāra Regula (EEK, *Euratom*, EOTK) Nr. 259/68, ar ko nosaka Eiropas Kopienu Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību, kā arī paredz īpašus Komisijas ierēdņiem uz laiku piemērojamus pasākumus (OV L 56, 4.3.1968., 1. lpp.).

8. Visas ar personālu saistītās izmaksas sedz Kompetenču centrs.

32. pants

Norīkotie valsts eksperti un cits personāls

1. Kompetenču centrs var izmantot norīkotos valsts ekspertus vai citus darbiniekus, kuri netiek nodarbināti Kompetenču centrā.
2. Valde, vienojoties ar Komisiju, pieņem lēmumu, ar ko paredz noteikumus par valsts ekspertu norīkošanu Kompetenču centrā.

33. pants

Privilēģijas un imunitāte

Uz Kompetenču centru un tā personālu attiecas Protokols Nr. 7 par privilēģijām un imunitāti Eiropas Savienībā, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību.

V NODAĻA
KOPĪGIE NOTEIKUMI

34. pants

Drošības noteikumi

1. Regulas (ES) Nr. XXX [Digitālās Eiropas programma] 12. panta 7. punkts attiecas uz dalību visās Kompetenču centra finansētajās darbībās.
2. Pamatprogrammas "Apvārsnis Eiropa" finansētajām darbībām piemēro šādus īpašos drošības noteikumus:
   (a) ņemot vērā Regulas (ES) Nr. XXX ["Apvārsnis Eiropa" regula] 34. panta 1. punktu ["Īpašumtiesības un aizsardzība"], ja tas paredzēts darba plānā, vienkāršu licenču piešķiršana var attiekties tikai uz trešām personām, kuras iedibinātas vai tiek uzskatītas par iedibinātām dalībvalstīs un kuras kontrolē dalībvalstis un/vai dalībvalstu valstspiederīgie;
   (b) ņemot vērā Regulas (ES) Nr. XXX ["Apvārsnis Eiropa" regula] 36. panta 4. punkta b) apakšpunktu ["Nodošana un licencēšana"], licences nodošana tiesību subjektam, kas iedibināts asociētā valstī vai kas iedibināts Savienībā, bet tiek kontrolēts no trešām valstīm, arī ir pamats iebildumiem pret rezultātu īpašumtiesību maiņu vai pret ekskluzīvas licences piešķiršanu attiecībā uz rezultātiem;
   (c) ņemot vērā Regulas (ES) Nr. XXX ["Apvārsnis Eiropa" regula] 37. panta 3. punkta a) apakšpunktu ["Piekļuves tiesības"], ja tas paredzēts darba plānā, piekļuve rezultātiem un iepriekš uzkrātām zināšanām var tikt ierobežota, piešķirot to tikai tiesību subjektam, kas iedibināts vai ko uzskata par iedibinātu dalībvalstīs, bet ko kontrolē dalībvalstis un/vai dalībvalstu valstspiederīgie.

35. pants

Pārredzamība

1. Kompetenču centrs savā darbībā nodrošina augsta līmeņa pārredzamību.

2. Kompetenču centrs gādā, lai sabiedrība un visas ieinteresētās personas saņemtu atbilstošu, objektīvu, ticamu un viegli pieejamu informāciju, jo īpaši attiecībā uz tā darba rezultātiem. Tas arī publicē interešu deklarācijas, kas iesniegtas saskaņā ar 41. pantu.

3. Valde pēc izpilddirektora priekšlikuma drīkst atļaut ieinteresētajām personām novērot dažu Kompetenču centra pasākumu norisi.

4. Kompetenču centrs savā reglamentā nosaka praktiskos pasākumus, lai īstenotu 1. un 2. punktā minētos pārredzamības noteikumus. Attiecībā uz darbībām, kuras finansē no pamatprogrammas "Apvārsnis Eiropa", pienācīgi tiks ņemti vērā "Apvārsnis Eiropa" regulas III pielikumā norādītie noteikumi.

36. pants

Drošības noteikumi par klasificētas informācijas un sensitīvas neklasificētas informācijas aizsardzību

1. Neskarot 35. pantu, Kompetenču centrs neizpauž trešām personām informāciju, ko tas apstrādā vai saņem, ja par visu informāciju vai tās daļu ir izteikts pamatots pieprasījums to uzskatīt par konfidenciālu.

2. Valdes locekļi, izpilddirektors, Industriālās un zinātniskās konsultatīvās padomes locekļi, ārējie eksperti, kas piedalās *ad hoc* darba grupās, un Kompetenču centra personāls ievēro konfidencialitātes prasības saskaņā ar Līguma par Eiropas Savienības darbību 339. pantu pat pēc tam, kad ir beiguši pildīt attiecīgos amata pienākumus.

3. Pēc tam, kad saņemts Komisijas apstiprinājums, Kompetenču centra Valde pieņem Kompetenču centra drošības noteikumus, pamatojoties uz principiem un noteikumiem, kas paredzēti Komisijas drošības noteikumos par Eiropas Savienības klasificētas informācijas (ESKI) un sensitīvas neklasificētas informācijas aizsardzību, tostarp noteikumos par šādas informācijas apstrādi un uzglabāšanu, kā izklāstīts Komisijas Lēmumos (ES, *Euratom*) 2015/443[33] un 2015/444[34].

4. Kompetenču centrs var veikt visus nepieciešamos pasākumus, lai atvieglotu ar tā uzdevumiem saistītās informācijas apmaiņu ar Komisiju un dalībvalstīm un attiecīgā gadījumā ar saistītajām Savienības aģentūrām un struktūrām. Attiecībā uz jebkādu šajā nolūkā noslēgtu administratīvu vienošanos par ESKI koplietošanu vai, ja šāda vienošanās nepastāv, jebkādu ESKI ārkārtas *ad hoc* izpaušanu jābūt iepriekš saņemtam Komisijas apstiprinājumam.

37. pants

Piekļuve dokumentiem

1. Kompetenču centrā glabātajiem dokumentiem piemēro Regulu (EK) Nr. 1049/2001.

---

33 Komisijas 2015. gada 13. marta Lēmums (ES, *Euratom*) 2015/443 par drošību Komisijā (OV L 72, 17.3.2015., 41. lpp.).

34 Komisijas 2015. gada 13. marta Lēmums (ES, *Euratom*) 2015/444 par drošības noteikumiem ES klasificētas informācijas aizsardzībai (OV L 72, 17.3.2015., 53. lpp.).

2. Sešu mēnešu laikā pēc Kompetenču centra izveides Valde pieņem pasākumus Regulas (EK) Nr. 1049/2001 īstenošanai.

3. Par lēmumiem, ko Kompetenču centrs pieņem atbilstīgi Regulas (EK) Nr. 1049/2001 8. pantam, var iesniegt sūdzību ombudam saskaņā ar Līguma par Eiropas Savienības darbību 228. pantu vai prasību Eiropas Savienības Tiesā saskaņā ar Līguma par Eiropas Savienības darbību 263. pantu.

