EVROPSKA
KOMISIJA

Bruselj, 12.9.2018
COM(2018) 630 final

2018/0328 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov

Prispevek Evropske komisije k srečanju voditeljev v Salzburgu 19. in 20. septembra 2018

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

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Ker postajata vsakdanje življenje in gospodarstvo vse bolj odvisna od digitalnih tehnologij, so državljani vedno bolj izpostavljeni resnim kibernetskim incidentom. Varnost bo v prihodnosti odvisna od povečanja zmogljivosti Unije za zaščito pred kibernetskimi grožnjami, saj se tako civilna infrastruktura kot tudi vojaške zmogljivosti zanašajo na varne digitalne sisteme.

Da bi Unija obravnavala vse večje izzive, stopnjuje svoje dejavnosti na tem področju, pri čemer upošteva strategijo za kibernetsko varnost iz leta 2013[1] ter njene cilje in načela za spodbujanje zanesljivega, varnega in odprtega kibernetskega ekosistema. Prve ukrepe na področju kibernetske varnosti je Unija sprejela leta 2016 z Direktivo (EU) 2016/1148 Evropskega parlamenta in Sveta[2] o varnosti omrežij in informacijskih sistemov.

Zaradi hitrega razvoja področja kibernetske varnosti sta Komisija in visoka predstavnica Unije za zunanje zadeve in varnostno politiko septembra 2017 predstavili skupno sporočilo[3] z naslovom „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“, da bi se dodatno okrepili odpornost, odvračanje in odzivanje Unije na kibernetske napade. Skupno sporočilo, ki temelji tudi na prejšnjih pobudah, je predstavilo sklop predlaganih ukrepov, ki med drugim vključujejo okrepitev Agencije Evropske unije za varnost omrežij in informacij (ENISA), oblikovanje prostovoljnega vseevropskega certifikacijskega okvira za kibernetsko varnost za povečanje kibernetske varnosti izdelkov in storitev v digitalnem svetu ter načrt za hiter in usklajen odziv na obsežne kibernetske incidente in krize.

V skupnem sporočilu je bilo potrjeno, da je tudi v strateškem interesu Unije, da se ohrani in razvije pomembne ključne tehnološke zmogljivosti kibernetske varnosti za zavarovanje njenega enotnega digitalnega trga ter zlasti za zaščito kritičnih mrež in informacijskih sistemov ter zagotavljanje ključnih storitev kibernetske varnosti. Unija mora biti sposobna samostojno zavarovati svoja digitalna sredstva in konkurirati na svetovnem trgu kibernetske varnosti.

Trenutno je Unija neto uvoznica izdelkov in rešitev za kibernetsko varnost ter je v veliki meri odvisna od neevropskih ponudnikov[4]. Svetovni trg kibernetske varnosti obsega 600 milijard EUR in pričakuje se, da bo v naslednjih petih letih dosegal povprečno 17-odstotno rast v smislu prodaje, števila podjetij in zaposlovanja. Vendar pa je na vrhu lestvice 20 vodilnih držav v kibernetski varnosti z vidika trga samo 6 držav članic[5].

Hkrati obstaja v Uniji veliko strokovnega znanja in izkušenj na področju kibernetske varnosti, in sicer več kot 660 organizacij iz vse EU, zabeleženih v okviru nedavnega kartiranja centrov strokovnega znanja iz kibernetske varnosti, ki ga je izvedla Komisija[6]. Če bi se to strokovno

---

1 SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU IN SVETU Strategija Evropske unije za kibernetsko varnost: Odprt, varen in zanesljiv kibernetski prostor, JOIN(2013) 1 final.

2 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

3 SKUPNO SPOROČILO EVROPSKEMU PARLAMENTU IN SVETU z naslovom Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU, JOIN(2017) 450 final.

4 Osnutek končnega poročila o raziskavi trga kibernetske varnosti iz leta 2018.

5 Osnutek končnega poročila o raziskavi trga kibernetske varnosti iz leta 2018.

6 Tehnična poročila JRC: Evropski centri strokovnega znanja o kibernetski varnosti, 2018

znanje spremenilo v tržne izdelke in rešitve, bi Uniji omogočilo kritje celotne vrednostne verige kibernetske varnosti. Vendar so prizadevanja raziskovalne in industrijske skupnosti razdrobljena, neusklajena, manjka jim skupno poslanstvo, kar ovira konkurenčnost EU na tem področju, pa tudi njeno sposobnost, da zavaruje svoja digitalna sredstva. Ustrezni sektorji kibernetske varnosti (npr. energija, vesolje, obramba, promet) in sektorji, povezani s kibernetsko varnostjo, danes niso dovolj podprti[7]. Sinergije med sektorji civilne in obrambne kibernetske varnosti v Evropi prav tako še niso v celoti izkoriščene.

Vzpostavitev javno-zasebnega partnerstva za kibernetsko varnost v Uniji leta 2016 je bil trden prvi korak k povezovanju skupnosti na področju raziskav, industrije in javnega sektorja za spodbujanje raziskav in inovacij na področju kibernetske varnosti, ki bi v okviru omejitev finančnega okvira za obdobje 2014–2020 moral zagotoviti dobre in bolj osredotočene rezultate na področju raziskav in inovacij. Javno-zasebno partnerstvo za kibernetsko varnost je industrijskim partnerjem omogočilo, da so izrazili zavezo o njihovi individualni porabi za področja, opredeljena v strateškem programu partnerstva za raziskave in inovacije.

Vendar pa si lahko Unija prizadeva za veliko večje naložbe in potrebuje učinkovitejši mehanizem, ki bi vzpostavil trajne zmogljivosti, združeval prizadevanja in strokovna znanja ter spodbujal razvoj inovativnih rešitev za odzivanje na industrijske izzive kibernetske varnosti na področju novih večnamenskih tehnologij (npr. umetne inteligence, kvantne računalniške tehnologije, blokovnih verig in varne digitalne identitete) ter v kritičnih sektorjih (npr. promet, energija, zdravje, finance, vlada, telekomunikacije, proizvodnja, obramba, vesolje).

Skupno sporočilo je obravnavalo možnost krepitve zmogljivosti Unije za kibernetsko varnost prek mreže strokovnih centrov za kibernetsko varnost z Evropskim strokovnim centrom za kibernetsko varnost na čelu. S tem bi se obstoječa prizadevanja za krepitev zmogljivosti na tem področju dopolnila na ravni Unije in na nacionalni ravni. V skupnem sporočilu je bila izražena namera Komisije, da v letu 2018 začne oceno učinka, da bi preučila možnosti za vzpostavitev takšne strukture. Da bi naredila prvi korak in pokazala pot za razmišljanje v prihodnje, je Komisija začela pilotno fazo v okviru programa Obzorje 2020, da bi pomagala povezati nacionalne centre v mrežo ter dala nov zagon razvoju strokovnih znanj in tehnologije kibernetske varnosti.

Voditelji držav in vlad so na digitalnem vrhu v Talinu septembra 2017 pozvali Unijo, naj postane „do leta 2025 vodilna v svetu na področju kibernetske varnosti, da se zagotovijo zaupanje, gotovost in zaščita državljanov, potrošnikov in podjetij na spletu ter omogoči brezplačen in zakonsko urejen internet.“

Svet je v svojih sklepih[8], sprejetih novembra 2017, pozval Komisijo, naj hitro zagotovi oceno učinka za posamezne možnosti in do sredine leta 2018 predlaga ustrezen pravni instrument za izvajanje pobude.

Program za digitalno Evropo, ki ga je Komisija predlagala junija 2018[9], skuša razširiti in čim bolj povečati koristi digitalne preobrazbe za evropske državljane in podjetja na vseh ustreznih področjih politik EU, okrepiti politike in podpreti ambicije enotnega digitalnega trga. Program

[7] Tehnično poročilo JRC: Rezultati popisa (za podrobnosti glej prilogi 4 in 5).

[8] Sklepi Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“, ki jo je sprejel Svet za splošne zadeve 20. novembra 2017.

[9] COM(2018) 434 Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027

predlaga skladen in vseobsegajoč pristop za zagotavljanje najboljše uporabe naprednih tehnologij in ustrezne kombinacije tehničnih zmogljivosti in človeških sposobnosti za digitalno preobrazbo – ne samo na področju kibernetske varnosti, ampak tudi v zvezi s pametno podatkovno infrastrukturo, umetno inteligenco, naprednimi spretnostmi in aplikacijami v industriji ter na področjih javnega interesa. Ti elementi so medsebojno odvisni in se vzajemno krepijo ter lahko, če se spodbujajo hkrati, dosežejo obseg, ki je potreben, da se omogoči razvoj podatkovnega gospodarstva[10]. V *programu Obzorje Evropa*[11], naslednjem okvirnem programu EU za raziskave in inovacije, je kibernetska varnost prav tako uvrščena med prednostne naloge.

V tem kontekstu se v tej uredbi predlaga vzpostavitev Evropskega industrijskega tehnološkega in raziskovalnega strokovnega centra z mrežo nacionalnih koordinacijskih centrov. Da bi ta namenski model sodelovanja spodbudil evropski tehnološki in industrijski ekosistem za kibernetsko varnost, bi moral delovati tako: strokovni center bo lajšal in pomagal koordinirati delo mreže ter podpiral strokovno skupnost za kibernetsko varnost, pri tem pa spodbujal tehnološko agendo na področju kibernetske varnosti in lajšal dostop do zbranega strokovnega znanja. Strokovni center bo to opravljal zlasti z izvajanjem zadevnih delov programa za digitalno Evropo in programa Obzorje Evrope ter z dodeljevanjem nepovratnih sredstev in javnimi naročili. Glede na znatne naložbe v kibernetsko varnost drugod po svetu in glede na potrebo po usklajevanju in združevanju pomembnih virov v Evropi se predlaga, da ima strokovni center obliko evropskega partnerstva[12], kar bo lajšalo skupne naložbe Unije, držav članic in/ali panoge. Zato predlog od držav članic zahteva, da k ukrepom strokovnega centra in mreže prispevajo sorazmeren znesek. Glavni organ odločanja je upravni odbor, v katerem sodelujejo vse države članice, glasovalno pravico pa imajo samo tiste, ki k strokovnemu centru finančno prispevajo. Sistem glasovanja v upravnem odboru sledi načelu dvojne večine, ki zahteva 75 % finančnih prispevkov in 75 % glasov. Glede na svojo odgovornost za proračun Unije ima Komisija 50 % glasov. Pri delu v upravnem odboru si bo Komisija po potrebi pomagala s strokovnim znanjem Agencije Evropske unije za varnost omrežij in informacij. Upravnemu odboru pomaga industrijsko-znanstveni svetovalni odbor, ki zagotavlja reden dialog z zasebnim sektorjem, združenji potrošnikov in drugimi ustreznimi zainteresiranimi stranmi.

V tesnem sodelovanju z mrežo nacionalnih koordinacijskih centrov in strokovno skupnostjo za kibernetsko varnost (ki vključuje veliko in raznoliko skupino akterjev, vključenih v tehnološki razvoj kibernetske varnosti, kot so raziskovalni subjekti, panoge na strani dobave in povpraševanja ter javni sektor), vzpostavljenima s to uredbo, bi bil Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost glavni izvedbeni organ za finančna sredstva EU, namenjena kibernetski varnosti v okviru predlaganih *programov za digitalno Evropo* in *Obzorje Evropa*.

Tak celovit pristop bi omogočil podpiranje kibernetske varnosti po celotni vrednostni verigi, od raziskav do podpore uvajanju in uporabi ključnih tehnologij. Finančni prispevek držav

---

10 Glej SWD(2018) 305.

11 COM 2018) 435 Predlog uredbe Evropskega parlamenta in Sveta o vzpostavitvi okvirnega programa za raziskave in inovacije Obzorje Evropa ter o določitvi pravil za sodelovanje in razširjanje njegovih rezultatov

12 Kot je določeno v Predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi okvirnega programa za raziskave in inovacije Obzorje Evropa ter o določitvi pravil za sodelovanje in razširjanje njegovih rezultatov, COM(2018) 435, in v Predlogu uredbe Evropskega parlamenta in Sveta o vzpostavitvi programa za digitalno Evropo za obdobje 2021–2027, COM(2018) 434.

članic mora biti sorazmeren s finančnim prispevkom EU k tej pobudi in je nepogrešljiv element za njegov uspeh.

Glede na njeno posebno strokovno znanje ter široko in ustrezno zastopanost deležnikov bi bilo treba Evropsko organizacijo za kibernetsko varnost, ki je za Komisijo nasprotna stran v pogodbenem javno-zasebnem partnerstvu za kibernetsko varnost v okviru programa Obzorje 2020, povabiti, da prispeva k delovanju centra in mreže.

Poleg tega bi si moral Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost prizadevati tudi za povečanje sinergijskih učinkov med civilnimi in obrambnimi razsežnostmi kibernetske varnosti. Državam članicam in drugim ustreznim akterjem bi moral nuditi podporo s svetovanjem, izmenjavo strokovnega znanja in spodbujanjem sodelovanja v zvezi s projekti in ukrepi. Na zahtevo držav članic bi lahko prevzel tudi vodenje projektov, zlasti v zvezi z Evropskim obrambnim skladom. Cilj te pobude je prispevati k reševanju naslednjih težav:

- **Nezadostno sodelovanje med panogami na strani povpraševanja in ponudbe na področju kibernetske varnosti.** Evropska podjetja se soočajo z izzivoma lastne varnosti ter ponudbe varnih izdelkov in storitev za svoje stranke. Vendar pogosto ne morejo ustrezno zavarovati svojih obstoječih izdelkov, storitev in premoženja ali oblikovati varnih inovativnih izdelkov in storitev. Ključna sredstva na področju kibernetske varnosti so pogosto predraga, da bi jih lahko razvili in vzpostavili posamezni akterji, katerih glavna poslovna dejavnost ni povezana s kibernetsko varnostjo. Hkrati pa povezave med povpraševanjem in ponudbo na trgu kibernetske varnosti niso dovolj dobro razvite, kar povzroča neoptimalno ponudbo evropskih izdelkov in rešitev, prilagojenih potrebam različnih sektorjev, ter nezadostno raven zaupanja med udeleženci na trgu.
- **Pomanjkanje učinkovitega mehanizma sodelovanja med državami članicami za krepitev industrijskih zmogljivosti.** Trenutno tudi ni učinkovitega mehanizma za sodelovanje med državami članicami, da bi si skupaj prizadevale za vzpostavitev potrebnih zmogljivosti, ki podpirajo inovacije na področju kibernetske varnosti v vseh industrijskih sektorjih in uvajanje vrhunskih evropskih rešitev na področju kibernetske varnosti. Obstoječi mehanizmi sodelovanja med državami članicami na področju kibernetske varnosti v skladu z Direktivo (EU) 2016/1148 v svojem mandatu ne predvidevajo tovrstnih dejavnosti.
- **Nezadostno sodelovanje znotraj raziskovalnih in industrijskih skupnosti ter med njimi.** Kljub temu, da je Evropa teoretično zmožna pokriti celotno vrednostno verigo kibernetske varnosti, obstajajo pomembni sektorji kibernetske varnosti (npr. energija, vesolje, obramba, promet) in podpodročja, ki jih raziskovalna skupnost danes slabo podpira, ali pa jih podpira le omejeno število centrov (npr. pokvantna in kvantna kriptografija, zaupanje in kibernetska varnost na področju umetne inteligence). Čeprav to sodelovanje očitno obstaja, je zelo pogosto kratkoročno in se izvaja v obliki svetovalnih storitev, kar ne omogoča izvajanja dolgoročnih raziskovalnih načrtov za reševanje industrijskih izzivov v zvezi s kibernetsko varnostjo.
- **Nezadostno sodelovanje med raziskovalnimi in inovacijskimi skupnostmi na področju kibernetske varnosti v civilnem in obrambnem sektorju.** Težava zaradi nezadostne stopnje sodelovanja zadeva tudi skupnosti na področju civilne in obrambne industrije. Obstoječi sinergijski učinki se ne uporabljajo v celoti zaradi pomanjkanja učinkovitih mehanizmov, ki bi tem skupnostim omogočili učinkovito sodelovanje in vzpostavitev zaupanja, ki je še bolj kot na drugih področjih predpogoj za uspešno sodelovanje. To je

povezano z omejenimi finančnimi zmožnostmi na trgu kibernetske varnosti v EU, vključno z nezadostnimi sredstvi za podporo inovacijam.

- **Skladnost z veljavnimi predpisi s področja zadevne politike**

Strokovna mreža za kibernetsko varnost ter Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost bosta delovala kot dodatna podpora obstoječim določbam in akterjem na področju politik kibernetske varnosti. Mandat Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost, bo dopolnjeval prizadevanja agencije ENISA, vendar se osredotoča na različna področja in zahteva drugačen sklop znanj in spretnosti. Medtem ko je v mandatu agencije ENISA predvidena svetovalna vloga glede raziskav in inovacij na področju kibernetske varnosti v EU, se njen predlagani mandat osredotoča predvsem na druge naloge, ki so ključne za krepitev odpornosti kibernetske varnosti v EU. Poleg tega mandat agencije ENISA ne predvideva vrst dejavnosti, ki bi bile osrednje naloge centra in mreže, tj. spodbujanje razvoja in uporabe tehnologije na področju kibernetske varnosti ter dopolnjevanje prizadevanj za krepitev zmogljivosti na tem področju na ravni EU in nacionalni ravni.

Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost in strokovna mreža za kibernetsko varnost bosta sodelovala tudi pri podpiranju raziskav, da se omogočijo in pospešijo postopki standardizacije in certificiranja, zlasti tisti, ki se nanašajo na certifikacijske sheme za kibernetsko varnost v smislu predlaganega akta o kibernetski varnosti[13][14].

Ta pobuda je dejansko okrepitev javno-zasebnega partnerstva za kibernetsko varnost, ki je bilo prvi poskus na ravni EU, da bi se panoga kibernetske varnosti, odjemalci (kupci izdelkov in rešitev za kibernetsko varnost, vključno z javno upravo in ključnimi sektorji, kot so promet, zdravje, energija, finance) in raziskovalna skupnost združili z namenom, da bi vzpostavili platformo za trajnostni dialog in ustvarili pogoje za prostovoljno sovlaganje. Pogodbeno javno-zasebno partnerstvo je bilo ustvarjeno leta 2016 in bo do leta 2020 sprožilo do 1,8 milijarde EUR naložb. Vendar obseg naložb, ki se izvajajo v drugih delih sveta (npr. ZDA so v kibernetsko varnost samo v letu 2017 vložile 19 milijard dolarjev), kaže, da mora EU storiti več za doseganje kritične mase naložb in odpraviti razdrobljenost zmogljivosti po vsej EU.

- **Skladnost z drugimi politikami Unije**

Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost bo deloval kot enoten izvedbeni organ za različne programe Unije, ki podpirajo kibernetsko varnost (program za digitalno Evropo in program Obzorje Evropa), ter povečal skladnost in sinergijske učinke med njimi.