38. pants

Uzraudzība, izvērtēšana un pārskatīšana

1. Kompetenču centrs nodrošina, ka tā pasākumi, tostarp tie, ko pārvalda ar nacionālo koordinācijas centru un Tīkla starpniecību, tiek regulāri un sistemātiski pārraudzīti un periodiski izvērtēti. Kompetenču centrs nodrošina, ka datu vākšana programmu īstenošanas un rezultātu uzraudzībai norit efektīvi, lietderīgi un savlaicīgi, un Savienības līdzekļu saņēmējiem un dalībvalstīm tiek piemērotas samērīgas ziņošanas prasības. Izvērtējuma rezultātus publisko.

2. Tiklīdz ir pieejama pietiekama informācija par šīs regulas īstenošanu, bet ne vēlāk kā trīsarpus gadus pēc šīs regulas īstenošanas sākuma, Komisija veic Kompetenču centra starpposma izvērtējumu. Komisija sagatavo ziņojumu par šo izvērtējumu un līdz 2024. gada 31. decembrim iesniedz to Eiropas Parlamentam un Padomei. Kompetenču centrs un dalībvalstis sniedz Komisijai informāciju, kas nepieciešama šā ziņojuma sagatavošanai.

3. Izvērtējums, kas minēts 2. punktā, ietver Kompetenču centra sasniegto rezultātu novērtējumu, ņemot vērā tā mērķus, pilnvaras un uzdevumus. Ja Komisija uzskata, ka Kompetenču centra darba turpināšana ir pamatota, ņemot vērā tā mērķus, pilnvaras un uzdevumus, tā var ierosināt pagarināt 46. pantā noteikto Kompetenču centra pilnvaru termiņu.

4. Pamatojoties uz 2. punktā minētā starpposma izvērtējuma secinājumiem, Komisija var rīkoties saskaņā ar [22. panta 5. punktu] vai veikt jebkādas citas atbilstīgas darbības.

5. Pamatprogrammas "Apvārsnis Eiropa" ieguldījuma uzraudzība, izvērtēšana, pakāpeniska pārtraukšana un atjaunošana notiek atbilstoši "Apvārsnis Eiropa" regulas 8., 45. un 47. pantam, kā arī III pielikumam un apstiprinātajai īstenošanas kārtībai.

6. Digitālās Eiropas programmas ieguldījuma uzraudzība, ziņošana un izvērtēšana notiek atbilstoši Digitālās Eiropas programmas 24. un 25. pantam.

7. Kompetenču centra likvidācijas gadījumā Komisija veic Kompetenču centra galīgo izvērtējumu sešu mēnešu laikā pēc tā likvidēšanas, bet ne vēlāk kā divus gadus pēc šīs regulas 46. pantā minētās likvidācijas procedūras uzsākšanas. Galīgā izvērtējuma rezultātus dara zināmus Eiropas Parlamentam un Padomei.

39. pants

Kompetenču centra atbildība

1. Kompetenču centra līgumisko atbildību reglamentē tiesību akti, kas piemērojami attiecīgajam nolīgumam, lēmumam vai līgumam.

2. Ārpuslīgumiskas atbildības gadījumā Kompetenču centrs saskaņā ar vispārējiem principiem, kas ir kopīgi dalībvalstu tiesību aktiem, atlīdzina jebkādu kaitējumu, ko, pildot pienākumus, radījuši tā darbinieki.

3. Visus Kompetenču centra veiktos maksājumus attiecībā uz 1. un 2. punktā minēto atbildību un ar to saistītās izmaksas un izdevumus uzskata par Kompetenču centra izdevumiem un sedz no centra līdzekļiem.

4. Kompetenču centrs atbild vienīgi par savu pienākumu izpildi.

40. pants

Eiropas Savienības Tiesas piekritība un piemērojamie tiesību akti

1. Eiropas Savienības Tiesai ir piekritība:

   (1) lietās saskaņā ar jebkuru šķīrējklauzulu, kas iekļauta Kompetenču centra noslēgtajos nolīgumos, lēmumos vai līgumos;

   (2) strīdos par kompensāciju Kompetenču centra darbinieku rīcības rezultātā radīta kaitējuma gadījumā;

   (3) visos strīdos starp Kompetenču centru un tā personālu atbilstīgi ierobežojumiem un nosacījumiem, kas paredzēti Civildienesta noteikumos.

2. Gadījumos, uz kuriem neattiecas šī regula un citi Savienības tiesību akti, piemēro Kompetenču centra mītnes valsts tiesību aktus.

41. pants

Locekļu atbildība un apdrošināšana

1. Attiecībā uz Kompetenču centra parādiem locekļu finansiālā atbildība aprobežojas tikai ar ieguldījumu, ko tie jau snieguši administratīvo izmaksu segšanai.

2. Kompetenču centrs noslēdz pienācīgus apdrošināšanas līgumus un uztur tos spēkā.

42. pants

Interešu konflikti

Kompetenču centra Valde pieņem noteikumus interešu konflikta novēršanai un pārvaldībai attiecībā uz Kompetenču centra locekļiem, struktūrām un norīkoto personālu. Tajos saskaņā ar Regulu XXX [jaunā Finanšu regula] ietver noteikumus, kas paredzēti, lai izvairītos no interešu konfliktiem, kuros var būt iesaistīti Valdes locekļu pārstāvji, kā arī Zinātniskās un industriālās konsultatīvās padomes locekļu pārstāvji.

43. pants

Personas datu aizsardzība

1. Uz Kompetenču centra veikto personas datu apstrādi attiecas Eiropas Parlamenta un Padomes Regula (ES) Nr. XXX/2018.

2. Valde pieņem īstenošanas pasākumus, kas minēti Regulas (ES) Nr. xxx/2018 xx. panta 3. punktā. Valde var pieņemt papildu pasākumus, kas Kompetenču centram nepieciešami Regulas (ES) Nr. xxx/2018 piemērošanai.

44. pants

Mītnes dalībvalsts atbalsts

Kompetenču centrs un dalībvalsts [Beļģija], kurā atrodas tā mītne, var noslēgt administratīvu vienošanos par privilēģijām un imunitāti, kā arī par citu atbalstu, ko šī dalībvalsts sniedz Kompetenču centram.

VII NODAĻA

NOBEIGUMA NOTEIKUMI

45. pants

Sākotnējās darbības

1. Komisija uzņemas atbildību par Kompetenču centra izveidi un darbības sākumu, līdz tas ir pietiekami darbotiesspējīgs, lai pats izpildītu savu budžetu. Komisija saskaņā ar Savienības tiesību aktiem veic visas nepieciešamās darbības, Kompetenču centra darbā iesaistot kompetentās struktūras.
2. Panta 1. punkta nolūkā līdz brīdim, kad izpilddirektors sāk pildīt savus pienākumus pēc tam, kad Valde ir iecēlusi viņu amatā saskaņā ar 16. pantu, Komisija var iecelt pagaidu izpilddirektoru un pildīt izpilddirektoram noteiktos pienākumus, un ierobežotā skaitā viņam var palīdzēt Komisijas ierēdņi. Komisija var norīkot ierobežotu skaitu pagaidu ierēdņu.
3. Pagaidu izpilddirektors var atļaut maksājumus, ko sedz no apropriācijām, kuras paredzētas Kompetenču centra gada budžetā, kad Valde to apstiprinājusi, kā arī slēgt nolīgumus, lēmumus un līgumus, ieskaitot darba līgumus pēc Kompetenču centra štatu saraksta pieņemšanas.
4. Pagaidu izpilddirektors, vienojies ar Kompetenču centra izpilddirektoru un saņēmis Valdes apstiprinājumu, nosaka datumu, kurā Kompetenču centrs spēs izpildīt savu budžetu. No minētā datuma Komisija neuzņemas saistības un neveic maksājumus saistībā ar Kompetenču centra pasākumiem.

46. pants

Ilgums

1. Kompetenču centru izveido laikposmam no 2021. gada 1. janvāra līdz 2029. gada 31. decembrim.
2. Šī perioda beigās, ja vien, pārskatot šo regulu, nav nolemts citādi, tiek uzsākta likvidācijas procedūra. Likvidācijas procedūra tiek uzsākta automātiski, ja Savienība vai visas iesaistītās dalībvalstis izstājas no Kompetenču centra.

3. Lai īstenotu Kompetenču centra likvidācijas procedūru, Valde ieceļ vienu vai vairākus likvidatorus, kas izpilda Valdes lēmumus.

4. Likvidējot Kompetenču centru, tā aktīvus izmanto, lai segtu centra saistības un izdevumus, kas saistīti ar tā likvidāciju. Jebkurš pārpalikums tiek sadalīts starp Savienību un iesaistītajām dalībvalstīm proporcionāli to finansiālajam ieguldījumam Kompetenču centrā. Jebkādu šādu Savienībai atdotu pārpalikumu atgriež Savienības budžetā.

47. pants

Stāšanās spēkā

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

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

Briselē,

Eiropas Parlamenta vārdā	*Padomes vārdā*
Priekšsēdētājs	*Priekšsēdētājs*

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

1.2. Attiecīgā(-ās) politikas joma(-as) ABM/ABB struktūrā

1.3. Priekšlikuma/iniciatīvas būtība

1.4. Mērķis(-ķi)

1.5. Priekšlikuma/iniciatīvas pamatojums

1.6. Ilgums un finansiālā ietekme

1.7. Paredzētais(-ie) pārvaldības veids(-di)

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

2.2. Pārvaldības un kontroles sistēma

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Attiecīgās daudzgadu finanšu shēmas izdevumu kategorija(-as) un budžeta izdevumu pozīcija(-as)

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

3.2.2. Paredzamā ietekme uz darbības apropriācijām

3.2.3. Paredzamā ietekme uz administratīvajām apropriācijām

3.2.4. Saderība ar kārtējo daudzgadu finanšu shēmu

3.2.5. Trešo personu iemaksas

3.3. Paredzamā ietekme uz ieņēmumiem

TIESĪBU AKTA PRIEKŠLIKUMA FINANŠU PĀRSKATS

1. PRIEKŠLIKUMA/INICIATĪVAS KONTEKSTS

1.1. Priekšlikuma/iniciatīvas nosaukums

Regula, ar ko izveido Eiropas Industriālo, tehnoloģisko un pētniecisko kiberdrošības kompetenču centru

1.2. Attiecīgā(-ās) politikas joma(-as) *ABM/ABB* struktūrā[35]

Zinātniskā izpēte un inovācija

Eiropas stratēģiskās investīcijas

1.3. Priekšlikuma/iniciatīvas būtība

☒ Priekšlikums/iniciatīva attiecas uz **jaunu darbību**

☐ Priekšlikums/iniciatīva attiecas uz **jaunu darbību, pamatojoties uz izmēģinājuma projektu / sagatavošanas darbību**[36]

☐ Priekšlikums/iniciatīva attiecas uz **esošas darbības pagarināšanu**

☐ Priekšlikums/iniciatīva attiecas uz **darbību, kas pārveidota jaunā darbībā**

1.4. Mērķis(-ķi)

1.4.1. Komisijas daudzgadu stratēģiskie mērķi, kurus plānots sasniegt ar priekšlikumu/iniciatīvu

1. Savienots digitālais vienotais tirgus

2. Jauns impulss nodarbinātībai, izaugsmei un ieguldījumiem

1.4.2. Attiecīgais(-ie) konkrētais(-ie) mērķis(-ķi)

Konkrētie mērķi

1.3. Digitālā ekonomika var pilnībā izmantot savu attīstības potenciālu, balstoties uz iniciatīvām, kas ļauj pilnībā attīstīt digitālās un datu tehnoloģijas.

2.1. Eiropa saglabā savu pasaules līdera pozīciju digitālajā ekonomikā, kurā Eiropas uzņēmumi var augt globālā mērogā, izmantojot spēcīgu digitālo uzņēmējdarbību un jaunuzņēmumu izveidi, un kur industrijas un sabiedrisko pakalpojumu pārstāvji prasmīgi īsteno digitalizāciju.

2.2. Eiropas pētniecība atklāj investīciju iespējas potenciāliem tehnoloģiskiem atklājumiem un vadošiem virzieniem, jo īpaši pamatprogrammās "Apvārsnis 2020" / "Apvārsnis Eiropa", kā arī izmantojot publiskā un privātā sektora partnerības.

[35] ABM: budžeta līdzekļu vadība pa darbības jomām; ABB: budžeta līdzekļu sadale pa darbības jomām.

[36] Kā paredzēts Finanšu regulas 54. panta 2. punkta a) vai b) apakšpunktā.

1.4.3. Paredzamais(-ie) rezultāts(-ti) un ietekme

Norādīt, kāda ir priekšlikuma/iniciatīvas iecerētā ietekme uz finansējuma saņēmējiem/mērķgrupām.

Kompetenču centrs sadarbībā ar Tīklu un Kopienu centīsies sasniegt šādus mērķus:

1) palīdzēt īstenot kiberdrošības darbības, kas paredzētas ar Regulu Nr. XXX izveidotajā Digitālās Eiropas programmā un jo īpaši minētās regulas 6. pantā, ar Regulu Nr. XXX izveidotajā pamatprogrammā "Apvārsnis Eiropa" un jo īpaši I pielikuma 2.2.6. iedaļā Lēmumā Nr. XXX, ar ko izveido īpašo programmu, ar kuru īsteno pētniecības un inovācijas pamatprogrammu "Apvārsnis Eiropa", kā arī citās Savienības programmās, ja tas paredzēts Savienības tiesību aktos.

2) uzlabot industriju, publiskā sektora un pētniecības kopienu rīcībā esošās kiberdrošības spējas, zināšanas un infrastruktūru

3) sekmēt jaunāko kiberdrošības produktu un risinājumu plašu ieviešanu visā ekonomikā,

4) uzlabot izpratni par kiberdrošību un palīdzēt mazināt prasmju trūkumu Savienībā saistībā ar kiberdrošību,

5) palīdzēt nostiprināt kiberdrošības pētniecību un izstrādi Savienībā,

6) uzlabot sadarbību starp civilo un aizsardzības jomu attiecībā uz divējāda lietojuma tehnoloģijām un to pielietošanu,

7) uzlabot sinerģijas starp kiberdrošības civilajām un aizsardzības dimensijām,

8) veicināt 10. pantā minētā Nacionālo koordinācijas centru tīkla (turpmāk "Tīkls") un 12. pantā minētās kiberdrošības kompetenču kopienas darbu un palīdzēt to koordinēt.