Ta pobuda bo tudi dopolnila prizadevanja držav članic z zagotavljanjem ustreznega prispevka oblikovalcem politik na področju izobraževanja, da se okrepijo spretnosti na področju kibernetske varnosti (npr. z razvojem izobraževalnih načrtov za kibernetsko varnost v civilnih in vojaških izobraževalnih sistemih), kar bo v EU pomagalo razviti usposobljeno delovno silo

[13] Predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti, COM(2017) 477 final/3).

[14] To ne posega v mehanizme potrjevanja v okviru Splošne uredbe o varstvu podatkov, v kateri imajo organi za varstvo podatkov vlogo v skladu z Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).

na področju kibernetske varnosti – ključno prednost za podjetja na tem področju ter druge industrije, ki so na njem udeležene. V zvezi z izobraževanjem in usposabljanjem na področju kibernetske obrambe bo ta pobuda skladna s tekočimi prizadevanji platforme za izobraževanje, usposabljanje in vaje na področju kibernetske obrambe, ki je bila vzpostavljena v okviru Evropske akademije za varnost in obrambo.

Pobuda bo dopolnjevala in podpirala prizadevanja vozlišč za digitalne inovacije v okviru programa za digitalno Evropo. Vozlišča za digitalne inovacije so neprofitne organizacije, ki podjetjem, zlasti zagonskim podjetjem, MSP in podjetjem s srednje veliko tržno kapitalizacijo, s pomočjo pametnih inovacij, ki jih omogoča digitalna tehnologija, omogočajo večjo konkurenčnost z izboljšanjem njihovih poslovnih in proizvodnih procesov ter izdelkov in storitev. Vozlišča za digitalne inovacije zagotavljajo podjetniško usmerjene inovacijske storitve, kot so tržne informacije, svetovanje o financiranju, dostop do ustreznih ustanov za preizkušanje in eksperimentiranje, usposabljanje in razvoj spretnosti, pomoč pri uspešnem tržnem nastopu z novimi izdelki ali storitvami ali uvedba boljših proizvodnih postopkov. Nekatera vozlišča za digitalne inovacije, ki imajo posebno strokovno znanje na področju kibernetske varnosti, bi lahko bila neposredno vključena v strokovno skupnost za kibernetsko varnost, ki bo vzpostavljena s to pobudo. Vendar pa bi vozlišča za digitalne inovacije, ki niso posebej usmerjena v kibernetsko varnost, v večini primerov svojemu članstvu olajšala dostop do strokovnih znanj in zmogljivosti s področja kibernetske varnosti, ki so na voljo v strokovni skupnosti za kibernetsko varnost, pri čemer bi tesno sodelovala z mrežo nacionalnih koordinacijskih centrov in Evropskim industrijskim, tehnološkim in raziskovalnim strokovnim centrom za kibernetsko varnost. Vozlišča za digitalne inovacije bi podpirala tudi uvajanje inovativnih izdelkov in rešitev za kibernetsko varnost, ki ustrezajo potrebam podjetij in drugih končnih uporabnikov, ki jih oskrbujejo. Nenazadnje bi lahko sektorska vozlišča za digitalne inovacije z mrežo in centrom delila svoje znanje o dejanskih potrebah posameznih sektorjev za razmislek o programu raziskav in inovacij, ki bi ustrezal potrebam industrije.

Iskali se bodo sinergijski učinki z ustreznimi skupnostmi znanja in inovacij Evropskega inštituta za inovacije, zlasti na področju digitalne tehnologije.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

• Pravna podlaga

Strokovni center bi moral zaradi svoje narave in posebnih ciljev imeti dvojno pravno podlago. Člen 187 PDEU, ki določa strukture, potrebne za učinkovito izvajanje programov Unije za raziskave, tehnološki razvoj in predstavitvene dejavnosti, strokovnemu centru omogoča ustvarjanje sinergijskih učinkov in združevanje virov za naložbe v potrebne zmogljivosti na ravni držav članic ter razvoj skupnih evropskih sredstev (npr. skupno naročanje potrebne infrastrukture za preizkušanje in eksperimentiranje na področju kibernetske varnosti). Prvi odstavek člena 188 določa sprejetje takšnih ukrepov. Ne glede na to prvi pododstavek člena 188 kot edina pravna podlaga ne bi omogočil, da bi dejavnosti presegle področje raziskav in razvoja, kar je potrebno za izpolnitev vseh ciljev strokovnega centra, določenih v tej uredbi, ki podpirajo uvedbo izdelkov in rešitev za kibernetsko varnost na trg, s čimer bi evropski panogi kibernetske varnosti pomagali, da bi postala bolj konkurenčna in povečala svoj tržni delež, ter dodatno prispevali k nacionalnim prizadevanjem za obravnavo vrzeli v spretnostih na področju kibernetske varnosti. Zato je za dosego teh ciljev treba kot pravno podlago dodati člen 173(3), ki Uniji omogoča, da določi ukrepe za podporo konkurenčnosti industrije.

- **Utemeljitev predloga z vidika načel subsidiarnosti in sorazmernosti**

Kibernetska varnost je vprašanje skupnega interesa Unije, kot potrjujejo zgoraj navedeni sklepi Sveta. Obseg in čezmejni značaj incidentov, kot sta *WannaCry* ali *NonPetya*, sta tipičen primer. Zaradi narave in obsega tehnoloških izzivov kibernetske varnosti ter nezadostnega usklajevanja prizadevanj znotraj panoge, javnega sektorja in raziskovalnih skupnosti ter med njimi mora EU še naprej podpirati prizadevanja za usklajevanje, da bi združili kritično maso virov in zagotovili boljše upravljanje znanja in premoženja. To je potrebno glede na potrebe po virih, povezane z določenimi zmogljivostmi za raziskave, razvoj in uporabo kibernetske varnosti; potrebo po zagotavljanju dostopa do interdisciplinarnega strokovnega znanja in izkušenj na področju kibernetske varnosti na različnih področjih (ki je na nacionalni ravni pogosto le delno na voljo); globalno naravo industrijskih vrednostnih verig in dejavnost svetovnih konkurentov, ki nastopajo na trgih.

Za to so potrebni viri in strokovno znanje v obsegu, ki ga posamezni ukrepi katere koli države članice težko dosežejo. Na primer, vseevropska mreža za kvantne komunikacije bi lahko zahtevala naložbe EU v višini približno 900 milijonov EUR, odvisno od naložb držav članic (ki bodo medsebojno povezane/dopolnjene) in od tega, v kolikšni meri bo tehnologija omogočila ponovno uporabo obstoječe infrastrukture. Pobuda bo ključnega pomena pri združevanju finančnih virov in omogočanju tovrstnih naložb v Uniji.

Države članice same ne morejo v celoti doseči ciljev te pobude. Kot je prikazano zgoraj, jih je mogoče bolje doseči na ravni Unije z združevanjem prizadevanj in izogibanjem njihovemu nepotrebnemu podvajanju ter s tem pomagati pri doseganju kritične mase naložb in zagotavljanju optimalne uporabe javnega financiranja. V skladu z načelom sorazmernosti ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja. Ukrepanje EU je zato utemeljeno na podlagi subsidiarnosti in sorazmernosti.

Ta instrument ne predvideva novih regulativnih obveznosti za podjetja. Hkrati bodo podjetja, zlasti MSP, zmanjšala stroške v zvezi s svojimi prizadevanji pri snovanju inovativnih izdelkov za kibernetsko varnost, saj pobuda omogoča združevanje virov za naložbe v potrebne zmogljivosti na ravni držav članic ali razvoj skupnih evropskih sredstev (npr. skupno naročanje potrebne infrastrukture za preizkušanje in eksperimentiranje na področju kibernetske varnosti). Ta sredstva bi lahko uporabila podjetja in MSP v različnih sektorjih, da bi zagotovili, da so njihovi izdelki kibernetsko varni in da bi se kibernetska varnost spremenila v konkurenčno prednost.

- **Izbira instrumenta**

S predlaganim instrumentom se vzpostavlja organ, namenjen izvajanju ukrepov kibernetske varnosti v okviru programa za digitalno Evropo in programa Obzorje Evropa. V njem so predstavljeni njegov mandat, naloge in upravljavska struktura. Vzpostavitev takega organa Unije zahteva sprejetje uredbe.

3. POSVETOVANJA Z ZAINTERESIRANIMI STRANMI IN OCENE UČINKA

Predlog za vzpostavitev strokovne mreže za kibernetsko varnost z Evropskim industrijskim tehnološkim in raziskovalnim strokovnim centrom za kibernetsko varnost je nova pobuda. Deluje kot nadaljevanje in okrepitev pogodbenega javno-zasebnega partnerstva za kibernetsko varnost, ki je bilo vzpostavljeno leta 2016.

- **Posvetovanja z zainteresiranimi stranmi**

Kibernetska varnost je široka in medsektorska tema. Komisija je uporabila različne posvetovalne metode, da bi zagotovila, da se splošni javni interes Unije – v nasprotju s posebnimi interesi majhnega obsega interesnih skupin – dobro odraža v tej pobudi. Ta metoda zagotavlja preglednost in odgovornost pri delu Komisije. Glede na ciljno skupino (industrijska in raziskovalna skupnost ter države članice) javno posvetovanje posebej za to pobudo ni bilo izvedeno, vendar je bila tema že zajeta v več drugih odprtih javnih posvetovanjih:

- Splošno odprto javno posvetovanje, opravljeno leta 2018 na temo naložb, raziskav in razvoja, MPS in enotnega trga.
- Dvanajsttedensko spletno javno posvetovanje za pridobivanje mnenj širše javnosti (približno 90 respondentov) o oceni in pregledu agencije ENISA, opravljeno v letu 2017.
- Dvanajsttedensko spletno javno posvetovanje, ki je bilo izvedeno leta 2016 ob začetku pogodbenega javno-zasebnega partnerstva za kibernetsko varnost (približno 240 respondentov).

Komisija je organizirala tudi usmerjena posvetovanja o tej pobudi, vključno z delavnicami, srečanji in usmerjenimi zahtevami za prispevke (od agencije ENISA in Evropske obrambne agencije). Obdobje posvetovanja je trajalo več kot 6 mesecev, od novembra 2017 do marca 2018. Komisija je izvedla tudi kartiranje strokovnih centrov, kar je omogočilo zbiranje prispevkov iz 665 strokovnih centrov za kibernetsko varnost o njihovem znanju in izkušnjah, dejavnosti, delovnih področjih in mednarodnem sodelovanju. Raziskava se je začela izvajati januarja, raziskave, predložene do 8. marca 2018, pa so bile upoštevane pri analizi poročila.

Zainteresirane strani iz industrijskih in raziskovalnih skupnosti so menile, da lahko pristojni center in mreža dodata vrednost sedanjim prizadevanjem na nacionalni ravni, tako da prispevata k vzpostavitvi vseevropskega ekosistema kibernetske varnosti, ki bi omogočil boljše sodelovanje med raziskovalnimi in industrijskimi skupnostmi. Menile so tudi, da je nujno, da EU in države članice obravnavajo kibernetsko industrijsko politiko s proaktivne, dolgoročnejše in strateške perspektive, ki presega le raziskave in inovacije. Zainteresirane strani so izrazile potrebo po dostopu do ključnih zmogljivosti, kot so zmogljivosti za preizkušanje in eksperimentiranje, ter po ambicioznejšem pristopu k zapolnjevanju vrzeli v spretnostih na področju kibernetske varnosti, npr. prek obsežnih evropskih projektov, ki privabljajo največje talente. Vse navedeno se je tudi štelo za potrebno, da bi bila Unija na svetovni ravni priznana kot vodilna na področju kibernetske varnosti.

Države članice so v okviru posvetovanj, ki so se izvajala od septembra lani[15], kot tudi v namenskih sklepih Sveta[16] pozdravile namen vzpostavitve strokovne mreže za kibernetsko varnost, da bi se spodbujala razvoj in uporaba tehnologij kibernetske varnosti, pri tem pa so poudarile, da je treba vključiti vse države članice ter njihove obstoječe centre odličnosti in strokovne centre ter nameniti posebno pozornost dopolnjevanju. Posebej v zvezi s prihodnjim strokovnim centrom so države članice poudarile pomen svoje usklajevalne vloge v podporo mreži. Zlasti v zvezi z nacionalnimi dejavnostmi in potrebami na področju kibernetske obrambe je popis potreb držav članic po kibernetski obrambi, ki ga je marca 2018 izvedla Evropska služba za zunanje delovanje, pokazal, da večina držav članic vidi dodano vrednost

[15] Npr. okrogla miza na visoki ravni z državami članicami, podpredsednikom Ansipom in komisarko Gabriel, 5. decembra 2017.

[16] Svet za splošne zadeve: Sklepi Sveta o Skupnem sporočilu Evropskemu parlamentu in Svetu: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“ (20. november 2017).

pomoči EU pri kibernetskem izobraževanju in usposabljanju ter podpiranju industrije z raziskavami in razvojem[17]. Pobuda bi se dejansko izvajala v sodelovanju z državami članicami ali subjekti, ki jih te podpirajo. Sodelovanje med industrijo, raziskovalno skupnostjo in/ali javnim sektorjem bi združilo in okrepilo obstoječe subjekte in prizadevanja in ne ustvarilo novih. Države članice bi bile vključene tudi pri opredelitvi posebnih ukrepov, usmerjenih v javni sektor, ki je neposredni uporabnik tehnologije in strokovnega znanja za kibernetsko varnost.

- **Ocena učinka**

Dne 11. aprila 2017 je bila Odboru za regulativni nadzor predložena ocena učinka, ki podpira to pobudo, in prejeto je bilo pozitivno mnenje s pridržki. Ocena učinka je bila nato pregledana ob upoštevanju pripomb odbora. Mnenje odbora in priloga, v kateri je razloženo, kako so bile obravnavane pripombe odbora, sta objavljena skupaj s tem predlogom.

V oceni učinka so bile obravnavane številne možnosti politike, tako zakonodajne kot nezakonodajne. Za poglobljeno oceno so bile ohranjene naslednje možnosti:

- Osnovni scenarij – sodelovalna možnost – predvideva nadaljevanje sedanjega pristopa k razvoju industrijskih in tehnoloških zmogljivosti na področju kibernetske varnosti v EU s podpiranjem raziskav in inovacij ter z njimi povezanih mehanizmov sodelovanja v okviru devetega okvirnega programa.
- Možnost 1: Strokovna mreža za kibernetsko varnost z Evropskim industrijskim, tehnološkim in raziskovalnim strokovnim centrom za kibernetsko varnost z dvojnim mandatom za izvajanje ukrepov v podporo industrijskim tehnologijam ter na področju raziskav in inovacij.
- Možnost 2: Strokovna mreža za kibernetsko varnost z Evropskim raziskovalnim in strokovnim centrom za kibernetsko varnost, ki je osredotočena na raziskovalne in inovacijske dejavnosti

Možnosti, ki so bile opuščene že v zgodnji fazi, so vključevale: 1) možnost brez ukrepanja, 2) možnost vzpostavitve samo strokovne mreže za kibernetsko varnost, 3) možnost vzpostavitve samo centralizirane strukture, pa tudi 4) možnost uporabe obstoječe agencije (Agencije Evropske unije za varnost omrežij in informacij (ENISA), Izvajalske agencije za raziskave (REA) ali Izvajalske agencije za inovacije in omrežja (INEA).

V analizi je bilo ugotovljeno, da je možnost 1 najbolj primerna za doseganje ciljev pobude, hkrati pa zagotavlja največje gospodarske, družbene in okoljske učinke ter varuje interese Unije. Glavni argumenti v korist te možnosti so vključevali zmožnost ustvarjanja resnične industrijske politike za kibernetsko varnost s podpiranjem dejavnosti, ki niso povezane le z raziskavami in razvojem, temveč tudi z uvajanjem na trg; prožnost glede omogočanja različnih modelov sodelovanja z mrežo strokovnih centrov za optimalno uporabo obstoječega znanja in virov; sposobnost strukturirati sodelovanje ter skupne zaveze javnih in zasebnih zainteresiranih strani iz vseh zadevnih sektorjev, vključno z obrambo. Poleg tega možnost 1 omogoča tudi večje sinergijske učinke in lahko deluje kot izvedbeni mehanizem za dva različna tokova financiranja kibernetske varnosti v EU v naslednjem večletnem finančnem okviru (Program za digitalno Evropo, Obzorje Evropa).

[17] EEAS, marec 2018.

- **Temeljne pravice**

Ta pobuda bo javnim organom in industriji v državah članicah omogočila učinkovitejše preprečevanje kibernetskih groženj in odzivanje nanje, saj bodo na voljo varnejši izdelki in rešitve. To je zlasti pomembno za zaščito dostopa do osnovnih storitev (npr. prevoznih, zdravstvenih, bančnih in finančnih storitev).

Poleg tega bo večja zmožnost Evropske unije, da samostojno zavaruje svoje izdelke in storitve, verjetno pomagala državljanom uživati njihove demokratične pravice in vrednote (npr. z boljšim varovanjem pravic, povezanih z informacijami, ki jih določa Listina o temeljnih pravicah, zlasti pravico do varstva osebnih podatkov in zasebnega življenja) ter posledično povečati njihovo zaupanje v digitalno družbo in gospodarstvo.

4. PRORAČUNSKE POSLEDICE

Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost bo v sodelovanju s strokovno mrežo za kibernetsko varnost glavni izvedbeni organ za finančna sredstva EU, namenjena kibernetski varnosti v okviru programa za digitalno Evropo in programa Obzorje Evropa.

Proračunske posledice, povezane z izvajanjem programa za digitalno Evropo, so podrobno navedene v oceni finančnih posledic zakonodajnega predloga, priloženi temu predlogu. Prispevek iz finančnih sredstev sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 21(1)(b) bo Komisija predlagala v zakonodajnem postopku, vsekakor pa pred političnim dogovorom. Predlog bo temeljil na izidu postopka strateškega načrtovanja, kot je opredeljen v členu 6(6) Uredbe XXX [okvirni program Obzorje Evropa].

5. DRUGI ELEMENTI

- **Načrti za izvedbo ter ureditev spremljanja, ocenjevanja in poročanja**

V tem predlogu (člen 38) je predvidena izrecna klavzula o ocenjevanju, po kateri bo Komisija izvedla neodvisno oceno. Komisija bo nato o oceni poročala Evropskemu parlamentu in Svetu ter ji bo po potrebi priložila predlog za revizijo akta, da se izmerita učinek instrumenta in njegova dodana vrednost. Za ocene se bo uporabljala metodologija Komisije za boljše pravno urejanje.

Izvršni direktor bi moral upravnemu odboru vsaki dve leti predložiti naknadno oceno dejavnosti Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter dejavnosti mreže, kot je določeno v členu 17 tega predloga. Izvršni direktor bi moral pripraviti tudi akcijski načrt za nadaljnje ukrepe glede ugotovitev naknadnih ocen in Komisiji vsaki dve leti poročati o napredku. Upravni odbor bi moral biti odgovoren za spremljanje ustreznega odzivanja na take ugotovitve, kot je določeno v členu 16 tega predloga.

Domnevne primere nepravilnosti v dejavnostih pravne osebe lahko preiskuje evropski varuh človekovih pravic v skladu z določbami člena 228 Pogodbe.

2018/0328 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov

Prispevek Evropske komisije k srečanju voditeljev v Salzburgu 19. in 20. septembra 2018

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti člena 173(3) in prvega odstavka člena 188 Pogodbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[18],

ob upoštevanju mnenja Odbora regij[19],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Vsakdanje življenje in gospodarstvo postajata vse bolj odvisna od digitalnih tehnologij, državljani pa vedno bolj izpostavljeni resnim kibernetskim incidentom. Varnost bo v prihodnosti med drugim odvisna od povečanja tehnološke in industrijske zmogljivosti Unije za zaščito pred kibernetskimi grožnjami, saj se tako civilna infrastruktura kot tudi vojaške zmogljivosti zanašajo na varne digitalne sisteme.

(2) Da bi Unija obravnavala vse večje kibernetskovarnostne izzive, stopnjuje svoje dejavnosti, pri čemer upošteva strategijo za kibernetsko varnost[20] iz leta 2013, katere cilj je spodbujanje zanesljivega, varnega in odprtega kibernetskega ekosistema. Prve ukrepe na področju kibernetske varnosti je Unija sprejela leta 2016 z Direktivo (EU) 2016/1148 Evropskega parlamenta in Sveta[21] o varnosti omrežij in informacijskih sistemov.

(3) Septembra 2017 sta Komisija in visoka predstavnica Unije za zunanje zadeve in varnostno politiko predstavili skupno sporočilo[22] z naslovom „Odpornost, odvračanje

---

18 UL C, str. .

19 UL C, , str. .

20 Skupno sporočilo Evropskemu parlamentu in Svetu: Strategija Evropske unije za kibernetsko varnost: Odprt, varen in zanesljiv kibernetski prostor, JOIN(2013) 1 final.

21 Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

22 Skupno sporočilo Evropskemu parlamentu in Svetu z naslovom „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“, JOIN(2017) 450 final.

in obramba: okrepitev kibernetske varnosti za EU“, da bi se dodatno okrepili odpornost, odvračanje in odzivanje Unije na kibernetske napade.

(4) Voditelji držav in vlad so na digitalnem vrhu v Talinu septembra 2017 pozvali Unijo, naj postane „do leta 2025 vodilna v svetu na področju kibernetske varnosti, da se zagotovijo zaupanje, gotovost in zaščita državljanov, potrošnikov in podjetij na spletu ter omogoči brezplačen in zakonsko urejen internet.“

(5) Znatne motnje v omrežjih in informacijskih sistemih lahko vplivajo na posamezne države članice in Unijo kot celoto. Varnost omrežij in informacijskih sistemov je zato bistvena za nemoteno delovanje notranjega trga. Trenutno je Unija odvisna od neevropskih ponudnikov kibernetske varnosti. Vendar je v strateškem interesu Unije, da ohrani in razvije pomembne ključne tehnološke zmogljivosti kibernetske varnosti za zavarovanje njenega enotnega digitalnega trga ter zlasti za zaščito kritičnih omrežij in informacijskih sistemov ter zagotavljanje ključnih storitev kibernetske varnosti.

(6) Unija ima bogato strokovno znanje in izkušnje v zvezi z raziskavami, tehnologijo in industrijskim razvojem na področju kibernetske varnosti, vendar so prizadevanja raziskovalne in industrijske skupnosti razdrobljena in neusklajena, poleg tega pa jim manjka skupno poslanstvo, kar ovira konkurenčnost na tem področju. Ta prizadevanja in strokovno znanje je treba združiti, povezati v omrežja in učinkovito uporabiti, da se okrepijo in dopolnijo obstoječe raziskave ter tehnološke in industrijske zmogljivosti na ravni Unije in nacionalnih ravneh.

(7) Svet je v svojih sklepih, sprejetih novembra 2017, pozval Komisijo, naj hitro zagotovi oceno učinka za posamezne možnosti vzpostavitve mreže strokovnih centrov za kibernetsko varnost pod okriljem Evropskega raziskovalnega in strokovnega centra ter do sredine leta 2018 predlaga ustrezen pravni instrument.

(8) Strokovni center bi moral biti glavni instrument Unije za združevanje naložb v raziskave, tehnologije in industrijski razvoj na področju kibernetske varnosti, pa tudi za izvajanje zadevnih projektov in pobud v sodelovanju s strokovno mrežo za kibernetsko varnost. Zagotoviti bi moral finančno podporo za kibernetsko varnost iz programa Obzorje Evropa in programa za digitalno Evropo ter bi moral biti po potrebi odprt tudi Evropskemu skladu za regionalni razvoj in drugim programom. Ta pristop naj bi prispeval k ustvarjanju sinergij in usklajevanju finančne podpore za raziskave, inovacije, tehnologijo in industrijski razvoj na področju kibernetske varnosti ter izogibanju podvajanja.

(9) Ob upoštevanju dejstva, da je cilje te pobude mogoče najbolje doseči, če sodelujejo vse države članice oziroma če jih sodeluje čim več, in da se države članice spodbudi k sodelovanju, bi morale imeti glasovalne pravice samo tiste države članice, ki finančno prispevajo k upravnim in operativnim stroškom strokovnega centra.

(10) Finančni prispevek sodelujočih držav članic bi moral biti sorazmeren s finančnim prispevkom Unije k tej pobudi.

(11) Strokovni center naj bi olajšal in spodbujal usklajevanje dela strokovne mreže za kibernetsko varnost (v nadaljnjem besedilu: mreža), sestavljene iz nacionalnih koordinacijskih centrov v vsaki državi članici. Nacionalni koordinacijski centri bi morali prejemati neposredno finančno podporo Unije, vključno z nepovratnimi sredstvi, dodeljenimi brez razpisa za zbiranje predlogov, in sicer za izvajanje dejavnosti, povezanih s to uredbo.

(12) Nacionalne koordinacijske centre bi morale določiti države članice. Poleg potrebne upravne zmogljivosti bi morali imeti ti centri tehnološko strokovno znanje s področja

kibernetske varnosti ali pa neposreden dostop do takšnega znanja, zlasti na področjih, kot so kriptografija, varnostne storitve IKT, zaznavanje vdorov, varnost sistemov in omrežij, programska oprema, varnost aplikacij ter človeški in družbeni vidiki varnosti in zasebnosti. Prav tako bi morali imeti zmogljivost, da učinkovito sodelujejo in se usklajujejo z industrijo, javnim sektorjem, vključno z organi, imenovanimi v skladu z Direktivo (EU) 2016/1148 Evropskega parlamenta in Sveta[23], in raziskovalno skupnostjo.

(13) Če nacionalni koordinacijski centri dobivajo finančno podporo za pomoč tretjim stranem na nacionalni ravni, se ta podpora dodeli ustreznim zainteresiranim stranem na podlagi sporazumov o kaskadnih nepovratnih sredstvih.

(14) Tehnologije v vzponu, kot so umetna inteligenca, internet stvari, visokozmogljivostno in kvantno računalništvo, blokovne verige, ter koncepti, kot so varne digitalne identitete, ustvarjajo nove izzive za kibernetsko varnost, obenem pa ponujajo rešitve. Za ocenjevanje in potrjevanje odpornosti obstoječih in prihodnjih sistemov IKT bo potrebno preizkušati varnostne rešitve za obrambo pred napadi s pomočjo visokozmogljivostnih in kvantnih računalniških tehnologij. Strokovni center, mreža in strokovna skupnost za kibernetsko varnost bi morali pomagati razvijati in razširjati najsodobnejše rešitve za kibernetsko varnost. Hkrati bi morala strokovni center in mreža podpirati razvijalce in operaterje v ključnih sektorjih, kot so promet, energija, zdravje, finance, uprava, telekomunikacije, proizvodnja, obramba in vesolje, da bi jim pomagala reševati izzive na področju kibernetske varnosti.

(15) Strokovni center bi moral opravljati več ključnih funkcij. Prvič, moral bi lajšati in pomagati usklajevati delo evropske strokovne mreže za kibernetsko varnost in podpirati strokovno skupnost za kibernetsko varnost. Center bi moral spodbujati tehnološko agendo na področju kibernetske varnosti in lajšati dostop do strokovnega znanja, zbranega v mreži in strokovni skupnosti za kibernetsko varnost. Drugič, z dodeljevanjem nepovratnih sredstev, običajno na podlagi razpisa za zbiranje predlogov, bi moral izvajati ustrezne dele programa za digitalno Evropo in programa Obzorje Evropa. Tretjič, strokovni center bi moral lajšati skupne naložbe Unije, držav članic in/ali industrije.

(16) Strokovni center bi moral spodbujati in podpirati sodelovanje in usklajevanje dejavnosti strokovne skupnosti za kibernetsko varnost, kar bi vključevalo široko, odprto in raznoliko skupino akterjev, dejavnih na področju tehnologij kibernetske varnosti. Navedena skupnost bi morala vključevati zlasti raziskovalne subjekte, panoge na strani dobave in povpraševanja ter javni sektor. Strokovna skupnost za kibernetsko varnost bi morala prispevati k dejavnostim in načrtu dela strokovnega centra ter izkoristiti dejavnosti za krepitev skupnosti, ki jih izvajata strokovni center in mreža, ne bi pa smela imeti prednosti pri razpisih za zbiranje predlogov ali ponudb.

(17) Da bi se strokovni center lahko odzval na potrebe panog na strani dobave in povpraševanja, bi se njegove naloge zagotavljanja znanja in tehnične pomoči za industrijo v zvezi s kibernetsko varnostjo morale nanašati tako na izdelke in storitve IKT kot na vse druge industrijske in tehnološke izdelke in rešitve, katerih del bo kibernetska varnost.

[23] Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

(18) Medtem ko bi si morala strokovni center in mreža prizadevati doseči sinergije med civilnim in obrambnim sektorjem na področju kibernetske varnosti, se bodo projekti, financirani s strani programa Obzorje Evropa, izvajali v skladu z Uredbo XXX [Uredba o programu Obzorje Evropa], ki določa, da so dejavnosti na področju raziskav in inovacij, ki se izvajajo v okviru Obzorja Evropa, osredotočene na uporabo v civilne namene.

(19) Da se zagotovi strukturirano in trajnostno sodelovanje med strokovnim centrom in nacionalnimi koordinacijskimi centri, bi moralo to temeljiti na pogodbenem sporazumu.

(20) Sprejeti bi bilo treba ustrezne določbe, ki bodo zagotavljale odgovornost in preglednost strokovnega centra.

(21) Glede na strokovno znanje s področja kibernetske varnosti, ki ga imata Skupno raziskovalno središče Komisije in Agencija Evropske unije za varnost omrežij in informacij, bi morala oba imeti dejavno vlogo v strokovni skupnosti za kibernetsko varnost ter industrijskem in znanstvenem svetovalnem odboru.

(22) Če nacionalni koordinacijski centri prejemajo finančni prispevek iz splošnega proračuna Unije, bi morali ti centri in subjekti, ki so del strokovne skupnosti za kibernetsko varnost, javno objaviti, da zadevne dejavnosti potekajo v okviru te pobude.

(23) Prispevek Unije k strokovnemu centru bi moral financirati polovico stroškov vzpostavitve ter administrativnih in usklajevalnih dejavnosti centra. Da bi se izognili dvojnemu financiranju, navedene dejavnosti ne bi smele hkrati prejemati prispevka iz drugih programov Unije.

(24) Upravni odbor, ki ga sestavljajo države članice in Komisija, bi moral določati splošno usmeritev dejavnosti strokovnega centra in zagotavljati, da ta naloge opravlja v skladu s to uredbo. Na upravni odbor bi bilo treba prenesti pooblastila, potrebna za pripravo proračuna, preverjanje njegovega izvrševanja, sprejetje ustreznih finančnih pravil, uvedbo preglednih delovnih postopkov za sprejemanje odločitev strokovnega centra, sprejetje programa dela in večletnega strateškega načrta, ki odražata prednostne naloge za doseganje ciljev in nalog strokovnega centra, ter lastnega poslovnika, imenovanje izvršnega direktorja ter odločitev o podaljšanju in koncu mandata izvršnega direktorja.

(25) Da bi strokovni center pravilno in učinkovito deloval, bi morale Komisija in države članice zagotoviti, da imajo osebe, ki so imenovane v upravni odbor, ustrezno strokovno znanje in izkušnje na funkcijskih področjih. Komisija in države članice bi si morale prizadevati tudi za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile njegovo neprekinjeno delovanje.

(26) Da bi strokovni center deloval nemoteno, je treba njegovega izvršnega direktorja imenovati na podlagi zaslug ter dokazanih upravnih in vodstvenih sposobnosti ter ustrezne usposobljenosti in izkušenj s področja kibernetske varnosti, izvršni direktor pa mora svoje naloge opravljati popolnoma neodvisno.

(27) Strokovni center bi moral imeti industrijsko-znanstveni svetovalni odbor, ki bi deloval kot svetovalni organ, da bi zagotovil reden dialog z zasebnim sektorjem, združenji potrošnikov in drugimi ustreznimi zainteresiranimi stranmi. Industrijsko-znanstveni svetovalni odbor bi se moral osredotočati na zadeve, ki so pomembne za zainteresirane strani, in o njih obvestiti upravni odbor strokovnega centra. Sestava industrijsko-znanstvenega svetovalnega odbora in naloge, dodeljene temu odboru, na primer

posvetovanje glede načrta dela, bi morale zagotoviti zadostno zastopanost zainteresiranih strani pri delu strokovnega centra.

(28) Med trajanjem programa Obzorje 2020 bi moral strokovni center prek industrijsko-znanstvenega svetovalnega odbora izkoristiti posebno strokovno znanje ter široko zastopanost zadevnih zainteresiranih strani na podlagi pogodbenega javno-zasebnega partnerstva za kibernetsko varnost.

(29) Strokovni center bi moral sprejeti pravila za preprečevanje in upravljanje nasprotij interesov. Strokovni center bi moral poleg tega uporabljati ustrezne predpise Unije o dostopu javnosti do dokumentov iz Uredbe Evropskega parlamenta in Sveta (ES) št. 1049/2001[24]. Strokovni center obdeluje osebne podatke v skladu z Uredbo (EU) št. XXX/2018 Evropskega parlamenta in Sveta. Strokovni center bi moral spoštovati določbe, ki veljajo za institucije Unije, in nacionalno zakonodajo o ravnanju s podatki, zlasti občutljivimi netajnimi podatki in tajnimi podatki EU.

(30) Finančne interese Unije in držav članic bi bilo treba v celotnem ciklu odhodkov zaščititi s sorazmernimi ukrepi, med katerimi so preprečevanje, odkrivanje in preiskovanje nepravilnosti, povračilo izgubljenih, neupravičeno izplačanih ali nepravilno porabljenih sredstev ter po potrebi izvrševanje upravnih in denarnih kazni v skladu z Uredbo (EU, Euratom) XXX Evropskega parlamenta in Sveta[25] [finančna uredba].

(31) Strokovni center bi moral delovati odprto in pregledno, s pravočasnim zagotavljanjem vseh ustreznih informacij in promocijo svojih dejavnosti, vključno z dejavnostmi obveščanja in razširjanja informacij v širši javnosti. Poslovnik organov strokovnega centra bi bilo treba objaviti.

(32) Notranji revizor Komisije bi moral imeti v zvezi s strokovnim centrom enaka pooblastila, kot jih ima v zvezi s Komisijo.

(33) Komisija, strokovni center, Računsko sodišče in Evropski urad za boj proti goljufijam bi morali imeti dostop do vseh informacij in prostorov, potrebnih za izvedbo revizij in preiskav glede nepovratnih sredstev, pogodb in sporazumov, ki jih podpiše strokovni center.

(34) Ker ciljev te uredbe, tj. ohranjanje in razvijanje tehnoloških in industrijskih zmogljivosti Unije na področju kibernetske varnosti, povečanje konkurenčnosti panoge kibernetske varnosti ter pretvarjanje kibernetske varnosti v konkurenčno prednost drugih panog v Uniji, države članice same ne morejo zadovoljivo doseči zaradi razpršenosti obstoječih, omejenih sredstev in zaradi obsega potrebnih naložb, temveč se ti cilji zaradi preprečevanja nepotrebnega podvajanja prizadevanj, prispevanja k doseganju kritične mase in zagotavljanja optimalne porabe javnega financiranja lažje dosežejo na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. Skladno z načelom sorazmernosti iz navedenega člena Pogodbe ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

---

[24] Uredba Evropskega parlamenta in Sveta (ES) št. 1049/2001 z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).

[25] [dodati naslov in sklic na UL]

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE IN NAČELA STROKOVNEGA CENTRA TER MREŽE

Člen 1

Predmet urejanja

1. Ta uredba vzpostavlja Evropski center za kibernetsko varnost (v nadaljnjem besedilu: strokovni center) in mrežo nacionalnih koordinacijskih centrov ter določa pravila za imenovanje nacionalnih koordinacijskih centrov ter vzpostavitev strokovne skupnosti za kibernetsko varnost.

2. Strokovni center prispeva k izvajanju kibernetskovarnostnega dela programa za digitalno Evropo, vzpostavljenega z Uredbo št. XXX in zlasti ukrepov, povezanih s členom 6 Uredbe (EU) št. XXX [program za digitalno Evropo] in programa Obzorje Evropa, vzpostavljenega z Uredbo št. XXX in zlasti Oddelkom 2.2.6 Stebra II Priloge I Sklepa št. XXX o vzpostavitvi posebnega programa za izvajanje okvirnega programa za raziskave in inovacije Obzorje Evropa [skl. št. posebnega programa].

3. Sedež strokovnega centra se nahaja v [Bruslju, Belgija.]

4. Strokovni center je pravna oseba. V vsaki državi članici uživa najširšo pravno in poslovno sposobnost, ki jo pravnim osebam priznava zakonodaja te države članice. Zlasti lahko pridobiva premičnine in nepremičnine ali z njimi razpolaga ter je lahko stranka v pravnih postopkih.

Člen 2

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „kibernetska varnost“ pomeni zaščito omrežij in informacijskih sistemov, uporabnikov ter drugih oseb pred kibernetskimi grožnjami;

(2) „izdelki in rešitve za kibernetsko varnost“ pomeni izdelke, storitve ali procese IKT s posebnim namenom zaščite omrežij in informacijskih sistemov, uporabnikov ter prizadetih oseb pred kibernetskimi grožnjami.

(3) „javni organ“ pomeni vlado ali drugo javno upravo, vključno z javnimi svetovalnimi organi, na nacionalni, regionalni ali lokalni ravni ali fizično ali pravno osebo, ki opravlja naloge javne uprave po nacionalnem pravu, vključno s posebnimi nalogami;

(4) „sodelujoča država članica“ pomeni državo članico, ki prostovoljno finančno prispeva k upravnim in operativnim stroškom strokovnega centra.