1.4.4. Rezultātu un ietekmes rādītāji

Norādīt priekšlikuma / iniciatīvas īstenošanas uzraudzībā izmantojamos rādītājus.

· Kopīgi iepirktās kiberdrošības infrastruktūras/rīku skaits.

· Testēšanas un eksperimentālo objektu izmantošanas laiks Eiropas pētniekiem un industrijai visa Tīkla un Kompetenču centra ietvaros. Gadījumos, kad šāds tehniskais nodrošinājums jau ir, šīm kopienām pieejamo stundu skaita palielinājums salīdzinājumā ar pašlaik pieejamām stundām.

· Apkalpoto lietotāju kopienu skaits un to pētnieku skaits, kuri piekļūst Eiropas kiberdrošības tehniskajam nodrošinājumam, palielinās, salīdzinot ar to cilvēku skaitu, kuriem šādi resursi jāmeklē ārpus Eiropas.

· Eiropas piegādātāju konkurētspēja sāk pieaugt, izsakot to kā pasaules tirgus daļu (25 % mērķa tirgus daļa tiks sasniegta līdz 2027. gadam), kā arī industrijas pārņemto Eiropas pētniecības un izstrādes rezultātu daļu.

· Ieguldījums nākamajās kiberdrošības tehnoloģijās, ko mēra autortiesībās, patentos, zinātniskās publikācijās un komerciālos produktos.

· Novērtēto un saskaņoto kiberdrošības prasmju mācību programmu skaits, novērtēto kiberdrošības profesionālās sertifikācijas programmu skaits;

· Apmācīto zinātnieku, studentu, lietotāju (industrijā un publiskās pārvaldes nozarēs) skaits.

1.5. Priekšlikuma/iniciatīvas pamatojums

1.5.1. Īstermiņa vai ilgtermiņa vajadzība(-as)

Sasniegt investīciju apjoma kritisko masu kiberdrošības tehnoloģiskajā un industriālajā attīstībā un pārvarēt attiecīgo spēju sadrumstalotību visā ES.

1.5.2. ES iesaistīšanās pievienotā vērtība

Kiberdrošība ir jautājums, kas skar Savienības kopējās intereses, kā to apstiprina iepriekšminētie Padomes secinājumi. Tam vērā ņemams piemērs ir tādu kiberincidentu kā *WannaCry* vai *NonPetya* mērogs un to pārrobežu raksturs. Kiberdrošības tehnoloģisko problēmu raksturs un mērogs, kā arī nepietiekami koordinēti centieni industrijas, publiskā sektora un pētniecības kopienu ietvaros un starp tām rada nepieciešamību ES turpināt koordinācijas pasākumu atbalstīšanu, lai apvienotu resursu kritisko masu un nodrošinātu labāku zināšanu, kā arī aktīvu pārvaldību. Tas ir nepieciešams, lai panāktu atbilstību resursu prasībām, kas saistītas ar noteiktām kiberdrošības izpētes, izstrādes un plašākas ieviešanas spējām; vajadzība nodrošināt piekļuvi starpdisciplinārai zinātībai kiberdrošības jautājumos dažādās jomās (kas bieži vien valsts līmenī ir tikai daļēji pieejama); industriālo vērtību ķēžu globālais raksturs, kā arī globālo konkurentu darbība visos tirgos

Tam ir nepieciešami resursi un lietpratība tādā apjomā, ko tikai ar grūtībām spētu nodrošināt kādas dalībvalsts atsevišķa rīcība. Piemēram, Eiropas mēroga kvantu sakaru tīkls varētu prasīt ES ieguldījumu 900 miljonu EUR apmērā atkarībā no dalībvalstu ieguldījumiem (kas būtu savstarpēji saistīti/papildinoši) un tā, cik lielā mērā šo tehnoloģiju būtu iespējams izmantot esošo infrastruktūru ietvaros.

1.5.3. Līdzīgas līdzšinējās pieredzes rezultātā gūtās atziņas

Pamatprogrammas "Apvārsnis 2020" starpposma izvērtējumā cita starpā tika apstiprināts, ka ES atbalsts pētniecībai un izstrādei, kā arī sabiedrības problēmjautājumu (tostarp ieguldījums jomā "Drošas sabiedrībās", ar kuru tiek atbalstīta kiberdrošības pētniecība un izstrāde) risināšanai joprojām ir būtisks. Vienlaikus izvērtējums apstiprina, ka vadošās lomas pastiprināšana industrijā joprojām ir problemātiska, kā arī to, ka joprojām pastāv inovāciju trūkums, ES atpaliekot no tirgus radošā inovāciju izrāviena.

Eiropas infrastruktūras savienošanas instrumenta (EISI) vidusposma izvērtējums šķietami apstiprina ES intervences pievienoto vērtību papildus pētniecībai un izstrādei, lai arī kiberdrošība saskaņā ar EISI bija vērsta nedaudz citādā (darbības drošības) virzienā un tai bija nedaudz citāda intervences loģika. Tajā pašā laikā lielākā daļa EISI kiberdrošības dotāciju saņēmēju — valstu datordrošības incidentu reaģēšanas vienību (CSIRT) kopienu — izteica vēlēšanos pēc konkrētas atbalsta programmas nākamajā daudzgadu finanšu shēmā.

ES līgumiskās publiskā un privātā sektora partnerības (*cPPP*) izveide kiberdrošības jomā 2016. gadā bija stabils pirmais solis industrijas, pētniecības un publiskā sektora kopienu apvienošanā, lai veicinātu pētniecību un inovāciju kiberdrošības jomā, un 2014.–2020. gada finanšu shēmas robežās tai būtu jāsniedz labus, koncentrētākus pētniecības un inovācijas rezultātus. Savienības kiberdrošības publiskā un privātā sektora partnerības izveide deva iespēju industriju partneriem paust apņemšanos par saviem individuālajiem izdevumiem jomās, kas noteiktas partnerības stratēģiskās pētniecības un inovācijas programmā.

1.5.4. Saderība un iespējamā sinerģija ar citiem atbilstošiem instrumentiem

Kiberdrošības kompetenču tīkls un Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs darbosies kā papildu atbalsts esošajiem kiberdrošības politikas noteikumiem un dalībniekiem. Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra pilnvarojums papildinās *ENISA* centienus, taču tā uzmanība ir vērsta uz atšķirīgiem mērķiem un pieprasa savādāku prasmju kopumu. Lai arī *ENISA* ir svarīga konsultatīva loma ES kiberdrošības pētniecības un inovācijas jomā, tās piedāvātais pilnvaru paplašinājums galvenokārt ir vērsts uz citiem būtiskiem uzdevumiem ES kiberdrošības noturības pastiprināšanai. Kompetenču centram būtu jāstimulē tehnoloģiju izstrāde un plašāka ieviešana kiberdrošības jomā, kā arī jāpapildina šīs jomas spēju veidošanas centieni ES un valstu līmenī.

Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs kopā ar Kiberdrošības kompetenču tīklu strādās arī pētniecības atbalsta nolūkā, lai atvieglotu un paātrinātu standartizācijas un sertifikācijas procesus, jo īpaši tos, kas saistīti ar kiberdrošības sertifikācijas shēmām Kiberdrošības akta izpratnē.

Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs darbosies kā vienots izpildmehānisms divām Eiropas programmām, kas atbalsta kiberdrošību (Digitālās Eiropas programma, "Apvārsnis Eiropa") un uzlabos saskaņotību un sinerģijas starp programmām.

Šī iniciatīva ļauj papildināt dalībvalstu centienus, nodrošinot atbilstošu ieguldījumu izglītības politikas veidošanā, lai uzlabotu izglītību kiberdrošības jomā (piemēram, izstrādājot kiberdrošības mācību programmas civilajās un militārajās izglītības sistēmās, taču sniedzot arī ieguldījumu pamatizglītībā kiberdrošības jomā). Tā ļautu arī atbalstīt profesionālo kiberdrošības sertifikācijas programmu saskaņošanu un nepārtrauktu novērtēšanu, īstenojot visus nepieciešamos pasākumus, lai palīdzētu novērst kiberdrošības prasmju trūkumu un atvieglotu industriju un citu kopienu piekļuvi kiberdrošības speciālistiem. Izglītības prasību un prasmju saskaņošana palīdzēs veidot kvalificētu darbaspēku ES kiberdrošības jomā — tā ir nozīmīga vērtība ne vien kiberdrošības uzņēmumiem, bet arī citām ar kiberdrošību saistītām industrijām.

1.6. Ilgums un finansiālā ietekme

☒ **Ierobežota ilguma** priekšlikums/iniciatīva

– ☒ Priekšlikuma/iniciatīvas darbības laiks: 1.1.2021.–31.12.2029.

– ☒ Finansiālā ietekme uz saistību apropriācijām no 2021. līdz 2027. gadam un uz maksājumu apropriācijām no 2021. līdz 2031. gadam.

☐ **Beztermiņa** priekšlikums/iniciatīva

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

– pēc kura turpinās normāla darbība.

1.7. Paredzētais(-ie) pārvaldības veids(-di)[37]

☐ Komisijas īstenota **tieša pārvaldība**

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

– ☐ ko veic izpildaģentūras.

☐ **Dalīta pārvaldība** kopā ar dalībvalstīm

☒

Netieša pārvaldība, kurā budžeta īstenošanas uzdevumi uzticēti:

– ☐ trešām valstīm vai to noteiktām 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 valsts pārvaldes uzdevumus, ja tie sniedz pienācīgas finanšu garantijas;

– ☐ struktūrām, kuru darbību reglamentē dalībvalsts privāttiesības, kurām ir uzticēta publiskā un privātā sektora partnerības īstenošana un kuras sniedz pienācīgas finanšu garantijas;

– ☐ personām, kurām ir uzticēts veikt īpašas darbības KĀDP saskaņā ar Līguma par Eiropas Savienību V sadaļu un kuras ir noteiktas attiecīgā pamataktā.

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

[37] Skaidrojumus par pārvaldības veidiem un atsauces uz Finanšu regulu skatīt *BudgWeb* tīmekļa vietnē: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

2. PĀRVALDĪBAS PASĀKUMI

2.1. Uzraudzības un ziņošanas noteikumi

Norādīt periodiskumu un nosacījumus.

28. pantā ir detalizēti izklāstīti uzraudzības un ziņošanas noteikumi.

2.2. Pārvaldības un kontroles sistēma

2.2.1. Apzinātie riski

Lai mazinātu riskus, kas saistīti ar Kompetenču centra darbību pēc tā izveidošanas un kavējumiem, Komisija šajā posmā Kompetenču centram sniegs atbalstu, lai nodrošinātu ātru svarīgākā personāla pieņemšanu darbā, kā arī efektīvas iekšējās kontroles sistēmas un pareizu procedūru ieviešanu.

2.2.2. Informācija par izveidoto iekšējās kontroles sistēmu

Izpilddirektors ir atbildīgs par Kompetenču centra darbību un ikdienas pārvaldību, kā arī ir tā likumīgais pārstāvis. Direktors ir pakļauts Valdei un pastāvīgi ziņo tai par Kompetenču centra darbības attīstību.

Valdei ir vispārēja atbildība par Kompetenču centra stratēģisko virzību un darbību, un Valde uzrauga tā pasākumu īstenošanu.

Kompetenču centram piemērojamos finanšu noteikumus pieņem Valde pēc apspriešanās ar Komisiju. Tie neatkāpjas no Regulas (ES) Nr. 1271/2013, ja vien atkāpšanās nav īpaši nepieciešama Kompetenču centra darbībai un Komisija iepriekš nav devusi piekrišanu.

Komisijas iekšējam revidentam Kompetenču centrā jābūt tādām pašām pilnvarām, kādas tam ir Komisijā. Revīzijas palātai ir tiesības, pārbaudot dokumentus un veicot pārbaudes uz vietas, revidēt visus dotāciju saņēmējus, līgumslēdzējus un apakšuzņēmējus, kuri no Kompetenču centra ir saņēmuši Savienības līdzekļus.

2.2.3. Paredzamās pārbaužu izmaksas un ieguvumi un gaidāmā kļūdas riska līmeņa novērtējums

Kontroles izmaksas un ieguvumi

Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra kontroles izmaksas ir sadalītas starp pārraudzības izmaksām Komisijas līmenī un izmaksu operatīvajām pārbaudēm īstenošanas struktūras līmenī.

Pārbaužu izmaksas Kompetenču centra līmenī tiek lēstas aptuveni 1,19 % apmērā no darbības maksājumu apropriācijām, kas ieviestas Kompetenču centra līmenī.

Pārraudzības izmaksas Komisijas līmenī tiek lēstas 1,20 % apmērā no darbības maksājumu apropriācijām, kas ieviestas Kompetenču centra līmenī.

Pieņemot, ka Komisija pasākumus pilnībā pārvaldīs bez īstenošanas struktūras atbalsta, kontroles izmaksas būtu ievērojami augstākas un varētu sasniegt aptuveni 7,7 % no maksājumu apropriācijām.

Paredzēto kontroles pasākumu mērķis ir nodrošināt Komisijas netraucētu un efektīvu pārraudzību attiecībā uz īstenošanas subjektiem un nodrošināt vajadzīgo ticamības pakāpi Komisijas līmenī.

Kontrolei ir šādi ieguvumi:

- Netiek pieļauts, ka tiek atlasīti vājāki vai neatbilstīgi priekšlikumi;
- Tiek optimizēta ES līdzekļu plānošana un izmantošana, lai saglabātu ES pievienoto vērtību;
- Tiek nodrošināta dotācijas līgumu kvalitāte, izvairoties no kļūdām tiesību subjektu identificēšanā, nodrošinot ES iemaksu pareizu aprēķināšanu un piemērojot vajadzīgās garantijas dotāciju pareizai funkcionēšanai;
- Neattiecināmas izmaksas tiek atklātas maksājumu veikšanas posmā;
- Kļūdas, kas skar darbību likumību un pareizību, tiek atklātas revīzijas posmā.