Člen 3

Poslanstvo centra in mreže

1. Strokovni center in mreža Uniji pomagata, da:

(a) ohrani in razvije potrebne kibernetskovarnostne tehnološke in industrijske zmogljivosti za varovanje enotnega digitalnega trga;

(b) poveča konkurenčnost kibernetskovarnostne panoge Unije in kibernetsko varnost pretvarja v konkurenčno prednost za druge panoge Unije.

2. Strokovni center opravlja svoje naloge, kadar je ustrezno, v sodelovanju z mrežo nacionalnih koordinacijskih centrov in strokovno skupnostjo za kibernetsko varnost.

Člen 4

Cilji in naloge centra

Strokovni center ima naslednje cilje in povezane naloge:

1. olajšati in pomagati koordinirati delo mreže nacionalnih koordinacijskih centrov (v nadaljnjem besedilu: mreža) iz člena 6 in strokovne skupnosti za kibernetsko varnost iz člena 8;

2. prispevati k izvajanju kibernetskovarnostnega dela programa za digitalno Evropo, vzpostavljenega z uredbo št. XXX[26] in zlasti ukrepov, povezanih s členom 6 Uredbe (EU) št. XXX [program za digitalno Evropo], in programa Obzorje Evropa, vzpostavljenega z Uredbo št. XXX[27], ter zlasti oddelka 2.2.6 stebra II Priloge I Sklepa št. XXX o vzpostavitvi posebnega programa za izvajanje okvirnega programa za raziskave in inovacije Obzorje Evropa [skl. št. posebnega programa] ter drugih programov Unije, kadar je določeno v pravnih aktih Unije;

3. izboljšati zmogljivosti, znanje in infrastrukturo na področju kibernetske varnosti v korist panog, javnega sektorja in raziskovalnih skupnosti z opravljanjem naslednjih nalog:

   (a) pridobivanjem, posodabljanjem, upravljanjem in dajanjem na voljo najsodobnejše industrijske in raziskovalne infrastrukture na področju kibernetske varnosti ter povezanih storitev različnim industrijskim uporabnikom po vsej Uniji, vključno z MSP, javnim sektorjem ter raziskovalno in znanstveno skupnostjo;

   (b) zagotavljanjem podpore, tudi finančne, drugim subjektom pri pridobivanju, posodabljanju, upravljanju in dajanju na voljo najsodobnejše industrijske in raziskovalne infrastrukture na področju kibernetske varnosti ter povezanih storitev različnim industrijskim uporabnikom po vsej Uniji, vključno z MSP, javnim sektorjem ter raziskovalno in znanstveno skupnostjo;

   (c) zagotavljanjem znanja na področju kibernetske varnosti in tehnične pomoči panogi in javnim organom, zlasti s podpiranjem ukrepov za lažji dostopa do strokovnega znanja, dostopnega v mreži in strokovni skupnosti za kibernetsko varnost;

4. prispevati k široki uvedbi najsodobnejših izdelkov in rešitev za kibernetsko varnost v gospodarstvu z opravljanjem naslednjih nalog:

[26] [dodaj polni naslov in sklic na UL]
[27] [dodaj polni naslov in sklic na UL]

(a) spodbujanjem raziskav na področju kibernetske varnosti, razvoja ter uporabe izdelkov in rešitev za kibernetsko varnost Unije s strani javnih organov in uporabniških panog;

(b) pomočjo javnim organom, panogam na strani povpraševanja in drugim uporabnikom pri sprejemanju in vključevanju najnovejših rešitev za kibernetsko varnost;

(c) podporo zlasti javnim organom pri organizaciji javnega naročanja ali izvajanju javnega naročanja najsodobnejših izdelkov in rešitev za kibernetsko varnost v imenu javnih organov;

(d) zagotavljanjem finančne podpore in tehnične pomoči za zagonska podjetja in MSP na področju kibernetske varnosti, da se povežejo s potencialnimi trgi in privabijo naložbe;

5. izboljšati razumevanje kibernetske varnosti in prispevati k zmanjšanju vrzeli v znanjih in spretnostih v Uniji na področju kibernetske varnosti z opravljanjem naslednjih nalog:

(a) podpiranjem nadaljnjega razvoja znanj in spretnosti na področju kibernetske varnosti, kadar je ustrezno, skupaj z ustreznimi agencijami in organi EU, vključno z agencijo ENISA;

6. prispevati h krepitvi raziskav in razvoja na področju kibernetske varnosti v Uniji:

(a) z zagotavljanjem finančne podpore raziskovalnim prizadevanjem na področju kibernetske varnosti, ki temeljijo na skupnem, nenehno vrednotenem in izboljševanem večletnem strateškem, industrijskem, tehnološkem in raziskovalnem programu;

(b) s podporo obsežnim raziskovalnim in predstavitvenim projektom v zvezi s kibernetskovarnostnimi tehnološkimi zmogljivostmi naslednje generacije v sodelovanju s panogo in mrežo;

(c) s podporo raziskavam in inovacijam za standardizacijo v tehnologiji na področju kibernetske varnosti;

7. s krepitvijo sodelovanja med civilnim in obrambnim področjem v zvezi s tehnologijami in aplikacijami z dvojno rabo na področju kibernetske varnosti, in sicer z opravljanjem naslednjih nalog:

(a) s podporo držav članic ter industrijskih in raziskovalnih zainteresiranih strani pri raziskavah, razvoju in uvedbi;

(b) s prispevanjem k sodelovanju med državami članicami tako, da se podpira izobraževanje, usposabljanje in vaje;

(c) z združevanjem zainteresiranih strani za spodbujanje sinergij med civilnim in obrambnim vidikom raziskav in trgov kibernetske varnosti;

8. izboljševati sinergijske učinke med civilnimi in obrambnimi vidiki kibernetske varnosti v zvezi z evropskim obrambnim skladom z opravljanjem naslednjih nalog:

(a) s svetovanjem, izmenjavo strokovnega znanja in olajševanjem sodelovanja med ustreznimi zainteresiranimi stranmi;

(b) z upravljanjem večnacionalnih projektov na področju kibernetske obrambe, kadar jih zahtevajo države članice, s čimer deluje kot vodja

projekta v smislu Uredbe XXX [uredba o vzpostavitvi Evropskega obrambnega sklada].

Člen 5

Naložba v infrastrukturo, zmogljivosti, izdelke ali rešitve in njihova uporaba

1. Kadar strokovni center zagotavlja financiranje infrastrukture, zmogljivosti, izdelkov ali rešitev v skladu s členom 4(3) in (4) v obliki nepovratnih sredstev ali nagrade, lahko delovni načrt strokovnega centra podrobno določi zlasti:

   (a) pravila o delovanju infrastrukture ali zmogljivosti, kadar je ustrezno tudi poverjanje dejavnosti organu gostitelju na podlagi meril, ki jih določi strokovni center;

   (b) pravila o dostopu do infrastrukture ali zmogljivosti in njuni uporabi.

2. Strokovni center je lahko odgovoren za splošno izvajanje ustreznih skupnih dejavnosti javnega naročanja, vključno s predkomercialnimi javnimi naročili v imenu članov mreže, članov strokovne skupnosti za kibernetsko varnost ali ostalih tretjih strani, ki predstavljajo uporabnike izdelkov in rešitev za kibernetsko varnost. V ta namen lahko strokovnemu centru pomaga eden ali več nacionalnih koordinacijskih centrov ali članov strokovne skupnosti za kibernetsko varnost.

Člen 6

Imenovanje nacionalnih koordinacijskih centrov

1. Do [datum] vsaka država članica imenuje subjekt, ki deluje kot nacionalni koordinacijski center za namene te uredbe, in o tem uradno obvesti Komisijo.

2. Komisija na podlagi ocene skladnosti navedenega subjekta z merili iz odstavka 4 v šestih mesecih od imenovanja, ki ga je posredovala država članica, izda sklep o akreditaciji subjekta kot nacionalnega koordinacijskega centra ali o zavrnitvi imenovanja. Komisija objavi seznam nacionalnih koordinacijskih centrov.

3. Države članice lahko za namene te uredbe kadar koli imenujejo nov subjekt kot nacionalni koordinacijski center. Za imenovanje vsakega novega subjekta se uporabljata odstavka 1 in 2.

4. Imenovani nacionalni koordinacijski center je strokovnemu centru in mreži sposoben pomagati pri izpolnjevanju njunega poslanstva iz člena 3 te uredbe. Ima tehnološko strokovno znanje na področju kibernetske varnosti ali neposreden dostop do njega in je sposoben učinkovitega sodelovanja ter usklajevanja z industrijo, javnim sektorjem in raziskovalno skupnostjo.

5. Razmerje med strokovnim centrom in nacionalnimi koordinacijskimi centri temelji na pogodbenem sporazumu, ki ga podpišeta strokovni center in vsak nacionalni koordinacijski center. Sporazum določa pravila o razmerju in delitvi nalog med strokovnim centrom in vsakim nacionalnim koordinacijskim centrom.

6. Mrežo nacionalnih koordinacijskih centrov sestavljajo vsi nacionalni koordinacijski centri, ki jih imenujejo države članice.

Člen 7

Naloge nacionalnih koordinacijskih centrov

1. Nacionalni koordinacijski centri imajo naslednje naloge:

   (a) podpirati strokovni center pri doseganju njegovih ciljev in zlasti pri usklajevanju strokovne skupnosti za kibernetsko varnost;

   (b) olajšati udeležbo industrije in drugih akterjev na ravni držav članic pri čezmejnih projektih;

   (c) skupaj s strokovnim centrom prispevati k opredelitvi in obravnavanju sektorskih industrijskih izzivov na področju kibernetske varnosti;

   (d) na nacionalni ravni delovati kot kontaktna točka za strokovno skupnost za kibernetsko varnost in strokovni center;

   (e) prizadevati si za sinergije z ustreznimi dejavnostmi na nacionalni in regionalni ravni;

   (f) izvajati posebne ukrepe, za katere je strokovni center dodelil nepovratna sredstva, vključno z zagotavljanjem finančne podpore tretjim osebam v skladu s členom 204 Uredbe XXX [nova finančna uredba], pod pogoji, določenimi v zadevnih sporazumih o dodelitvi sredstev;

   (g) spodbujati in razširjati ustrezne delovne rezultate mreže, strokovne skupnosti za kibernetsko varnost in strokovnega centra na nacionalni ali regionalni ravni;

   (h) ocenjevati zahtevke subjektov, ki imajo sedež v isti državi članici kot koordinacijski center, da postanejo del strokovne skupnosti za kibernetsko varnost.

2. Za namene točke (f) se lahko finančna podpora tretjim osebam zagotovi v kateri koli obliki iz člena 125 Uredbe XXX [nova finančna uredba], tudi v obliki pavšalnih zneskov.

3. Nacionalni koordinacijski centri lahko v povezavi z opravljanjem nalog iz tega člena od Unije prejmejo nepovratna sredstva v skladu s členom 195(d) Uredbe XXX [nova finančna uredba].

4. Kadar je ustrezno, nacionalni koordinacijski centri sodelujejo prek mreže za namen izvajanja nalog iz točk (a), (b), (c), (e) in (g) odstavka 1.

Člen 8

Strokovna skupnost za kibernetsko varnost

1. Strokovna skupnost za kibernetsko varnost prispeva k poslanstvu strokovnega centra, kot je določeno v členu 3, ter krepi in razširja strokovno znanje o kibernetski varnosti po vsej Uniji.

2. Strokovno skupnost za kibernetsko varnost sestavljajo industrija, akademske in neprofitne raziskovalne organizacije in združenja ter javni in drugi subjekti, ki se ukvarjajo z operativnimi in tehničnimi zadevami. Združuje glavne zainteresirane strani v zvezi s tehnološkimi in industrijskimi kibernetskovarnostnimi zmogljivostmi v Uniji. Vključuje nacionalne koordinacijske centre ter institucije in organe Unije z ustreznim strokovnim znanjem.

3. Kot člani strokovne skupnosti za kibernetsko varnost so lahko akreditirani samo subjekti s sedežem v Uniji. Izkazovati morajo strokovno znanje na področju kibernetske varnosti na najmanj enem od naslednjih področij:

(a) raziskave,

(b) industrijski razvoj,

(c) usposabljanje in izobraževanje.

4. Strokovni center akreditira subjekte, ustanovljene po nacionalnem pravu, kot člane strokovne skupnosti za kibernetsko varnost, ko nacionalni koordinacijski center države članice, v kateri ima subjekt sedež, oceni, ali navedeni subjekt izpolnjuje merila iz odstavka 3. Akreditacija ni časovno omejena, vendar jo lahko strokovni center kadar koli prekliče, če sam ali ustrezni nacionalni koordinacijski center meni, da subjekt ne izpolnjuje meril iz odstavka 3 ali če zanj veljajo ustrezne določbe iz člena 136 Uredbe XXX [nova finančna uredba].

5. Strokovni center akreditira ustrezne organe, agencije in urade Unije kot člane strokovne skupnosti za kibernetsko varnost, ko oceni, ali navedeni subjekt izpolnjuje merila iz odstavka 3. Akreditacija ni časovno omejena, vendar jo lahko strokovni center kadar koli prekliče, če meni, da subjekt ne izpolnjuje meril iz odstavka 3 ali če zanj veljajo ustrezne določbe iz člena 136 Uredbe XXX [nova finančna uredba].

6. Predstavniki Komisije lahko sodelujejo pri delu strokovne skupnosti za kibernetsko varnost.

Člen 9

Naloge članov strokovne skupnosti za kibernetsko varnost

Člani strokovne skupnosti za kibernetsko varnost:

(1) podpirajo strokovni center pri izpolnjevanju poslanstva in ciljev iz členov 3 in 4 ter v ta namen tesno sodelujejo s strokovnim centrom in ustreznimi nacionalnimi koordinacijskimi centri;

(2) sodelujejo pri dejavnostih, ki jih spodbuja strokovni center in nacionalni koordinacijski centri;

(3) kadar je ustrezno, sodelujejo v delovnih skupinah, ki jih ustanovi upravni odbor strokovnega centra, za opravljanje posebnih dejavnosti, kot je določeno v delovnem načrtu strokovnega centra;

(4) kadar je ustrezno, podpirajo strokovni center in nacionalne koordinacijske centre pri promociji konkretnih projektov;

(5) promovirajo in razširjajo ustrezne izide dejavnosti in projektov, opravljenih v okviru strokovne skupnosti za kibernetsko varnost.

Člen 10

Sodelovanje strokovnega centra z institucijami, organi, uradi in agencijami Unije

1. Strokovni center sodeluje z ustreznimi institucijami, organi, uradi in agencijami Unije, vključno z Agencijo Evropske unije za varnost omrežij in informacij, skupino za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU), Evropsko službo za zunanje delovanje, skupnim raziskovalnim središčem Komisije, Izvajalsko agencijo za raziskave, Evropskim centrom za boj proti kibernetski kriminaliteti pri Europolu in Evropsko obrambno agencijo.

2. Tako sodelovanje poteka v okviru delovnih dogovorov. Navedeni dogovori se predložijo Komisiji v predhodno odobritev.

POGLAVJE II

ORGANIZIRANOST STROKOVNEGA CENTRA

Člen 11

Članstvo in struktura

1. Člani strokovnega centra so Unija, ki jo zastopa Komisija, in države članice.
2. Struktura strokovnega centra vključuje:
   (a) upravni odbor, ki izvaja naloge iz člena 13;
   (b) izvršnega direktorja, ki izvaja naloge iz člena 16;
   (c) industrijski in znanstveni svetovalni odbor, ki izvaja naloge iz člena 20.

ODDELEK I

UPRAVNI ODBOR

Člen 12

Sestava upravnega odbora

1. Upravni odbor sestavljajo po en predstavnik vsake države članice in pet predstavnikov Komisije v imenu Unije.
2. Vsak član upravnega odbora ima namestnika, ki ga zastopa v njegovi odsotnosti.
3. Člani upravnega odbora in njihovi namestniki so imenovani zaradi svojega znanja na področju tehnologije in ustreznih vodstvenih, upravnih in proračunskih znanj in spretnosti. Komisija in države članice si prizadevajo za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile njegovo neprekinjeno delovanje. Komisija in države članice si prizadevajo za uravnoteženo zastopanost moških in žensk v upravnem odboru.
4. Mandat članov upravnega odbora in njihovih namestnikov traja štiri leta. Ta mandat se lahko podaljša.
5. Člani upravnega odbora delujejo v interesu strokovnega centra ter neodvisno in pregledno varujejo njegove cilje in poslanstvo, identiteto, avtonomnost in skladnost.
6. Komisija lahko na sestanke upravnega odbora povabi opazovalce, vključno s predstavniki zadevnih organov, uradov in agencij Unije.
7. Agencija Evropske unije za varnost omrežij in informacij (ENISA) je stalna opazovalka v upravnem odboru.

Člen 13

Naloge upravnega odbora

1. Upravni odbor je v celoti odgovoren za strateško usmeritev in delovanje strokovnega centra ter nadzira izvajanje njegovih dejavnosti.

2. Upravni odbor sprejme svoj poslovnik. Ta poslovnik vključuje posebne postopke za ugotavljanje in preprečevanje nasprotij interesov ter zagotavljanje zaupnosti vseh občutljivih informacij.

3. Upravni odbor sprejema potrebne strateške odločitve, zlasti:

(a) sprejme večletni strateški načrt, ki vsebuje izjavo o glavnih prednostnih nalogah in načrtovanih pobudah strokovnega centra, vključno z oceno potreb po financiranju in virih;

(b) na podlagi predloga izvršnega direktorja sprejme delovni načrt strokovnega centra, letne računovodske izkaze in bilanco stanja ter letno poročilo o dejavnostih;

(c) sprejme posebna finančna pravila strokovnega centra v skladu s [členom 70 FU];

(d) sprejme postopek za imenovanje izvršnega direktorja;

(e) sprejme merila in postopke za ocenjevanje in akreditacijo subjektov kot članov strokovne skupnosti za kibernetsko varnost;

(f) imenuje, razreši, in spremlja uspešnost izvršnega direktorja, mu podaljša mandat in daje usmeritve ter imenuje računovodjo;

(g) sprejme letni proračun strokovnega centra, vključno z ustreznim kadrovskim načrtom, v katerem sta navedeni število začasnih delovnih mest po funkcionalnih skupinah in plačnih razredih ter število pogodbenih uslužbencev in napotenih nacionalnih strokovnjakov v ekvivalentih polnega delovnega časa;

(h) sprejme pravila glede nasprotij interesov;

(i) ustanovi delovne skupine s člani strokovne skupnosti za kibernetsko varnost;

(j) imenuje člane industrijskega in znanstvenega svetovalnega odbora;

(k) vzpostavi funkcijo notranjega revizorja v skladu z Delegirano uredbo Komisije (EU) št. 1271/2013[28];

(l) promovira strokovni center na svetovni ravni, da se poveča njegova privlačnost in postane vrhunski organ za odličnost na področju kibernetske varnosti;

(m) na podlagi priporočila izvršnega direktorja določi komunikacijsko politiko strokovnega centra;

(n) nosi odgovornost za spremljanje ustreznih nadaljnjih ukrepov v zvezi z ugotovitvami retrospektivnih vrednotenj;

(o) kadar je ustrezno, določi izvedbena pravila h Kadrovskim predpisom in Pogojem za zaposlitev v skladu s členom 31(3);

(p) kadar je ustrezno, določi pravila o napotitvi nacionalnih strokovnjakov v strokovni center in o uporabi pripravnikov v skladu s členom 32(2);

(q) sprejme varnostna pravila za strokovni center;

[28] Delegirana uredba Komisije (EU) št. 1271/2013 z dne 30. septembra 2013 o okvirni finančni uredbi za organe iz člena 208 Uredbe (EU, Euratom) št. 966/2012 Evropskega parlamenta in Sveta (UL L 328, 7.12.2013, str. 42).