Aplēstais kļūdu līmenis

Mērķis ir saglabāt atlikušo kļūdu līmeni zem 2 % sliekšņa visā programmas laikā, vienlaikus ierobežojot kontroles slogu atbalsta saņēmējiem, lai panāktu pareizu līdzsvaru starp likumības un pareizības mērķi un citiem mērķiem, piemēram, veicinātu programmas pievilcīgumu, jo īpaši MVU skatījumā, un kontroles izmaksām.

2.3. Krāpšanas un pārkāpumu novēršanas pasākumi

Norādīt esošos vai plānotos novēršanas pasākumus un citus pretpasākumus.

OLAF var veikt izmeklēšanu, tostarp pārbaudes un inspekcijas uz vietas, saskaņā ar noteikumiem un procedūrām, kas noteiktas Eiropas Parlamenta un Padomes Regulā Nr. 883/2013 un Padomes 1996. gada 11. novembra Regulā (*Euratom*, EK) Nr. 2185/9640 par pārbaudēm un apskatēm uz vietas, ko Komisija veic, lai aizsargātu Savienības finanšu intereses pret krāpšanu un citām nelikumībām, lai noteiktu, vai nav notikusi krāpšana, korupcija vai kādas citas nelikumīgas darbības, kas ietekmē Savienības finansiālās intereses, kuras saistītas ar Kompetenču centra finansētu dotāciju vai līgumu.

Nolīgumos, lēmumos un līgumos, kas izriet no šīs regulas īstenošanas, ietver noteikumus, kas nepārprotami pilnvaro Komisiju, Kompetenču centru, Revīzijas palātu un *OLAF* veikt revīzijas un izmeklēšanu saskaņā ar to attiecīgajām kompetencēm.

Veicot vai pasūtot atbilstīgus iekšējas un ārējas kontroles pasākumus, Kompetenču centrs gādā par tā locekļu finansiālo interešu pienācīgu aizsardzību.

Kompetenču centrs pievienojas Iestāžu nolīgumam (1999. gada 25. maijs) starp Eiropas Parlamentu, Eiropas Savienības Padomi un Eiropas Kopienu Komisiju par iekšējo izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*). Kompetenču centrs pieņem vajadzīgos pasākumus, kas *OLAF* atvieglo iekšējās izmeklēšanas.

Kompetenču centrs pieņems stratēģiju krāpšanas apkarošanai, pamatojoties uz krāpšanas riska analīzi, kā arī izmaksu un ieguvumu apsvērumiem. Tas aizsargā Savienības finansiālās intereses, piemērojot profilaktiskus pasākumus pret krāpšanu, korupciju un citām nelikumīgām darbībām, veicot efektīvas pārbaudes un, ja ir atklāti pārkāpumi, atgūstot nepamatoti izmaksātas summas un attiecīgos gadījumos

piemērojot iedarbīgas, samērīgas un atturošas administratīvas un finansiālas sankcijas.

3. PRIEKŠLIKUMA/INICIATĪVAS PAREDZAMĀ FINANSIĀLĀ IETEKME

3.1. Daudzgadu finanšu shēmas izdevumu kategorija un jauna(-as) ierosinātā(-ās) budžeta izdevumu pozīcija(-as)

- No jauna veidojamās budžeta pozīcijas

  Sarindotas pa daudzgadu finanšu shēmas izdevumu kategorijām un budžeta pozīcijām:

Daudzgadu finanšu shēmas izdevumu kategorija	Budžeta pozīcija	Izdevumu veids	Iemaksas			
	Numurs	Dif./nedif. [38]	no EBTA valstīm [39]	no kandidātvalstīm [40]	no trešām valstīm	Finanšu regulas [21. panta 2. punkta b) apakšpunkta] nozīmē
1. pozīcija: vienotais tirgus, inovācijas un digitālā joma	01 02 XX XX "Apvārsnis Eiropa", Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs — atbalsta izdevumi 01 02 XX XX "Apvārsnis Eiropa", Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs 02 06 01 XX Digitālās Eiropas programma, Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs — atbalsta izdevumi 02 06 01 XX Digitālās Eiropas programma, Eiropas Industriālais, tehnoloģiskais un pētnieciskais kiberdrošības kompetenču centrs	Dif.	JĀ	JĀ (ja norādīts gada darba programmā)	JĀ (attiecas tikai uz programmas daļām)	NĒ

[38] Dif. = diferencētās apropriācijas / nedif. = nediferencētās apropriācijas.

[39] EBTA: Eiropas Brīvās tirdzniecības asociācija.

[40] Kandidātvalstis un attiecīgā gadījumā potenciālās kandidātvalstis no Rietumbalkāniem.

- Ieguldījums šajās budžeta pozīcijās ir gaidāms no:

miljonos EUR (trīs zīmes aiz komata)

Budžeta pozīcija	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.	**Kopā**
01 01 01 01 Izdevumi, kas saistīti ar pētniecības ierēdņu pagaidu pārstāvjiem — "Apvārsnis Eiropa"	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Ārējais personāls, kas īsteno pētniecības programmas — "Apvārsnis Eiropa"	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Citi pētniecības pārvaldības izdevumi — "Apvārsnis Eiropa"	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globālās problēmas un industriālā konkurētspēja	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 administratīvais atbalsts — Digitālās Eiropas programma	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Kiberdrošība — Digitālās Eiropas programma	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1957,922**
Kopējie izdevumi	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1981,668**

Ieguldījuma apmēru no 21. panta 1. punkta b) apakšpunktā minētās "Apvārsnis Eiropa" pamatprogrammas otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma Komisija ierosinās likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas. Priekšlikuma pamatā būs stratēģiskās plānošanas procesa rezultāts, kā noteikts Regulas XXX [pamatprogramma "Apvārsnis Eiropa"] 6. panta 6. punktā.

Augstākminētās summas neietver Savienības finansiālajam ieguldījumam atbilstošu dalībvalstu ieguldījumu Kompetenču centra darbības un administratīvo izmaksu segšanai.

3.2. Paredzamā ietekme uz izdevumiem

3.2.1. Kopsavilkums par paredzamo ietekmi uz izdevumiem

miljonos EUR (trīs zīmes aiz komata)

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

			2021. g.[41]	**2022. g.**	**2023. g.**	**2024. g.**	**2025. g.**	**2026. g.**	**2027. g.**	***Pēc 2027. gada***	**KOPĀ**
1. sadaļa (personāla izdevumi)	Saistības = maksājumi	1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
2. sadaļa (infrastruktūras un darbības izdevumi)	Saistības = maksājumi	2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
3. sadaļa (darbības izdevumi)	Saistības	3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1957,922**
	Maksājumi	4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1061,715	**1957,922**
KOPĒJĀS programmu finansējuma apropriācijas[42]	Saistības	= 1 + 2 + 3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1981,668**
	Maksājumi	= 1 + 2 + 4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1061,715**	**1981,668**

41 2021. gadā personāla apropriācijas ir uzskaitītas tikai par pusgadu.