(r) sprejme strategijo za boj proti goljufijam, ki je sorazmerna s tveganji goljufije, in sicer ob upoštevanju analize stroškov in koristi ukrepov, ki jih je treba izvesti;

(s) sprejme metodologijo za izračun finančnega prispevka držav članic;

(t) nosi odgovornost za vse naloge, ki niso posebej dodeljene kateremu od organov strokovnega centra; take naloge lahko dodeli kateremu koli članu strokovnega centra.

Člen 14

Predsednik in seje upravnega odbora

1. Upravni odbor med svojimi člani z glasovalno pravico izvoli predsednika in njegovega namestnika za obdobje dveh let. Mandat predsednika in njegovega namestnika se lahko na podlagi sklepa upravnega odbora enkrat podaljša. Če njuno članstvo v upravnem odboru preneha med njunim mandatom, na isti datum samodejno preneha tudi njun mandat. Namestnik predsednika po uradni dolžnosti nadomešča predsednika, kadar slednji ne more opravljati svojih nalog. Predsednik se udeleži glasovanja.
2. Upravni odbor se redno sestane najmanj trikrat na leto. Na zahtevo Komisije, tretjine članov, predsednika ali izvršnega direktorja pri izpolnjevanju njegovih nalog se lahko sestane na izredni seji.
3. Izvršni direktor sodeluje v razpravah, razen če upravni odbor odloči drugače, vendar nima glasovalnih pravic. Upravni odbor lahko v posameznih primerih povabi druge osebe, da se udeležijo njegovih sestankov kot opazovalke.
4. Člani industrijskega in znanstvenega svetovalnega odbora se lahko na povabilo predsednika udeležijo upravnega odbora, vendar nimajo glasovalnih pravic.
5. Če to omogoča poslovnik, lahko članom upravnega odbora in njihovim namestnikom na sejah pomagajo svetovalci ali strokovnjaki.
6. Strokovni center zagotovi sekretariat za upravni odbor.

Člen 15

Pravila glasovanja upravnega odbora

1. Unija ima 50 % glasovalnih pravic. Glasovalne pravice Unije so nedeljive.
2. Vsaka sodelujoča država članica ima en glas.
3. Upravni odbor sklepe sprejema z večino najmanj 75 % vseh glasov, vključno z glasovi odsotnih članov, ki predstavljajo najmanj 75 % vseh finančnih prispevkov strokovnemu centru. Finančni prispevek bo izračunan na podlagi ocenjenih odhodkov iz člena 17(2)(c), ki jih predlagajo države članice, in na podlagi poročila o vrednosti prispevkov sodelujočih držav članic iz člena 22(5).
4. Glasovalne pravice imajo samo predstavniki Komisije in predstavniki sodelujočih držav članic.
5. Predsednik se udeleži glasovanja.

ODDELEK II

IZVRŠNI DIREKTOR

Člen 16

Imenovanje, razrešitev ali podaljšanje mandata izvršnega direktorja

1. Izvršni direktor je oseba s strokovnim znanjem in velikim ugledom na področjih delovanja strokovnega centra.

2. Izvršni direktor je zaposlen kot začasni uslužbenec strokovnega centra v skladu s členom 2(a) Pogojev za zaposlitev drugih uslužbencev.

3. Izvršnega direktorja imenuje upravni odbor s seznama kandidatov, ki jih predlaga Komisija, po javnem in preglednem izbirnem postopku.

4. Strokovni center pri sklenitvi pogodbe z izvršnim direktorjem zastopa predsednik upravnega odbora.

5. Mandat izvršnega direktorja traja štiri leta. Komisija do konca tega obdobja opravi oceno, pri kateri upošteva vrednotenje uspešnosti dela izvršnega direktorja ter prihodnjih nalog in izzivov strokovnega centra.

6. Upravni odbor lahko na predlog Komisije, ki upošteva oceno iz odstavka 5, mandat izvršnega direktorja enkrat podaljša za največ štiri leta.

7. Izvršni direktor, katerega mandat je bil podaljšan, ne sme sodelovati pri drugem izbirnem postopku za isto delovno mesto.

8. Izvršni direktor se lahko razreši samo s sklepom upravnega odbora, sprejetim na predlog Komisije.

Člen 17

Naloge izvršnega direktorja

1. Izvršni direktor nosi odgovornost za delovanje in tekoče vodenje strokovnega centra in je njegov zakoniti zastopnik. Odgovoren je upravnemu odboru in svoje naloge opravlja povsem samostojno v okviru podeljenih pristojnosti.

2. Izvršni direktor neodvisno izvaja zlasti naslednje naloge:

   (a) izvaja sklepe, ki jih sprejme upravni odbor;

   (b) podpira upravni odbor pri delu, mu zagotavlja sekretariat za seje in vse potrebne informacije za opravljanje nalog;

   (c) po posvetovanju z upravnim odborom in Komisijo pripravi osnutek večletnega strateškega načrta in osnutek letnega delovnega načrta strokovnega centra, vključno z obsegom razpisov za zbiranje predlogov, razpisov za prijavo interesa in razpisov za zbiranje ponudb, ki so potrebni za izvajanje delovnega načrta in vključno z ustreznimi ocenami odhodkov, kot so jih predlagale države članice in Komisija, ter ju predloži v sprejetje upravnemu odboru;

   (d) pripravi osnutek letnega proračuna, vključno z ustreznim kadrovskim načrtom, v katerem sta navedeni število začasnih delovnih mest za vsak plačni razred in funkcionalno skupino ter število pogodbenih uslužbencev in napotenih nacionalnih strokovnjakov v ekvivalentih polnega delovnega časa, ter ga predloži v sprejetje upravnemu odboru;

   (e) izvaja delovni načrt in o njem poroča upravnemu odboru;

(f) pripravi osnutek letnega poročila o dejavnostih strokovnega centra, vključno z informacijami o ustreznih odhodkih;

(g) zagotavlja izvajanje učinkovitih postopkov spremljanja in vrednotenja uspešnosti strokovnega centra;

(h) pripravi akcijski načrt, pri čemer upošteva ugotovitve retrospektivnih vrednotenj in poroča Komisiji o napredku vsaki dve leti;

(i) pripravi sporazume z nacionalnimi koordinacijskimi centri, se o njih pogaja in jih sklepa;

(j) nosi odgovornost za upravne, finančne in kadrovske zadeve, vključno z izvajanjem proračuna strokovnega centra, pri čemer ustrezno upošteva mnenja funkcije notranjega revizorja v okviru omejitev iz pooblastila upravnega odbora;

(k) odobri in vodi objave razpisov za zbiranje predlogov v skladu z delovnim načrtom ter upravlja sporazume in sklepe o dodelitvi nepovratnih sredstev;

(l) na podlagi prednostnega seznama, ki ga pripravi skupina neodvisnih strokovnjakov, odobri seznam ukrepov, izbranih za financiranje;

(m) odobri in vodi objave razpisov za zbiranje ponudb v skladu z delovnim načrtom ter upravlja pogodbe;

(n) odobri ponudbe, izbrane za financiranje;

(o) predloži osnutek letnih računovodskih izkazov in bilance stanja funkciji notranjega revizorja in nato upravnemu odboru;

(p) zagotovi izvajanje ocen in obvladovanja tveganja;

(q) podpisuje posamezne sporazume, sklepe in pogodbe o dodelitvi nepovratnih sredstev;

(r) podpisuje pogodbe o javnih naročilih;

(s) pripravi akcijski načrt ob upoštevanju ugotovitev notranjih ali zunanjih revizijskih poročil in preiskav Evropskega urada za boj proti goljufijam (OLAF) ter poroča Komisiji o napredku dvakrat letno, upravnemu odboru pa redno;

(t) pripravi osnutke finančnih pravil, ki se uporabljajo za strokovni center;

(u) vzpostavi in zagotovi delovanje uspešnega in učinkovitega sistema notranjega nadzora ter upravnemu odboru poroča o vseh večjih spremembah tega sistema;

(v) skrbi za učinkovito komuniciranje z institucijami Unije;

(w) sprejme vse druge ukrepe, potrebne za oceno napredka strokovnega centra pri njegovem poslanstvu in ciljih iz členov 3 in 4 te uredbe;

(x) opravlja vse druge naloge, ki mu jih naloži upravni odbor ali ga zanje pooblasti.

ODDELEK III

INDUSTRIJSKI IN ZNANSTVENI SVETOVALNI ODBOR

Člen 18

Sestava industrijskega in znanstvenega svetovalnega odbora

1. Industrijski in znanstveni svetovalni odbor sestavlja največ 16 članov. Člane imenuje upravni odbor izmed predstavnikov subjektov strokovne skupnosti za kibernetsko varnost.
2. Člani industrijskega in znanstvenega svetovalnega odbora imajo strokovno znanje v zvezi z raziskavami na področju kibernetske varnosti, industrijskim razvojem, strokovnimi storitvami ali njihovim uvajanjem. Zahteve po takem strokovnem znanju podrobneje določi upravni odbor.
3. Postopki v zvezi z imenovanjem članov upravnega odbora in delovanjem svetovalnega odbora se podrobno določijo v poslovniku strokovnega centra in se objavijo.
4. Mandat članov industrijskega in znanstvenega svetovalnega odbora traja tri leta. Ta mandat se lahko podaljša.
5. Predstavniki Komisije in Agencije Evropske unije za varnost omrežij in informacij lahko sodelujejo pri delu industrijskega in znanstvenega svetovalnega odbora ter ga pri tem podpirajo.

Člen 19

Delovanje industrijskega in znanstvenega svetovalnega odbora

1. Industrijski in znanstveni svetovalni odbor se sestane najmanj dvakrat letno.
2. Industrijski in znanstveni svetovalni odbor lahko upravnemu odboru svetuje o ustanovitvi delovnih skupin za posebna vprašanja, pomembna za delo strokovnega centra, po potrebi v okviru splošnega usklajevanja prek enega ali več članov industrijskega in znanstvenega svetovalnega odbora.
3. Industrijski in znanstveni svetovalni odbor izvoli svojega predsednika.
4. Industrijski in znanstveni svetovalni odbor sprejme svoj poslovnik, ki vključuje določbe o imenovanju predstavnikov, ki zastopajo svetovalni odbor, kadar je ustrezno, in obdobju, za katerega so imenovani.

Člen 20

Naloge industrijskega in znanstvenega svetovalnega odbora

Industrijski in znanstveni svetovalni odbor svetuje strokovnemu centru glede izvajanja svojih dejavnosti in:

(1) izvršnemu direktorju ter upravnemu odboru v rokih, ki jih določi upravni odbor, strateško svetuje in prispeva k pripravi osnutka delovnega načrta ter večletnega strateškega načrta;

(2) organizira javna posvetovanja, odprta za vse javne in zasebne zainteresirane strani, ki imajo interes na področju kibernetske varnosti, da bi zbral mnenja za strateško svetovanje iz odstavka 1;

(3) spodbuja in zbira povratne informacije o delovnem načrtu in večletnem strateškem načrtu strokovnega centra.

POGLAVJE III
FINANČNE DOLOČBE

Člen 21

Finančni prispevek Unije

1. Prispevek Unije strokovnemu centru za kritje upravnih in operativnih stroškov vključuje naslednje:

   (a) 1 981 668 000 EUR iz programa za digitalno Evropo, kar vključuje do 23 746 000 EUR za upravne stroške;

   (b) znesek iz programa Obzorje Evropa, vključno z upravnimi stroški, ki se določi ob upoštevanju postopka strateškega načrtovanja, ki se bo izvajal v skladu s členom 6(6) Uredbe XXX [uredba Obzorje Evropa].

2. Najvišji možni prispevek Unije se plača iz odobritev splošnega proračuna Unije, dodeljenih [programu za digitalno Evropo] in posebnemu programu za izvajanje programa Obzorje Evropa, vzpostavljenemu s Sklepom XXX.

3. Strokovni center izvaja ukrepe v zvezi s kibernetsko varnostjo [program za digitalno Evropo] in [program Obzorje Evropa] v skladu s točko (c)(iv) člena 62 Uredbe (EU, Euratom) XXX[29] [finančna uredba].

4. Finančni prispevek Unije ne krije nalog iz člena 4(8)(b).

Člen 22

Prispevki sodelujočih držav članic

1. Skupni znesek prispevka sodelujočih držav članic k operativnim in upravnim stroškom strokovnega centra je najmanj enak zneskom iz člena 21(1) te uredbe.

2. Za oceno prispevkov iz odstavka 1 in točke (b)ii člena 23(3) se stroški določijo v skladu z običajnimi praksami stroškovnega računovodstva zadevnih držav članic, veljavnimi računovodskimi standardi države članice in veljavnimi mednarodnimi računovodskimi standardi ter mednarodnimi standardi računovodskega poročanja. Stroške potrdi neodvisni zunanji revizor, ki ga imenuje zadevna država članica. V primeru morebitne negotovosti v zvezi s to potrditvijo lahko strokovni center preveri metodo, po kateri se je ocenila vrednost.

3. Če katera koli sodelujoča država članica ne izpolni obveznosti v zvezi s svojim finančnim prispevkom, jo izvršni direktor o tem pisno obvesti in določi razumen rok, do katerega mora izpolniti obveznosti. Če obveznosti do navedenega roka ne izpolni, izvršni direktor skliče sestanek upravnega odbora, ki odloči o tem, ali se glasovalne pravice sodelujoče države članice prekličejo oziroma ali se sprejmejo drugi ukrepi, dokler obveznosti niso izpolnjene. Glasovalne pravice se sodelujoči državi članici, ki ne izpolnjuje obveznosti, začasno odvzamejo, dokler ne izpolni obveznosti.

4. Komisija lahko ukine, sorazmerno zmanjša ali začasno ustavi finančni prispevek Unije strokovnemu centru, če sodelujoče države članice v zvezi s prispevki iz odstavka 1 ne prispevajo, prispevajo le delno ali z zamudo.

[29] [dodaj polni naslov in sklic na UL]

5. Sodelujoče države članice vsako leto do 31. januarja poročajo upravnemu odboru o vrednosti prispevkov iz odstavka 1, in sicer za vsako predhodno proračunsko leto.

Člen 23

Stroški in sredstva strokovnega centra

1. Strokovni center skupaj financirajo Unija in države članice s finančnimi prispevki, plačanimi v obrokih, in s prispevki, ki zajemajo stroške nacionalnih koordinacijskih centrov in upravičencev pri izvajanju ukrepov, ki jih ne povrne strokovni center.
2. Upravni stroški strokovnega centra niso višji od [številka] EUR in se krijejo s finančnimi prispevki, ki so na letni ravni enakovredno porazdeljeni med Unijo in sodelujoče države članice. Če se del prispevka za upravne stroške ne porabi, se lahko da na voljo za kritje operativnih stroškov strokovnega centra.
3. Operativni stroški strokovnega centra se krijejo s:
   (a) finančnim prispevkom Unije;
   (b) prispevki sodelujočih držav članic v obliki:
      (i) finančnih prispevkov in
      (ii) kadar je ustrezno, prispevkov v naravi sodelujočih držav članic za stroške, ki jih imajo nacionalni koordinacijski centri in upravičenci pri izvajanju posrednih ukrepov, od česar se odšteje prispevek strokovnega centra in kateri koli drug prispevek Unije k tem stroškom.
4. Sredstva strokovnega centra, vključena v njegov proračun, so sestavljena iz naslednjih prispevkov:
   (a) finančnih prispevkov sodelujočih držav članic za upravne stroške;
   (b) finančnih prispevkov sodelujočih držav članic za operativne stroške;
   (c) morebitnih prihodkov, ki jih ustvari strokovni center;
   (d) morebitnih drugih finančnih prispevkov, sredstev in prihodkov.
5. Vse obresti na prispevke, ki jih strokovnemu centru plačajo sodelujoče države članice, se štejejo za njegov prihodek.
6. Namen vseh sredstev in dejavnosti strokovnega centra je doseganje ciljev iz člena 4.
7. Strokovni center ima v lasti vsa sredstva, ki jih ustvari ali so bila nanj prenesena za izpolnjevanje ciljev.
8. Razen v primeru prenehanja delovanja strokovnega centra se presežki prihodkov nad odhodki ne izplačajo sodelujočim članom strokovnega centra.

Člen 24

Finančne obveznosti

Finančne obveznosti strokovnega centra niso višje od zneska finančnih sredstev, ki je na voljo ali ki ga v njegov proračun vplačajo njegovi člani.

Člen 25

Proračunsko leto

Proračunsko leto traja od 1. januarja do 31. decembra.

Člen 26

Določitev proračuna

1. Izvršni direktor vsako leto pripravi osnutek poročila o oceni prihodkov in odhodkov strokovnega centra za naslednje proračunsko leto in ga skupaj z osnutkom kadrovskega načrta predloži upravnemu odboru. Prihodki in odhodki so uravnoteženi. Odhodki strokovnega centra vključujejo stroške za osebje, upravne stroške ter stroške za infrastrukturo in poslovanje. Upravni izdatki se omejijo na najnižjo možno raven.
2. Upravni odbor na podlagi osnutka poročila o oceni prihodkov in odhodkov iz odstavka 1 vsako leto pripravi poročilo o oceni prihodkov in odhodkov strokovnega centra za naslednje proračunsko leto.
3. Upravni odbor vsako leto do 31. januarja Komisiji pošlje poročilo o oceni iz odstavka 2, ki je del osnutka enotnega programskega dokumenta.
4. Komisija na podlagi poročila o oceni v osnutek proračuna Unije, ki ga predloži Evropskemu parlamentu in Svetu v skladu s členoma 313 in 314 PDEU, vnese ocene, ki so po njenem mnenju potrebne v skladu s kadrovskim načrtom, in znesek prispevka v breme splošnega proračuna.
5. Evropski parlament in Svet odobrita odobritve za prispevek, namenjen strokovnemu centru.
6. Evropski parlament in Svet sprejmeta kadrovski načrt strokovnega centra.
7. Upravni odbor sprejme proračun centra skupaj z delovnim načrtom. Proračun je dokončen, ko je dokončno sprejet splošni proračun Unije. Upravni odbor po potrebi prilagodi proračun in delovni načrt strokovnega centra v skladu s splošnim proračunom Unije.

Člen 27

Priprava zaključnega računa strokovnega centra in razrešnica

Začasni in zaključni račun strokovnega centra ter razrešnica se predložijo po pravilih in časovnem razporedu iz finančne uredbe ter njenih finančnih pravil, sprejetih v skladu s členom 29.

Člen 28

Operativno in finančno poročanje

1. Izvršni direktor upravnemu odboru letno poroča o opravljanju svojih nalog v skladu s finančnimi pravili strokovnega centra.
2. Izvršni direktor v dveh mesecih po koncu vsakega proračunskega leta upravnemu odboru v odobritev predloži letno poročilo o dejavnostih in napredku strokovnega centra v preteklem koledarskem letu, zlasti v zvezi z delovnim načrtom za zadevno leto. To poročilo med drugim vključuje informacije o naslednjih zadevah:

   (a) opravljenih operativnih ukrepih in ustreznih odhodkih;

(b) predloženih ukrepih, vključno z njihovo razčlenitvijo po vrsti udeležencev, vključno z MSP, in po državah članicah;

(c) ukrepih, izbranih za financiranje, vključno z njihovo razčlenitvijo po vrsti udeležencev, vključno z MSP, in po državah članicah ter navedbo prispevka strokovnega centra za posamezne udeležence in ukrepe;

(d) napredku pri doseganju ciljev iz člena 4 in predlogih za nadaljnje delo, potrebno za dosego teh ciljev.

3. Letno poročilo o dejavnostih se po odobritvi upravnega odbora objavi.

Člen 29

Finančna pravila

Strokovni center sprejme posebna finančna pravila v skladu s členom 70 Uredbe št. XXX [nova finančna uredba].

Člen 30

Zaščita finančnih interesov

1. Strokovni center sprejme ustrezne ukrepe za zagotovitev, da se ob izvajanju ukrepov, financiranih na podlagi te uredbe, finančni interesi Unije zaščitijo s preventivnimi ukrepi proti goljufijam, korupciji in kakršnim koli drugim nezakonitim dejavnostim, z izvajanjem učinkovitih pregledov in, če so ugotovljene nepravilnosti, z izterjavo neupravičeno plačanih zneskov ter, kadar je to ustrezno, z učinkovitimi, sorazmernimi in odvračilnimi upravnimi sankcijami.

2. Strokovni center osebju Komisije in drugim osebam, ki jih je ta pooblastila, ter Računskemu sodišču omogoči dostop do svojih objektov in prostorov ter do vseh informacij, tudi tistih v elektronski obliki, ki so potrebne za izvedbo revizij.

3. Evropski urad za boj proti goljufijam (OLAF) lahko izvaja preiskave, vključno s pregledi in inšpekcijami na kraju samem, v skladu z določbami in postopki iz Uredbe Sveta (EU, Euratom) št. 2185/96[30] in Uredbo (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta[31], da ugotovi, ali je pri sporazumu o dodelitvi nepovratnih sredstev ali pogodbi, ki se neposredno ali posredno financira v skladu s to uredbo, prišlo do goljufije, korupcije ali kakršne koli druge nezakonite dejavnosti, ki vpliva na finančne interese Unije.

4. Brez poseganja v odstavke 1, 2 in 3 tega člena pogodbe in sporazumi o dodelitvi nepovratnih sredstev, ki izhajajo iz izvajanja te uredbe, vsebujejo določbe, ki Komisijo, strokovni center, Računsko sodišče in urad OLAF izrecno pooblaščajo, da izvedejo take revizije in preiskave v skladu s svojimi pristojnostmi. Kadar se izvajanje ukrepa v celoti ali delno odda zunanjim izvajalcem ali opravlja na podlagi nadaljnjega prenosa pooblastil ali kadar izvajanje ukrepa zahteva oddajo javnega

[30] Uredba Sveta (Euratom, ES) št. 2185/96 z dne 11. novembra 1996 o pregledih in inšpekcijah na kraju samem, ki jih opravlja Komisija za zaščito finančnih interesov Evropskih skupnosti pred goljufijami in drugimi nepravilnostmi (UL L 292, 15.11.1996, str. 2).

[31] Uredba (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 11. septembra 2013 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF), ter razveljavitvi Uredbe (ES) št. 1073/1999 Evropskega parlamenta in Sveta in Uredbe Sveta (Euratom) št. 1074/1999 (UL L 248, 18.9.2013, str. 1).

naročila ali finančno podporo tretji strani, pogodba ali sporazum o dodelitvi nepovratnih sredstev vključuje obveznost izvajalca ali upravičenca, da od vsake udeležene tretje strani zahteva izrecno sprejetje teh pooblastil Komisije, strokovnega centra, Računskega sodišča in urada OLAF.

POGLAVJE IV

OSEBJE STROKOVNEGA CENTRA

Člen 31

Osebje

1. Za osebje strokovnega centra se uporabljajo Kadrovski predpisi za uradnike Evropske unije in Pogoji za zaposlitev drugih uslužbencev Evropske unije, kakor so določeni z določeni z Uredbo (EGS, Euratom, ESPJ) št. 259/68[32] (v nadaljnjem besedilu: Kadrovski predpisi in Pogoji za zaposlitev) ter pravila, ki so jih institucije Unije skupaj sprejele za uporabo Kadrovskih predpisov in Pogojev za zaposlitev.
2. Upravni odbor v zvezi z osebjem strokovnega centra izvaja pooblastila, ki so s Kadrovskimi predpisi podeljena organu za imenovanja, s Pogoji za zaposlitev drugih uslužbencev pa organu, pristojnemu za sklepanje pogodb (v nadaljnjem besedilu: pooblastila organa za imenovanja).
3. Upravni odbor v skladu s členom 110 Kadrovskih predpisov sprejme sklep na podlagi člena 2(1) Kadrovskih predpisov in člena 6 Pogojev za zaposlitev, s katerim na izvršnega direktorja prenese ustrezna pooblastila organa za imenovanja in opredeli pogoje, v skladu s katerimi se lahko navedeni prenos pooblastil začasno prekine. Izvršni direktor ima dovoljenje za nadaljnji prenos navedenih pooblastil.
4. Upravni odbor lahko zaradi izjemnih okoliščin s sklepom začasno prekine prenos pooblastil organa za imenovanja na izvršnega direktorja in vsa pooblastila, ki jih je ta prenesel naprej. V takem primeru upravni odbor pooblastila organa za imenovanja izvaja sam ali jih prenese na enega od svojih članov ali uslužbenca strokovnega centra, razen izvršnega direktorja.
5. Upravni odbor sprejme izvedbena pravila v zvezi s Kadrovskimi predpisi in Pogoji za zaposlitev v skladu s členom 110 Kadrovskih predpisov.
6. Kadrovski viri se določijo v kadrovskem načrtu strokovnega centra, v katerem sta navedeni število začasnih delovnih mest po funkcionalnih skupinah in plačnih razredih ter število pogodbenih uslužbencev v ekvivalentu polnega delovnega časa, v skladu z letnim proračunom strokovnega centra.
7. Osebje strokovnega centra vključuje začasne in pogodbene uslužbence.
8. Vse stroške v zvezi z osebjem nosi strokovni center.

Člen 32

Napoteni nacionalni strokovnjaki in drugo osebje

[32] Uredba Sveta (EGS, Euratom, ESPJ) št. 259/68 z dne 29. februarja 1968 o določitvi Kadrovskih predpisov za uradnike in Pogojev za zaposlitev drugih uslužbencev Evropskih skupnosti ter o uvedbi posebnih ukrepov, ki se začasno uporabljajo za uradnike Komisije (UL L 56, 4.3.1968, str. 1).

1. Strokovni center lahko uporabi napotene nacionalne strokovnjake ali drugo osebje, ki ni zaposleno v strokovnem centru.

2. Upravni odbor v dogovoru s Komisije sprejme sklep, s katerim določi pravila o napotitvi nacionalnih strokovnjakov v strokovni center.

Člen 33

Privilegiji in imunitete

Za strokovni center in njegovo osebje se uporablja Protokol št. 7 o privilegijih in imunitetah Evropske unije, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije.

POGLAVJE V
SKUPNE DOLOČBE

Člen 34

Varnostni predpisi

1. Za sodelovanje pri vseh ukrepih, ki jih financira strokovni center, se uporablja člen 12(7) Uredbe (EU) št. XXX [program za digitalno Evropo].

2. Za ukrepe, ki se financirajo iz programa Obzorje Evropa, se uporabljajo naslednji posebni varnostni predpisi:

   (a) za namene člena 34(1) [Lastništvo in zaščita] Uredbe (EU) št. XXX [Obzorje Evropa] se lahko dodelitev neizključnih licenc, kadar je tako določeno v delovnem načrtu, omeji na tretje osebe, ki imajo sedež ali se šteje, da imajo sedež v državi članici in jih upravlja država članica in/ali državljan države članice;

   (b) za namene člena 36(4)(b) [Prenos in podelitev licenc] Uredbe (EU) št. XXX [Obzorje Evropa] je prenos lastništva ali podelitev licence pravnemu subjektu s sedežem v pridruženi tretji državi ali s sedežem v Uniji, a nadzorovanem iz tretjih držav, prav tako razlog za nasprotovanje prenosu lastništva rezultatov ali podelitvi izključne licence v zvezi z rezultati;

   (c) za namene člena 37(3)(a) [Pravice dostopa] Uredbe (EU) št. XXX [Obzorje Evropa] se lahko, kadar je tako določeno v delovnem načrtu, dodelitev dostopa do rezultatov in ozadja omeji le na pravni subjekt, ki ima sedež v državi članici in ga nadzoruje država članica in/ali državljan države članice ali se zanj to šteje.

Člen 35

Preglednost

1. Strokovni center svoje dejavnosti opravlja zelo pregledno.

2. Strokovni center zagotovi, da javnost in vse zainteresirane strani dobijo ustrezne, objektivne, zanesljive in zlahka dostopne informacije, zlasti glede rezultatov njegovega dela. Objavi tudi izjave o interesih, ki so bile podane v skladu s členom 41.

3. Upravni odbor lahko na predlog izvršnega direktorja odobri, da zainteresirane strani kot opazovalci sodelujejo pri nekaterih dejavnostih strokovnega centra.

4. Strokovni center v poslovniku določi praktične ureditve za izvajanje pravil o preglednosti iz odstavkov 1 in 2. Pri ukrepih, ki se financirajo iz programa Obzorje Evropa, se bodo ustrezno upoštevale določbe iz Priloge III k uredbi o programu Obzorje Evropa.

Člen 36

Varnostni predpisi v zvezi z varovanjem tajnih podatkov in občutljivih netajnih podatkov

1. Brez poseganja v člen 35 strokovni center tretjim stranem ne razkrije informacij, ki jih obdeluje ali prejme in v zvezi s katerimi je bila podana utemeljena zahteva, da se z njimi v celoti ali deloma ravna zaupno.

2. Člani upravnega odbora, izvršni direktor, člani industrijskega in znanstvenega svetovalnega odbora, zunanji strokovnjaki, ki sodelujejo v priložnostnih delovnih skupinah, in člani osebja centra izpolnjujejo zahteve glede zaupnosti iz člena 339 Pogodbe o delovanju Evropske unije, tudi po prenehanju njihovih nalog.

3. Upravni odbor strokovnega centra sprejme varnostne predpise strokovnega centra po odobritvi Komisije na podlagi načel in pravil, določenih v varnostnih predpisih Komisije za varovanje tajnih podatkov Evropske unije (EUCI) in občutljivih netajnih podatkov, vključno z določbami za obdelavo in shranjevanje teh informacij, kot je določeno v sklepih Komisije (EU, Euratom) 2015/443[33] in 2015/444[34].

4. Agencija lahko sprejme vse potrebne ukrepe za olajšanje izmenjave informacij, pomembnih za njene naloge, s Komisijo in državami članicami ter po potrebi z ustreznimi agencijami in organi Unije. Komisija mora predhodno odobriti vsako upravno ureditev o izmenjavi tajnih podatkov EU, sklenjeno v ta namen, ali če take ureditve ni, vsako izjemno priložnostno posredovanje tajnih podatkov EU.

Člen 37

Dostop do dokumentov

1. Za dokumente, ki jih ima v posesti strokovni center, se uporablja Uredba (ES) št. 1049/2001.

2. Upravni odbor v šestih mesecih po ustanovitvi strokovnega centra sprejme ukrepe za izvajanje Uredbe (ES) št. 1049/2001.

3. Sklepi, ki jih sprejme strokovni center na podlagi člena 8 Uredbe (ES) št. 1049/2001, so lahko predmet pritožbe varuhu človekovih pravic na podlagi člena 228 Pogodbe o delovanju Evropske unije ali tožbe pred Sodiščem Evropske unije v skladu na podlagi člena 263 Pogodbe o delovanju Evropske unije.

---

[33] Sklep Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji (UL L 72, 17.3.2015, str. 41).

[34] Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72, 17.3.2015, str. 53).

Člen 38

Spremljanje, vrednotenje in pregled

1. Strokovni center zagotovi, da se njegove dejavnosti, zlasti tiste, ki se upravljajo prek nacionalnih koordinacijskih centrov in mreže, stalno in sistematično spremljajo ter redno vrednotijo. Strokovni center zagotovi, da se podatki za spremljanje izvajanja programa in rezultatov zberejo učinkovito, uspešno in pravočasno ter da so prejemnikom sredstev Unije in državam članicam naložene sorazmerne obveznosti glede poročanja. Rezultati vrednotenja se objavijo.
2. Ko je na voljo dovolj informacij o izvajanju te uredbe, vendar najpozneje tri leta in pol po začetku njenega izvajanja, Komisija opravi vmesno vrednotenje strokovnega centra. Komisija pripravi poročilo o tem vrednotenju in ga predloži Evropskemu parlamentu in Svetu do 31. decembra 2024. Strokovni center in države članice Komisiji zagotovijo informacije, potrebne za pripravo navedenega poročila.
3. Vrednotenje iz odstavka 2 vključuje oceno rezultatov, ki jih je dosegel strokovni center glede na njegove cilje, mandat in naloge. Če Komisija meni, da je nadaljnje delovanje strokovnega centra upravičeno glede na njegove dodeljene cilje, pooblastila in naloge, lahko predlaga podaljšanje mandata strokovnega centra iz člena 46.
4. Komisija lahko na podlagi ugotovitev vmesnega vrednotenja iz odstavka 2 ukrepa v skladu s [členom 22(5)] ali sprejme katere koli druge ustrezne ukrepe.
5. Pri spremljanju, vrednotenju, postopnem ukinjanju in podaljševanju prispevka iz Obzorja Evropa se bodo upoštevale določbe členov 8, 45 in 47 ter Priloge III uredbe o programu Obzorje Evropa ter dogovorjeni načini izvajanja.
6. Spremljanje, poročanje in vrednotenje prispevka programa za digitalno Evropo se bo izvajalo skladno z določbami členov 24 in 25 programa za digitalno Evropo.
7. V primeru prenehanja strokovnega centra Komisija opravi končno vrednotenje strokovnega centra v šestih mesecih po prenehanju, vendar najpozneje v dveh letih po sprožitvi postopka prenehanja iz člena 46 te uredbe. Rezultati tega končnega vrednotenja se predložijo Evropskemu parlamentu in Svetu.

Člen 39

Odgovornost strokovnega centra

1. Pogodbeno odgovornost strokovnega centra ureja pravo, ki se uporablja za zadevni sporazum, sklep ali pogodbo.
2. V primeru nepogodbene odgovornosti strokovni center v skladu s splošnimi načeli, ki so skupna pravnim ureditvam držav članic, povrne vso škodo, ki jo je njegovo osebje povzročilo pri opravljanju svojih nalog.
3. Vsako izplačilo strokovnega centra v zvezi z odgovornostjo iz odstavkov 1 in 2 ter s tem povezani stroški in izdatki se štejejo kot odhodki strokovnega centra in se krijejo iz njegovih sredstev.
4. Strokovni center je izključno odgovoren za izpolnjevanje svojih obveznosti.

Člen 40

Pristojnost Sodišča Evropske unije in pravo, ki se uporablja

1. Sodišče Evropske unije je pristojno:

   (1) na podlagi arbitražnih klavzul v sporazumih, sklepih ali pogodbah, ki jih sklene strokovni center;

   (2) za spore v zvezi z nadomestilom za škodo, ki jo povzroči osebje strokovnega centra pri opravljanju svojih nalog;

   (3) v vseh sporih med strokovnim centrom in njegovim osebjem v okvirih in pod pogoji, določenimi v Kadrovskih predpisih.

2. Za vse zadeve, ki jih ne ureja ta uredba ali drugi pravni akti Unije, se uporablja pravna ureditev države članice, v kateri je sedež strokovnega centra.

Člen 41

Odgovornost članov in zavarovanje

1. Finančna odgovornost članov za dolgove strokovnega centra je omejena na njihov že vplačani prispevek za upravne stroške.

2. Strokovni center sklene in vzdržuje ustrezno zavarovanje.

Člen 42

Nasprotja interesov

Upravni odbor strokovnega centra sprejme pravila za preprečevanje in obvladovanje nasprotij interesov, ki se uporabljajo za njegove člane, organe in osebje. Navedena pravila vsebujejo določbe, katerih namen je preprečevati nasprotje interesov v zvezi s predstavniki članov, ki so dejavni v upravnem ter znanstvenem in industrijskem svetovalnem odboru v skladu z Uredbo XXX [nova finančna uredba].

Člen 43

Varstvo osebnih podatkov

1. Urad obdeluje osebne podatke v skladu z Uredbo (EU) št. XXX/2018 Evropskega parlamenta in Sveta.

2. Upravni odbor sprejme izvedbene ukrepe iz člena xx(3) Uredbe (EU) št. xxx/2018. Upravni odbor lahko sprejme dodatne ukrepe, ki so potrebni za uporabo Uredbe (EU) št. xxx/2018 s strani strokovnega centra.

Člen 44

Podpora države članice gostiteljice

Strokovni center in država članica [Belgija], v kateri ima sedež, lahko skleneta upravni sporazum o privilegijih in imunitetah ter drugi podpori, ki jo navedena država članica zagotovi strokovnemu centru.

POGLAVJE VII

KONČNE DOLOČBE

Člen 45

Začetni ukrepi

1. Komisija je odgovorna za ustanovitev in začetno delovanje strokovnega centra, dokler ne pridobi ustrezne operativne zmogljivosti za izvrševanje lastnega proračuna. Komisija v skladu s pravom Unije izvaja vse potrebne ukrepe s sodelovanjem pristojnih organov strokovnega centra.

2. Za namen odstavka 1 lahko Komisija imenuje začasnega izvršnega direktorja, ki opravlja naloge, dodeljene izvršnemu direktorju, in ki mu lahko pomaga omejeno število uradnikov Komisije, dokler upravni odbor v skladu s členom 16 ne imenuje izvršnega direktorja in ta ne prevzame svojih nalog. Komisija lahko začasno dodeli omejeno število svojih uradnikov.