42 Kopējās noteiktās apropriācijas attiecas tikai uz ES finanšu resursiem, kas atvēlēti kiberdrošības jomai Digitālās Eiropas programmas ietvaros. Ieguldījuma apmēru no 5. panta 1. punkta b) apakšpunktā minētās pamatprogrammas "Apvārsnis Eiropa" otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma Komisija ierosinās likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas. Priekšlikuma pamatā būs stratēģiskās plānošanas procesa rezultāts, kā noteikts Regulas XXX [pamatprogramma "Apvārsnis Eiropa"] 6. panta 6. punktā.

Daudzgadu finanšu shēmas izdevumu kategorija	7.	"Administratīvie izdevumi"

miljonos EUR (trīs zīmes aiz komata)

		2021. g.	**2022. g.**	**2023. g.**	**2024. g.**	**2025. g.**	**2026. g.**	**2027. g.**	***Pēc 2027. g ada***	**KOPĀ**
Cilvēkresursi		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Pārējie administratīvie izdevumi		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
KOPĒJĀS daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS apropriācijas	(Saistību summa = maksājumu summa)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

miljonos EUR (trīs zīmes aiz komata)

		2021. g.	**2022. g.**	**2023. g.**	**2024. g.**	**2025. g.**	**2026. g.**	**2027. g.**	***Pēc 2027. g ada***	**KOPĀ**
Visu KATEGORIJU KOPĒJĀS apropriācijas daudzgadu finanšu shēmā	Saistības	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2005,637**
	Maksājumi	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1²061,715**	**2005,637**

3.2.2. Kopsavilkums par paredzamo ietekmi uz administratīvajām apropriācijām

– ☐ Priekšlikums/iniciatīva neparedz izmantot administratīvās apropriācijas

– ☒ Priekšlikums/iniciatīva paredz izmantot administratīvās apropriācijas šādā veidā:

miljonos EUR (trīs zīmes aiz komata)

Gads	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.	KOPĀ
7. IZDEVUMU KATEGORIJA daudzgadu finanšu shēmā								
Cilvēkresursi	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Pārējie administratīvie izdevumi	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
7. IZDEVUMU KATEGORIJAS starpsumma daudzgadu finanšu shēmā	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**
Ārpus 7. IZDEVUMU KATEGORIJAS[43] daudzgadu finanšu shēmā								
Cilvēkresursi								
Citi administratīva veida izdevumi	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Starpsumma Ārpus 7. IZDEVUMU KATEGORIJAS daudzgadu finanšu shēmā	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**
KOPĀ	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

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

Augstākminētās cilvēkresursiem un citiem administratīvajiem izdevumiem nepieciešamās apropriācijas ārpus 7. izdevumu kategorijas atbilst summām, kuras sedz Savienības finansiālais ieguldījums no Digitālās Eiropas programmas.

Apropriācijas cilvēkresursiem un citiem administratīvajiem izdevumiem ārpus 7. izdevumu kategorijas tiks palielinātas par summām, kuras segs Savienības finansiālais ieguldījums no pamatprogrammas "Apvārsnis Eiropa", tiklīdz Komisija likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas ierosinās ieguldījuma apmēru no

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

21. panta 1. punkta b) apakšpunktā minētās pamatprogrammas "Apvārsnis Eiropa" otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma.

Augstākminētās cilvēkresursiem un citiem administratīvajiem izdevumiem nepieciešamās apropriācijas ārpus 7. izdevumu kategorijas neietver Savienības finansiālajam ieguldījumam atbilstošu dalībvalstu ieguldījumu Kompetenču centra darbības un administratīvo izmaksu segšanai.

3.2.2.1. Komisijas paredzamās cilvēkresursu vajadzības

– ☐ Priekšlikums/iniciatīva neparedz cilvēkresursu izmantošanu.

– ■ Priekšlikums/iniciatīva paredz cilvēkresursu izmantošanu šādā veidā:

Aplēse izsakāma pilnslodzes ekvivalentos

Gads		2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.
• Štatu sarakstā ietvertās amata vietas (ierēdņi un pagaidu darbinieki)								
Galvenajā mītnē un Komisijas pārstāvniecībās		20	21	21	21	21	21	22
Delegācijās								
Pētniecībā								
• Ārštata darbinieki (izsakot pilnslodzes ekvivalentos) — AC, AL, END, INT un JED [44] 7. izdevumu kategorija								
Finansēta no daudzgadu finanšu shēmas 7. IZDEVUMU KATEGORIJAS	- galvenajā mītnē	3	3	3	3	3	3	3
	- delegācijās							
Finansēts no programmas piešķīruma [45]	- galvenajā mītnē							
	- delegācijās							
Pētniecībā								
Citur (norādīt)								
KOPĀ		**23**	**23**	**24**	**24**	**24**	**25**	**25**

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

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki	Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram uzticēto uzdevumu koordinēšana, uzraudzība un vadība, ieskaitot atbalsta un koordinācijas izmaksas. Politikas izstrāde un koordinācija kiberdrošības jomā saistībā ar uzdevumiem, kas uzticēti Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram, piemēram, attiecībā uz pētniecības un industriālās politikas prioritāšu noteikšanu, vispārēju dalībvalstu un uzņēmēju sadarbību, saskaņotību ar turpmāko ES kiberdrošības sertifikācijas sistēmu, darbu saistībā ar atbildību un pienākumu ņemt vērā ierēdņu intereses, kā arī politikas koordinēšanu attiecībā uz *HPC*, mākslīgo intelektu un digitālajām prasmēm. .
Ārštata darbinieki	Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram uzticēto uzdevumu koordinēšana, uzraudzība un vadība, ieskaitot atbalsta un

[44] AC = līgumdarbinieki; AL = vietējie darbinieki; END = norīkotie valsts eksperti; INT = aģentūras darbinieki; JED = jaunākie eksperti delegācijās.

[45] Ārštata darbiniekiem paredzētā maksimālā summa, ko finansē no darbības apropriācijām (kādreizējām "BA" pozīcijām).

	koordinācijas izmaksas. Politikas izstrāde un koordinācija kiberdrošības jomā saistībā ar uzdevumiem, kas uzticēti Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram, piemēram, attiecībā uz pētniecības un industriālās politikas prioritāšu noteikšanu, vispārēju dalībvalstu un uzņēmēju sadarbību, saskaņotību ar turpmāko ES kiberdrošības sertifikācijas sistēmu, darbu saistībā ar atbildību un pienākumu ņemt vērā ierēdņu intereses, kā arī politikas koordinēšanu attiecībā uz *HPC*, mākslīgo intelektu un digitālajām prasmēm. .