3. Začasni izvršni direktor lahko po potrditvi upravnega odbora odobri vsa plačila, krita z odobritvami iz letnega proračuna strokovnega centra, sklepa sporazume in pogodbe ter sprejema sklepe, po sprejetju kadrovskega načrta strokovnega centra pa lahko sklepa tudi pogodbe o zaposlitvi.

4. Začasni izvršni direktor v soglasju z izvršnim direktorjem strokovnega centra in po odobritvi upravnega odbora določi dan, ko strokovni center postane sposoben izvrševati lastni proračun. Komisija od navedenega dne ne prevzema več obveznosti in ne izvršuje plačil za dejavnosti strokovnega centra.

Člen 46

Trajanje

1. Strokovni center se ustanovi za obdobje od 1. januarja 2021 do 31. decembra 2029.

2. Ob koncu tega obdobja, razen če se v pregledu te uredbe ne določi drugače, se sproži postopek prenehanja. Postopek prenehanja se sproži samodejno, če se Unija ali vse sodelujoče države članice umaknejo iz strokovnega centra.

3. Upravni odbor za vodenje postopkov v zvezi s prenehanjem strokovnega centra imenuje enega ali več likvidacijskih upraviteljev, ki ravnajo v skladu s sklepi upravnega odbora.

4. Med postopkom prenehanja strokovnega centra se njegova sredstva porabijo za kritje njegovih obveznosti in odhodkov, povezanih s prenehanjem delovanja. Morebitni presežki se porazdelijo med Unijo in sodelujoče države članice sorazmerno z njihovim finančnim prispevkom za strokovni center. Vsi presežki, ki se dodelijo Uniji, se vrnejo v proračun Unije.

Člen 47

Začetek veljavnosti

Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1 Naslov predloga/pobude

1.2 Zadevna področja v strukturi ABM/ABB

1.3 Vrsta predloga/pobude

1.4 Cilji

1.5 Utemeljitev predloga/pobude

1.6 Trajanje ukrepa in finančnih posledic

1.7 Načrtovani načini upravljanja

2. UKREPI UPRAVLJANJA

2.1 Pravila o spremljanju in poročanju

2.2 Upravljavski in kontrolni sistem

2.3 Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1 Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

3.2 Ocenjene posledice za odhodke

3.2.1 Povzetek ocenjenih posledic za odhodke

3.2.2 Ocenjene posledice za odobritve za poslovanje

3.2.3 Ocenjene posledice za odobritve za upravne zadeve

3.2.4 Skladnost z veljavnim večletnim finančnim okvirom

3.2.5 Udeležba tretjih oseb pri financiranju

3.3 Ocenjene posledice za prihodke

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1 Naslov predloga/pobude

Uredba o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost

1.2 Zadevna področja v strukturi ABM/ABB[35]

Raziskave in inovacije

Evropske strateške naložbe

1.3 Vrsta predloga/pobude

☒Predlog/pobuda se nanaša na **nov ukrep**.

☐Predlog/pobuda se nanaša **na nov ukrep na podlagi pilotnega projekta/ pripravljalnega ukrepa**[36].

☐Predlog/pobuda se nanaša na **podaljšanje obstoječega ukrepa**.

☐Predlog/pobuda se nanaša na **obstoječ ukrep, preusmerjen v nov ukrep**.

1.4 Cilji

1.4.1 Večletni strateški cilji Komisije, ki naj bi bili doseženi s predlogom/pobudo

1. Povezan enotni digitalni trg

2. Nova spodbuda za delovna mesta, rast in naložbe

1.4.2 Zadevni specifični cilji

Specifični cilji

1.3 Digitalno gospodarstvo lahko razvije ves svoj potencial ob podpori pobud, ki omogočajo polno rast digitalnih in podatkovnih tehnologij.

2.1 Evropa ohrani vodilni položaj v digitalnem gospodarstvu, pri čemer imajo evropska podjetja možnost za globalno rast, opirajoč se na močno razvito digitalno podjetništvo in uspešna zagonska podjetja, industrija in javne službe pa obvladajo digitalno preobrazbo.

2.2 Evropske raziskave so deležne naložbenih priložnosti za potencialne tehnološke prebojne inovacije in vodilne pobude, zlasti v okviru programa Obzorje 2020/Obzorje Evropa ter z izkoriščanjem javno-zasebnih partnerstev.

[35] ABM: upravljanje po dejavnostih, ABB: oblikovanje proračuna po dejavnostih.

[36] Po členu 54(2)(a) oz. (b) finančne uredbe.

1.4.3 Pričakovani rezultati in posledice

Navedite, kakšne posledice naj bi imel(-a) predlog/pobuda za upravičence/ciljne skupine.

Strokovni center si bo skupaj z mrežo in skupnostjo prizadeval doseči naslednje cilje:

(1) prispevati k izvajanju kibernetskovarnostnega dela programa za digitalno Evropo, vzpostavljenega z Uredbo št. XXX, in zlasti ukrepov v povezavi s členom 6 Uredbe (EU) št. XXX [program za digitalno Evropo], ter programa Obzorje Evropa, vzpostavljenega z Uredbo št. XXX, in zlasti oddelka 2.2.6 Priloge I k Sklepu št. XXX o vzpostavitvi posebnega programa za izvajanje okvirnega programa za raziskave in inovacije Obzorje Evropa, ter drugih programov Unije, če je tako določeno v pravnih aktih Unije;

(2) okrepiti zmogljivosti, znanje in infrastrukturo na področju kibernetske varnosti v korist različnim panogam, javnemu sektorju in raziskovalnim skupnostim;

(3) prispevati k širšemu uvajanju najsodobnejših izdelkov in rešitev za kibernetsko varnost v celotnem gospodarstvu;

(4) izboljšati razumevanje kibernetske varnosti in prispevati k zmanjšanju vrzeli v spretnostih v Uniji na področju kibernetske varnosti;

(5) prispevati k okrepitvi raziskav in razvoja na področju kibernetske varnosti v Uniji;

(6) olajšati sodelovanje med civilnim in obrambnim sektorjem v zvezi s tehnologijami in aplikacijami z dvojno rabo;

(7) okrepiti sinergije med civilnimi in obrambnimi razsežnostmi kibernetske varnosti;

(8) pomagati usklajevati in lajšati delo mreže nacionalnih koordinacijskih centrov iz člena 10 in strokovne skupnosti za kibernetsko varnost iz člena 12.

1.4.4 Kazalniki rezultatov in posledic

Navedite, s katerimi kazalniki se bo spremljalo izvajanje predloga/pobude.

· Število skupno naročene infrastrukture/orodij za kibernetsko varnost.

· Omogočen dostop do priložnosti za preizkušanje in eksperimentiranje za evropske raziskovalce in industrijo po celotni mreži in v centru. Če zmogljivosti že obstajajo, se tem skupnostim v primerjavi s trenutno razpoložljivimi urami da na voljo več časa.

· Število uporabniških skupnosti, ki so jim zagotovljene storitve, in število znanstvenikov, ki dobijo dostop do evropskih zmogljivosti za kibernetsko varnost, se v primerjavi s številom znanstvenikov, ki morajo vire iskati zunaj Evropa, poveča.

· Konkurenčnost evropskih dobaviteljev, merjena kot svetovni tržni delež (cilj je 25-odstotni tržni delež do leta 2027) ter delež rezultatov evropskih raziskav in razvoja, ki jih sprejme industrija, se poveča.

· Prispevek k naslednji generaciji tehnologije za kibernetsko varnost, merjen v smislu patentov, znanstvenih publikacij in tržnih proizvodov.

· Število ocenjenih in usklajenih izobraževalnih načrtov s področja kibernetske varnosti, število ocenjenih programov za pridobitev spričevala o strokovni usposobljenosti na področju kibernetske varnosti.

· Število usposobljenih znanstvenikov, študentov, uporabnikov (v industriji in javnih upravah).

1.5 Utemeljitev predloga/pobude

1.5.1 Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno

Doseči kritično maso naložb v tehnološki in industrijski razvoj na področju kibernetske varnosti ter odpraviti razdrobljenost zadevnih zmogljivosti po vsej EU.

1.5.2 Dodana vrednost ukrepanja EU

Kibernetska varnost je vprašanje skupnega interesa Unije, kot potrjujejo zgoraj navedeni sklepi Sveta. Obseg in čezmejni značaj incidentov, kot sta WannaCry ali NonPetya, sta tipičen primer. Zaradi narave in obsega tehnoloških izzivov kibernetske varnosti ter nezadostnega usklajevanja prizadevanj znotraj panoge, javnega sektorja in raziskovalnih skupnosti ter med njimi mora EU še naprej podpirati prizadevanja za usklajevanje, da bi združili kritično maso virov in zagotovili boljše upravljanje znanja in premoženja. To je potrebno glede na potrebe po virih, povezane z določenimi zmogljivostmi za raziskave, razvoj in uporabo kibernetske varnosti; potrebo po zagotavljanju dostopa do interdisciplinarnega strokovnega znanja in izkušenj na področju kibernetske varnosti na različnih področjih (ki je na nacionalni ravni pogosto le delno na voljo); globalno naravo industrijskih vrednostnih verig in dejavnost svetovnih konkurentov, ki nastopajo na trgih.

Za to so potrebni viri in strokovno znanje v obsegu, ki ga posamezni ukrepi katere koli države članice težko dosežejo. Na primer, vseevropska mreža za kvantne komunikacije bi lahko zahtevala naložbe EU v višini približno 900 milijonov EUR, odvisno od naložb držav članic (ki bodo medsebojno povezane/dopolnjene) in od tega, v kolikšni meri bo tehnologija omogočila ponovno uporabo obstoječe infrastrukture.

1.5.3 Spoznanja iz podobnih izkušenj v preteklosti

Vmesna ocena programa Obzorje 2020 je med drugim potrdila, da je podpora EU še vedno pomembna za raziskave in razvoj ter obravnavanje družbenih izzivov (med drugim „varne družbe“, v okviru katerih je zagotovljena podpora za raziskave in razvoj na področju kibernetske varnosti). Hkrati je ocena potrdila, da utrditev vodilnega položaja industrije ostaja izziv in da še vedno obstaja vrzel v inovacijah, saj EU zaostaja na področju prodornih inovacij, ki oblikujejo trg.

Zdi se, da vmesna ocena Instrumenta za povezovanje Evrope potrjuje dodano vrednost ukrepanja EU tudi na področjih, ki presegajo raziskave in razvoj, vendar pa sta bila poudarek (na operativni varnosti) in logika ukrepanja na področju kibernetske varnosti v okviru IPE nekoliko drugačna. Hkrati je večina prejemnikov nepovratnih sredstev za kibernetsko varnost v okviru IPE (skupnost nacionalnih skupin CSIRT) izrazila željo po prilagojenem programu podpore v okviru naslednjega večletnega finančnega okvira.

Vzpostavitev javno-zasebnega partnerstva za kibernetsko varnost v EU leta 2016 je bil trden prvi korak k povezovanju skupnosti na področju raziskav, industrije in javnega sektorja za spodbujanje raziskav in inovacij na področju kibernetske varnosti, ki bi v okviru omejitev finančnega okvira za obdobje 2014–2020 moral zagotoviti dobre in bolj osredotočene rezultate na področju raziskav in inovacij.

Javno-zasebno partnerstvo za kibernetsko varnost je industrijskim partnerjem omogočilo, da so izrazili zavezo o njihovi individualni porabi za področja, opredeljena v strateškem programu partnerstva za raziskave in inovacije.

1.5.4 Skladnost in možnosti sinergij z drugimi ustreznimi instrumenti

Strokovna mreža za kibernetsko varnost ter Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost bosta delovala kot dodatna podpora obstoječim določbam in akterjem na področju politik kibernetske varnosti. Pooblastila Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost bo dopolnjevala prizadevanja agencije ENISA, vendar se osredotoča na različna področja in zahteva drugačen sklop znanj in spretnosti. Medtem ko je v mandatu agencije ENISA predvidena svetovalna vloga glede raziskav in inovacij na področju kibernetske varnosti v EU, se njen predlagani mandat osredotoča predvsem na druge naloge, ki so ključne za krepitev odpornosti kibernetske varnosti v EU. Center bi moral spodbujati razvoj in uvajanje tehnologije na področju kibernetske varnosti ter dopolnjevati prizadevanja za krepitev zmogljivosti na tem področju na ravni EU in nacionalni ravni.

Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost in strokovna mreža za kibernetsko varnost bosta sodelovala tudi pri podpiranju raziskav, da se omogočijo in pospešijo postopki standardizacije in certificiranja, zlasti tisti, ki se nanašajo na certifikacijske sheme za kibernetsko varnost v smislu akta o kibernetski varnosti.

Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost bo deloval kot enoten izvedbeni mehanizem za dva evropska programa, ki podpirata kibernetsko varnost (program za digitalno Evropo in program Obzorje Evropa), ter povečal skladnost in sinergijske učinke med njima.

Ta pobuda omogoča dopolnjevanje prizadevanj držav članic z zagotavljanjem ustreznega prispevka oblikovalcem politik na področju izobraževanja, da se okrepi izobrazba na področju kibernetske varnosti (npr. z razvojem izobraževalnih načrtov za kibernetsko varnost v civilnih in vojaških izobraževalnih sistemih, pa tudi s prispevanjem k osnovni izobrazbi na področju kibernetske varnosti). Prav tako bi omogočila uskladitev in redno ocenjevanje programov za pridobitev spričeval o strokovni usposobljenosti na področju kibernetske varnost, kar je potrebno, da se zapolni vrzel v spretnostih na tem področju in olajša dostop panog in drugih skupnosti do specialistov za kibernetsko varnost. Uskladitev izobraževanja in spretnosti po pomagala pri razvoju usposobljene delovne sile na področju kibernetske varnosti – ključne prednosti za podjetja na tem področju ter druge industrije, ki so na njem udeležene.

1.6 Trajanje ukrepa in finančnih posledic

☒ **Časovno omejen(-a)** predlog/pobuda:

– ☒ trajanje predloga/pobude od 1. 1. 2021 do 31. 12. 2029,

– ☒ finančne posledice med letoma 2021 in 2027 za odobritve za prevzem obveznosti ter med letoma 2021 in 2031 za odobritve plačil.

☐ **Časovno neomejen(-a)** predlog/pobuda:

– izvajanje z obdobjem uvajanja med letoma LLLL in LLLL,

– ki mu sledi izvajanje predloga/pobude v celoti.

1.7 Načrtovani načini upravljanja[37]

☐ **Neposredno upravljanje** – Komisija:

– ☐ z lastnimi službami, vključno z zaposlenimi v delegacijah Unije,

– ☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☒

Posredno upravljanje s poverjanjem nalog izvrševanja proračuna:

– ☐ tretjim državam ali organom, ki jih te imenujejo,

– ☐ mednarodnim organizacijam in njihovim agencijam (navedite),

– ☐ EIB in Evropskemu investicijskemu skladu,

– ☒ organom iz členov 70 in 71 finančne uredbe,

– ☐ subjektom javnega prava,

– ☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

– ☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

– ☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP v skladu z naslovom V PEU in opredeljenim v zadevnem temeljnem aktu.

– *Pri navedbi več kot enega načina upravljanja je treba to natančneje obrazložiti v oddelku „opombe“.*

[37] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. UKREPI UPRAVLJANJA

2.1 Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Člen 28 vsebuje podrobne določbe o spremljanju in poročanju.

2.2 Upravljavski in kontrolni sistem

2.2.1 Ugotovljena tveganja

Za ublažitev tveganj, povezanih z delovanjem strokovnega centra po njegovi vzpostavitvi, in za zmanjšanje zamud bo Komisija v tej fazi podpirala strokovni center, da bi zagotovila hitro zaposlitev ključnega osebja in vzpostavitev učinkovitega sistema notranje kontrole ter zanesljivih postopkov.

2.2.2 Podatki o vzpostavljenem sistemu notranje kontrole

Izvršni direktor je odgovoren za operacije in dnevno vodenje strokovnega centra ter je njegov zakoniti zastopnik. Direktor odgovarja upravnemu odboru in mu redno poroča o poteku dejavnosti strokovnega centra.

Upravni odbor je v celoti odgovoren za strateško usmerjanje in delovanje strokovnega centra ter nadzira izvajanje njegovih dejavnosti.

Upravni odbor po posvetovanju s Komisijo sprejme finančna pravila, ki se uporabljajo za strokovni center. Pravila ne odstopajo od Uredbe (EU) št. 1271/2013, razen če je tako odstopanje posebej potrebno za delovanje strokovnega centra in je Komisija dala predhodno soglasje.

Notranji revizor Komisije ima v zvezi s strokovnim centrom enaka pooblastila, kot jih ima v zvezi s Komisijo. Evropsko računsko sodišče ima pooblastilo za opravljanje revizij na podlagi dokumentov in na kraju samem pri vseh prejemnikih nepovratnih sredstev, izvajalcih in podizvajalcih, ki so od strokovnega centra prejeli sredstva Unije.

2.2.3 Ocena stroškov in koristi kontrol ter ocena pričakovane stopnje tveganja napak

Stroški in koristi kontrol

Stroški kontrol za Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost so razdeljeni med stroške nadzora na ravni Komisije in stroške operativnih kontrol na ravni izvajalskega organa.

Stroški kontrol na ravni strokovnega centra so ocenjeni na približno 1,19 % operativnih odobritev plačil, izvedenih na ravni strokovnega centra.

Stroški nadzora na ravni Komisije so ocenjeni na približno 1,20 % operativnih odobritev plačil, izvedenih na ravni strokovnega centra.

Ob predpostavki, da bi dejavnosti v celoti upravljala Komisija brez podpore izvajalskega organa, bi bili stroški kontrol znatno višji in bi lahko znašali približno 7,7 % odobritev plačil.

Namen predvidenih kontrol je zagotoviti gladek in učinkovit nadzor Komisije nad subjekti izvajanja in zagotoviti potrebno stopnjo gotovosti na ravni Komisije.

Koristi kontrol so naslednje:

- izognitev slabšim ali neustreznim predlogom,
- optimizacija načrtovanja in izrabe sredstev EU za ohranitev dodane vrednosti EU,
- zagotavljanje kakovosti sporazumov o dodelitvi nepovratnih sredstev, izogibanje napakam pri ugotavljanju istovetnosti pravnih oseb, zagotavljanje pravilnega izračuna prispevkov EU in sprejem potrebnih poroštev za pravilno delovanje nepovratnih sredstev,
- odkrivanje neupravičenih stroškov v fazi plačila,
- odkrivanje napak, ki vplivajo na zakonitost in pravilnost postopkov v fazi revizije.

Ocenjena stopnja napak

Cilj je ohraniti stopnjo napak ob zaključku pod pragom 2 % za celoten program ter ob tem omejiti breme kontrol, da lahko upravičenci dosežejo pravilno ravnovesje med ciljem zakonitosti in pravilnosti ter drugimi cilji, kot je privlačnost programa, zlasti za MSP, in strošek kontrol.

2.3 Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe.

OLAF lahko izvaja preiskave, vključno s pregledi in inšpekcijami na kraju samem, v skladu z določbami in postopki iz Uredbe št. 883/2013 Evropskega parlamenta in Sveta ter Uredbe Sveta (Euratom, ES) št. 2185/96 z dne 11. novembra 1996 o pregledih in inšpekcijah na kraju samem, ki jih opravlja Komisija za zaščito finančnih interesov Evropskih skupnosti pred goljufijami in drugimi nepravilnostmi, da bi ugotovil, ali je prišlo do goljufije, korupcije ali katere koli nezakonite dejavnosti, ki vpliva na finančne interese Unije v povezavi z nepovratnimi sredstvi ali pogodbo, ki jo je financiral strokovni center.

Sporazumi, sklepi in pogodbe, ki izhajajo iz izvajanja te uredbe, vsebujejo določbe, ki Komisijo, strokovni center, Računsko sodišče in urad OLAF izrecno pooblaščajo, da izvedejo revizije in preiskave v skladu s svojimi pristojnostmi.

Strokovni center z izvajanjem ali naročanjem ustreznega notranjega in zunanjega nadzora zagotovi, da so finančni interesi njegovih članic ustrezno zaščiteni.

Strokovni center pristopi k Medinstitucionalnemu sporazumu z dne 25. maja 1999 med Evropskim parlamentom, Svetom Evropske unije in Komisijo Evropskih skupnosti o notranjih preiskavah Evropskega urada za boj proti goljufijam (OLAF). Sprejme potrebne ukrepe za olajšanje notranjih preiskav, ki jih izvaja urad OLAF.

Strokovni center bo na podlagi analize tveganja goljufij in ob upoštevanju stroškov in koristi sprejel strategijo za boj proti goljufijam. Strokovni center zaščiti finančne interese Unije s preventivnimi ukrepi proti goljufijam, korupciji in kakršnim koli drugim nezakonitim dejavnostim, z izvajanjem učinkovitih pregledov in, če so ugotovljene nepravilnosti, z izterjavo neupravičeno plačanih zneskov ter z

učinkovitimi, sorazmernimi in odvračilnimi upravnimi in finančnimi kaznimi, kjer je to ustrezno.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1 Predlagani razdelek večletnega finančnega okvira in nove odhodkovne proračunske vrstice

- Zahtevane nove proračunske vrstice

  Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic:

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	Številka	dif./nedif.[38]	držav Efte[39]	držav kandidatk[40]	tretjih držav	po členu [21(2)(b)] finančne uredbe
Razdelek 1: Enotni trg, inovacije in digitalno	01 02 XX XX Obzorje Evropa Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost – odhodki za podporo 01 02 XX XX Obzorje Evropa Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost 02 06 01 XX Program za digitalno Evropo Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost – odhodki za podporo 02 06 01 XX Program za digitalno Evropo Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost	dif.	DA	DA (če je določeno v letnem programu dela)	DA (omejeno ne nekatere dela programa)	NE

- Pričakuje se, da se bodo prispevki za te proračunske vrstice zagotovili iz:

[38] Dif. = diferencirana sredstva/ nedif. = nediferencirana sredstva.

[39] Efta: Evropsko združenje za prosto trgovino.

[40] Države kandidatke in, kjer je ustrezno, potencialne kandidatke z Zahodnega Balkana.

v mio. EUR (na tri decimalna mesta natančno)

Proračunska vrstica	Leto 2021	Leto 2022	Leto 2023	Leto 2024	Leto 2025	Leto 2026	Leto 2027	**Skupaj**
01 01 01 01 Stroški, povezani z začasnimi uslužbenci za raziskave – Obzorje Evropa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 02 Zunanji sodelavci, ki izvajajo raziskovalne programe – Obzorje Evropa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 01 01 03 Drugi odhodki za upravljanje pri raziskavah – Obzorje Evropa	pm	pm	pm	pm	pm	pm	pm	**pm**
01 02 02 Globalni izzivi in industrijska konkurenčnost	pm	pm	pm	pm	pm	pm	pm	**pm**
02 01 04 Upravna podpora – program za digitalno Evropo	1,238	3,030	3,743	3,818	3,894	3,972	4,051	**23,746**
02 06 01 Kibernetska varnost – program za digitalno Evropo	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Odhodki skupaj	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Prispevek iz finančnih sredstev sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 21(1)(b) bo Komisija predlagala v zakonodajnem postopku, vsekakor pa pred političnim dogovorom. Predlog bo temeljil na izidu postopka strateškega načrtovanja, kot je opredeljen v členu 6(6) Uredbe XXX [okvirni program Obzorje Evropa].

Navedeni zneski ne vključujejo prispevka držav članic k operativnim in upravnim stroškom strokovnega centra, sorazmernega s finančnim prispevkom Unije.

3.2 Ocenjene posledice za odhodke

3.2.1 Povzetek ocenjenih posledic za odhodke

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	**1**	Enotni trg, inovacije in digitalno

			2021[41]	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po letu 2027***	**SKUPAJ**
Naslov 1 (odhodki za zaposlene)	obveznosti = plačila	(1)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Naslov 2 (infrastruktura in odhodki za poslovanje)	obveznosti = plačila	(2)	0,619	1,515	1,871	1,909	1,947	1,986	2,026		**11,873**
Naslov 3 (odhodki za poslovanje)	obveznosti	(3)	284,892	322,244	327,578	248,382	253,295	258,214	263,316		**1 957,922**
	plačila	(4)	21,221	102,765	150,212	167,336	156,475	150,124	148,074	1 061,715	**1 957,922**
Odobritve za sredstva programov SKUPAJ[42]	obveznosti	=1+2+3	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**		**1 981,668**
	plačila	=1+2+4	**22,459**	**105,795**	**153,954**	**171,154**	**160,369**	**154,096**	**152,126**	**1 061,715**	**1 981,668**

41 Odobritve za zaposlene v letu 2021 so izračunane samo za pol leta

42 Določene skupne odobritve se nanašajo samo na finančna sredstva EU, namenjena kibernetski varnosti v okviru programa za digitalno Evropo. Prispevek iz finančnih sredstev sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 5(1)(b) bo Komisija predlagala v zakonodajnem postopku, vsekakor pa pred političnim dogovorom. Predlog bo temeljil na izidu postopka strateškega načrtovanja, kot je opredeljen v členu 6(6) Uredbe XXX [okvirni program Obzorje Evropa].

Razdelek večletnega finančnega okvira	7	„Upravni odhodki“

v mio. EUR (na tri decimalna mesta natančno)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po letu 2027***	**SKUPAJ**
Človeški viri		3,090	3,233	3,233	3,233	3,233	3,233	3,805		**23,060**
Drugi upravni odhodki		0,105	0,100	0,104	0,141	0,147	0,153	0,159		**0,909**
Odobritve iz RAZDELKA 7 večletnega finančnega okvira SKUPAJ	(obveznosti skupaj = plačila skupaj)	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**		**23,969**

v mio. EUR (na tri decimalna mesta natančno)

		2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**	***Po letu 2027***	**SKUPAJ**
Odobritve iz vseh RAZDELKOV večletnega finančnega okvira SKUPAJ	obveznosti	**289,325**	**328,607**	**334,657**	**255,574**	**260,569**	**265,572**	**271,332**		**2 005,637**
	plačila	**25,654**	**109,128**	**157,291**	**174,528**	**163,749**	**157,482**	**156,090**	**1 061,715**	**2 005,637**

3.2.2 Povzetek ocenjenih posledic za odobritve za upravne zadeve

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– ☒ Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

Leto	2021	2022	2023	2024	2025	2026	2027	SKUPAJ
RAZDELEK 7 večletnega finančnega okvira								
Človeški viri	3,090	3,233	3,233	3,233	3,233	3,233	3,805	**23,060**
Drugi upravni odhodki	0,105	0,100	0,104	0,141	0,147	0,153	0,159	**0,909**
Seštevek za RAZDELEK 7 večletnega finančnega okvira	**3,195**	**3,333**	**3,337**	**3,374**	**3,380**	**3,386**	**3,964**	**23,969**

Zunaj RAZDELKA 7[43] večletnega finančnega okvira								
Človeški viri								
Drugi odhodki upravnega značaja	1,238	3,030	3,743	3,818	3,894	3,972	4,051	23,746
Seštevek za odobritve zunaj RAZDELKA 7 večletnega finančnega okvira	**1,238**	**3,030**	**3,743**	**3,818**	**3,894**	**3,972**	**4,051**	**23,746**

SKUPAJ	**4,433**	**6,363**	**7,079**	**7,192**	**7,274**	**7,358**	**8,016**	**47,715**

Potrebe po odobritvah za človeške vire in druge upravne odhodke se krijejo z odobritvami GD, ki so že dodeljene za upravljanje ukrepa in/ali so bile prerazporejene znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v okviru postopka letne dodelitve virov glede na proračunske omejitve.

Potrebe po odobritvah za človeške vire in druge upravne odhodke zunaj razdelka 7 ustrezajo zneskom, kritim s finančnim prispevkom Unije iz programa za digitalno Evropo.

Potrebe po odobritvah za človeške vire in druge upravne odhodke zunaj razdelka 7 se bodo povečale za zneske, krite s finančnim prispevkom Unije iz programa Obzorje Evropa, ko bo Komisija v zakonodajnem postopku, vsekakor pa pred političnim dogovorom, predlagala prispevek iz finančnih sredstev sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 21(1)(b).

[43] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

Navedeni zneski potrebnih odobritev za človeške vire in druge upravne odhodke zunaj razdelka 7 ne vključujejo prispevka držav članic k upravnim stroškom strokovnega centra, sorazmernega s finančnim prispevkom Unije.

3.2.2.1 Ocenjene potrebe po človeških virih v Komisiji

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– ■ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v ekvivalentu polnega delovnega časa

Leto		**2021**	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
• Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)								
Sedež in predstavništva Komisije		20	21	21	21	21	21	22
Delegacije								
Raziskave								
• Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ) – PU, LU, NNS, ZU in MSD [44] Razdelek 7								
Financirano iz RAZDELKA 7 večletnega finančnega okvira	– na sedežu	3	3	3	3	3	3	3
	– na delegacijah							
Financirano iz sredstev programa [45]	– na sedežu							
	– na delegacijah							
Raziskave								
Drugo (navedite)								
SKUPAJ		**23**	**23**	**24**	**24**	**24**	**25**	**25**

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v okviru postopka letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	Usklajevanje, spremljanje in usmerjanje nalog, zaupanih Evropskemu industrijskemu, tehnološkemu in raziskovalnemu strokovnemu centru za kibernetsko varnost, vključno s stroški za podporo in usklajevanje. Oblikovanje in usklajevanje politike na področju kibernetske varnosti v povezavi z nalogami, zaupanimi Evropskemu industrijskemu, tehnološkemu in raziskovalnemu strokovnemu centru za kibernetsko varnost, npr. v zvezi z določanjem prednostnih nalog za raziskave in industrijsko politiko, splošnim sodelovanjem med državami članicami in gospodarskimi subjekti, skladnostjo s prihodnjim certifikacijskim okvirom EU za kibernetsko varnost, prevzemanjem odgovornosti in dolžnosti skrbnega ravnanja ali usklajevanjem s politikami na področju visokozmogljivostnega računalništva, umetne inteligence in digitalnih spretnosti. .
Zunanji sodelavci	Usklajevanje, spremljanje in usmerjanje nalog, zaupanih Evropskemu industrijskemu, tehnološkemu in raziskovalnemu strokovnemu centru za kibernetsko varnost, vključno s stroški za podporo in usklajevanje. Oblikovanje in usklajevanje politike na področju kibernetske varnosti v povezavi z nalogami, zaupanimi Evropskemu industrijskemu, tehnološkemu in raziskovalnemu strokovnemu centru za kibernetsko varnost, npr. v zvezi z določanjem prednostnih nalog za raziskave in industrijsko politiko, splošnim sodelovanjem med državami članicami in

[44] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

[45] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

	gospodarskimi subjekti, skladnostjo s prihodnjim certifikacijskim okvirom EU za kibernetsko varnost, prevzemanjem odgovornosti in dolžnosti skrbnega ravnanja ali usklajevanjem s politikami na področju visokozmogljivostnega računalništva, umetne inteligence in digitalnih spretnosti. .

3.2.2.2 Ocenjene potrebe po človeških virih v Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost

	2021	2022	2023	2024	2025	2026	2027
Uradniki Komisije							
od tega AD							
od tega AST							
od tega AST-SC							
Začasni uslužbenci							
od tega AD	10	11	13	13	13	13	13
od tega AST							
od tega AST-SC							
Pogodbeni uslužbenci	26	32	39	39	39	39	39
Napoteni nacionalni strokovnjaki	1	1	1	1	1	1	1
Skupaj	**37**	**44**	**53**	**53**	**53**	**53**	**53**

Opis nalog:

Uradniki in začasni uslužbenci	Operativno izvajanje nalog, zaupanih Evropskemu industrijskemu, tehnološkemu in raziskovalnemu strokovnemu centru za kibernetsko varnost v skladu s členom 4 te uredbe, vključno s stroški podpore in usklajevanja.
Zunanji sodelavci	Operativno izvajanje nalog, zaupanih Evropskemu industrijskemu, tehnološkemu in raziskovalnemu strokovnemu centru za kibernetsko varnost v skladu s členom 4 te uredbe, vključno s stroški podpore in usklajevanja.

Navedene ocenjene potrebe po človeških virih v Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost ustrezajo ocenjenim potrebam za izvrševanje finančnega prispevka Unije v okviru programa za digitalno Evropo.

Navedene ocenjene potrebe po človeških virih v Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost se bodo povečale za ocenjene potrebe za izvrševanje finančnega prispevka Unije v okviru programa Obzorje Evropa, ko bo Komisija v zakonodajnem postopku, vsekakor pa pred političnim dogovorom, predlagala prispevek iz finančnih sredstev sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 21(1)(b).

3.2.2.3 Kadrovski načrt za Evropski industrijski, tehnološki in raziskovalni strokovni center za kibernetsko varnost

Funkcionalna skupina in razred	2021	2022	2023	2024	2025	2025	2025
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
Skupaj AD	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							
Skupaj AST							
AST/SC 6							
AST/SC 5							
AST/SC 4							
AST/SC 3							
AST/SC 2							
AST/SC 1							

Skupaj AST/SC							
VSE SKUPAJ	**10**	**11**	**13**	**13**	**13**	**13**	**13**

3.2.2.4 Ocenjene posledice za uslužbence (dodatne) – zunanji sodelavci Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost

Pogodbeni uslužbenci	2021	2022	2023	2024	2025	2026	2027
Funkcionalna skupina IV	20	22	29	29	29	29	29
Funkcionalna skupina III	2	4	4	4	4	4	4
Funkcionalna skupina II	4	6	6	6	6	6	6
Funkcionalna skupina I							
Skupaj	**26**	**32**	**39**	**39**	**39**	**39**	**39**

Za zagotovitev nevtralnosti števila zaposlenih bo dodatno osebje v Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost delno izravnano z zmanjšanjem števila uradnikov in zunanjih sodelavcev (tj. trenutni kadrovski načrt in zunanji sodelavci) v zadevnih službah Komisije.
Izravnava števila uslužbencev Evropskega industrijskega, tehnološkega in raziskovalnega strokovnega centra za kibernetsko varnost iz točk 3.2.2.2–4[46]:

SKUPAJ	2021	2022	2023	2024	2025	2026	2027
Uradniki Komisije	5	5	6	6	6	6	6
Začasni uslužbenci							
Pogodbeni uslužbenci	14	17	20	20	20	20	20
Napoteni nacionalni strokovnjaki							
EPDČ skupaj	19	22	26	26	26	26	26
Število zaposlenih	19	22	26	26	26	26	26

Izravnava človeških virov v Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost bo sorazmerna z deležem finančnega prispevka Unije, tj. 50 %.

[46] Glede na končni znesek proračuna, katerega izvajanje bo zaupano strokovnemu centru.

Navedena izravnava se nanaša na ocenjene potrebe po človeških virih v Evropskem industrijskem, tehnološkem in raziskovalnem strokovnem centru za kibernetsko varnost za izvrševanje finančnega prispevka Unije v okviru programa za digitalno Evropo.

Navedena izravnava se bo povečala z ocenjenimi potrebami po izvrševanju finančnega prispevka Unije v okviru programa Obzorje Evropa, ko bo Komisija v zakonodajnem postopku, vsekakor pa pred političnim dogovorom, predlagala prispevek iz finančnih sredstev sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 21(1)(b).

3.2.3 Udeležba tretjih oseb pri financiranju

V predlogu/pobudi:

– ☐ ni načrtovano sofinanciranje tretjih oseb.

– ☒ je načrtovano sofinanciranje tretjih oseb[47], kot je ocenjeno v nadaljevanju:

odobritve v mio. EUR (na tri decimalna mesta natančno)

Leto	2021	2022	2023	2024	2025	2026	2027	SKUPAJ
Države članice – prispevek k odhodkom za zaposlene	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Države članice – prispevek k infrastrukturi in operativnim odhodkom	0,619	1,515	1,871	1,909	1,947	1,986	2,026	**11,873**
Države članice – prispevek k odhodkom za poslovanje	284,892	322,244	327,578	248,382	253,295	258,214	263,316	**1 957,922**
Sofinancirane odobritve SKUPAJ	**286,130**	**325,274**	**331,320**	**252,200**	**257,189**	**262,186**	**267,368**	**1 981,668**

Navedeni prispevki tretjih strani se nanašajo samo na sofinanciranje, sorazmerno s finančnimi sredstvi EU, namenjenimi za kibernetsko varnost v okviru programa za digitalno Evropo. Navedeni prispevek tretjih strani se bo povečal, ko bo Komisija v zakonodajnem postopku, vsekakor pa pred političnim dogovorom, predlagala finančni prispevek sklopa „Vključujoča in varna družba“ v okviru stebra II „Globalni izzivi in industrijska konkurenčnost“ programa Obzorje Evropa (skupna sredstva v višini 2 800 000 000 EUR) iz člena 21(1)(b). Predlog bo temeljil na izidu postopka strateškega načrtovanja, kot je opredeljen v členu 6(6) Uredbe XXX [okvirni program Obzorje Evropa].

3.3 Ocenjene posledice za prihodke

– ☒ Predlog/pobuda nima finančnih posledic za prihodke.

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

☐ za lastna sredstva,

☐ za druge prihodke.

navedite, ali so prihodki dodeljeni za odhodkovne vrstice: ☐

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Posledice predloga/pobude[48]						
	2021	**2022**	**2023**	**2024**	**2025**	**2026**	**2027**
Člen …….							

[47] Ocenjeni prispevek v naravi s strani držav članic

[48] Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.

Za namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

Druge opombe (npr. metoda/formula za izračun posledic za prihodke ali druge informacije).