3.2.2.2. Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra paredzamās cilvēkresursu vajadzības

	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.
Komisijas pārstāvji							
No kuriem AD							
No kuriem AST							
No kuriem AST-SC							
Pagaidu darbinieki							
No kuriem AD	10	11	13	13	13	13	13
No kuriem AST							
No kuriem AST-SC							
Līgumdarbinieki	26	32	39	39	39	39	39
Norīkotie valsts eksperti	1	1	1	1	1	1	1
Kopā	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Veicamo uzdevumu apraksts:

Ierēdņi un pagaidu darbinieki	Uzdevumi, kas saskaņā ar šīs regulas 4. pantu uzticēti Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram, ieskaitot atbalstu un koordinācijas izmaksas.
Ārštata darbinieki	Uzdevumi, kas saskaņā ar šīs regulas 4. pantu uzticēti Eiropas Industriālajam, tehnoloģiskajam un pētnieciskajam kiberdrošības kompetenču centram, ieskaitot atbalstu un koordinācijas izmaksas.

Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra augstāk aplēstās paredzamās cilvēkresursu vajadzības atbilst aplēstajām prasībām, lai īstenotu Savienības finansiālo ieguldījumu Digitālās Eiropas programmā.

Augstāk aplēstās Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra cilvēkresursu prasības tiks palielinātas, ņemot vērā paredzamās prasības, lai īstenotu Savienības finanšu ieguldījumu pamatprogrammā "Apvārsnis Eiropa", tiklīdz Komisija likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas ierosinās ieguldījuma apmēru no 21. panta 1. punkta b) apakšpunktā minētās pamatprogrammas "Apvārsnis Eiropa" otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma.

3.2.2.3. Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra štatu saraksts

Funkciju grupa un pakāpe	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2025. g.	2025. g.
AD 16							

AD 15							
AD 14	1	1	1	1	1	1	1
AD 13							
AD 12							
AD 11							
AD 10							
AD 9	5	5	6	6	6	6	6
AD 8	1	1	1	1	1	1	1
AD 7	1	2	3	3	3	3	3
AD 6	1	1	1	1	1	1	1
AD 5	1	1	1	1	1	1	1
AD kopā	10	11	13	13	13	13	13
AST 11							
AST 10							
AST 9							
AST 8							
AST 7							
AST 6							
AST 5							
AST 4							
AST 3							
AST 2							
AST 1							
AST kopā							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							

AST/SC 2							
AST/SC 1							
AST/SC kopā							
PAVISAM KOPĀ	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4. Paredzamā (papildu) ietekme uz personālu — Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra ārštata darbinieki

Līgumdarbinieki	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.
IV funkciju grupa	20	22	29	29	29	29	29
III funkciju grupa	2	4	4	4	4	4	4
II funkciju grupa	4	6	6	6	6	6	6
I funkciju grupa							
Kopā	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Lai nodrošinātu darbinieku skaita neitralitāti, papildu darbinieku skaitu Eiropas Industriālajā, tehnoloģiskajā un pētnieciskajā kiberdrošības kompetenču centrā daļēji kompensēs ierēdņu un ārštata darbinieku skaita samazināšana (t. i., štatu saraksts un pašreizējais ārštata darbinieku skaits) attiecīgajos Komisijas dienestos.
Eiropas Industriālā, tehnoloģiskā un pētnieciskā kiberdrošības kompetenču centra 3.2.2.2. līdz 4. punkta darbinieku skaits tiks kompensēts šādi[46]:

KOPĀ	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.
Komisijas pārstāvji	5	5	6	6	6	6	6
Pagaidu darbinieki							
Līgumdarbinieki	14	17	20	20	20	20	20
Norīkotie valsts eksperti							
Kopējais pilnslodzes ekvivalents	19	22	26	26	26	26	26
Darbinieku skaits	19	22	26	26	26	26	26

[46] Ievērojot galīgo summu budžetā, kura īstenošana tiks deleģēta Kompetenču centram

Cilvēkresursu kompensācija Industriālajā, tehnoloģiskajā un pētnieciskajā kiberdrošības kompetenču centrā būs proporcionāla Savienības finansiālā ieguldījuma īpatsvaram, t. i., 50 %.

Augstākminētā kompensācija attiecas uz aplēstajām cilvēkresursu prasībām Industriālajā, tehnoloģiskajā un pētnieciskajā kiberdrošības kompetenču centrā, lai īstenotu Digitālās Eiropas programmas Savienības finansiālo ieguldījumu.

Augstākminētā kompensācija tiks palielināta, ņemot vērā paredzamās prasības, lai īstenotu Eiropas Savienības finansiālo ieguldījumu no pamatprogrammas "Apvārsnis Eiropa", tiklīdz Komisija likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas ierosinās ieguldījuma apmēru no 21. panta 1. punkta b) apakšpunktā minētās pamatprogrammas "Apvārsnis Eiropa" otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma.

3.2.3. Trešo personu iemaksas

Priekšlikums/iniciatīva:

– ☐ neparedz trešo personu līdzfinansējumu

– ☒ paredz trešo personu[47] līdzfinansējumu šādā veidā:

Apropriācijas miljonos EUR (trīs zīmes aiz komata)

Gads	2021. g.	2022. g.	2023. g.	2024. g.	2025. g.	2026. g.	2027. g.	KOPĀ
Dalībvalstis — ieguldījums personāla izdevumos	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Dalībvalstis — ieguldījums infrastruktūras un ekspluatācijas izdevumos	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Dalībvalstis — ieguldījums darbības izdevumos	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1957,922**
KOPĒJĀS līdzfinansētās apropriācijas	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1981,668**

Augstākminētais trešo personu ieguldījums attiecas tikai uz līdzfinansējumu, kas ir atbilstošs ES finanšu resursiem, kuri atvēlēti kiberdrošības jomai Digitālās Eiropas programmas ietvaros. Augstākminētais trešās personu ieguldījums tiks palielināts, tiklīdz Komisija likumdošanas procesa gaitā un, jebkurā gadījumā, pirms politiskas vienošanās panākšanas ierosinās ieguldījuma apmēru no 21. panta 1. punkta b) apakšpunktā minētās pamatprogrammas "Apvārsnis Eiropa" otrā pīlāra "Globālās problēmas un industriālā konkurētspēja" kopas "Iekļaujoša un droša sabiedrība" (kopējā finansējuma summa 2 800 000 000 EUR) finansējuma. Priekšlikuma pamatā būs stratēģiskās plānošanas procesa rezultāts, kā noteikts Regulas XXX [pamatprogramma "Apvārsnis Eiropa"] 6. panta 6. punktā.

3.3. Paredzamā ietekme uz ieņēmumiem

– ☒ Priekšlikums/iniciatīva finansiāli neietekmē ieņēmumus.

– ☐ Priekšlikums/iniciatīva finansiāli ietekmē:

☐ pašu resursus

☐ citus ieņēmumus

lūdzu, norādiet, ja ieņēmumi ir piešķirti izdevumu pozīcijām ☐

miljonos EUR (trīs zīmes aiz komata)

Budžeta ieņēmumu	Priekšlikuma/iniciatīvas ietekme[48]

[47] Paredzamais dalībvalstu ieguldījums natūrā

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

pozīcija:	**2021. g.**	**2022. g.**	**2023. g.**	**2024. g.**	**2025. g.**	**2026. g.**	**2027. g.**
……. pants							

Attiecībā uz piešķirtajiem ieņēmumiem norādīt attiecīgo(-ās) budžeta izdevumu pozīciju(-as).

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