Svet
Evropske unije

Bruselj, 20. april 2023
(OR. en)

8512/23

Medinstitucionalna zadeva:
2023/0109 (COD)

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

PREDLOG

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	19. april 2023
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2023) 209 final
Zadeva:	Predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje

Delegacije prejmejo priloženi dokument COM(2023) 209 final.

Priloga: COM(2023) 209 final

EVROPSKA
KOMISIJA

Strasbourg, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Ta obrazložitveni memorandum je priložen predlogu akta o kibernetski solidarnosti. Uporaba informacijskih in komunikacijskih tehnologij ter odvisnost od njih sta postali ključna vidika v vseh sektorjih gospodarske dejavnosti, saj so naše javne uprave, podjetja in državljani v različnih sektorjih in prek meja tesneje medsebojno povezani in bolj odvisni drug od drugega kot kdaj koli prej. Večja uporaba digitalnih tehnologij povzroča večjo izpostavljenost kibernetskim incidentom in njihovim morebitnim posledicam. Hkrati se države članice srečujejo z vse večjimi tveganji za kibernetsko varnost in na splošno zapleteno krajino groženj, pri čemer obstaja očitno tveganje hitrega prelivanja kibernetskih incidentov iz ene države članice v druge.

Poleg tega so kibernetske operacije vse pogosteje del hibridnih strategij in strategij vojskovanja z znatnimi učinki na tarčo. Zlasti je bila pred rusko vojaško agresijo proti Ukrajini sprejeta in se še vedno uporablja strategija sovražnih kibernetskih operacij, ki predstavlja prelomnico pri dojemanju in ocenjevanju skupne pripravljenosti EU na obvladovanje kibernetskovarnostnih kriz ter zahteva nujno ukrepanje. Zaradi nevarnosti morebitnega incidenta velikih razsežnosti, ki bi povzročil znatne motnje in škodo na kritičnih infrastrukturah, je treba povečati pripravljenost na vseh ravneh kibernetskovarnostnega ekosistema EU. Ta nevarnost presega rusko vojaško agresijo na Ukrajino in vključuje stalne kibernetske grožnje državnih in nedržavnih akterjev, ki se bodo verjetno nadaljevale glede na številne na državni ravni usklajene, kriminalne in hektivistične akterje, vpletene v trenutne geopolitične napetosti. V zadnjih letih se je število kibernetskih napadov močno povečalo, vključno z napadi na oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Leta 2020 je napad na oskrbovalno verigo SolarWinds prizadel več kot 18 000 organizacij po vsem svetu, vključno z vladnimi agencijami in pomembnimi podjetji. Motnje, ki jih povzročijo pomembni kibernetskovarnostni incidenti, so lahko prevelike, da bi jih lahko obvladala ena sama ali več prizadetih držav članic. Zato je za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter boljšo pripravo in odzivanje nanje potrebna okrepljena solidarnost na ravni Unije.

Kar zadeva odkrivanje kibernetskih groženj in incidentov, je nujno treba povečati izmenjavo informacij in izboljšati naše skupne zmogljivosti, da bi se znatno skrajšal čas, potreben za odkrivanje kibernetskih groženj, preden lahko te povzročijo veliko škodo in stroške[1]. Čeprav imajo številne kibernetskovarnostne grožnje in incidenti zaradi medsebojne povezanosti digitalnih infrastruktur potencialno čezmejno razsežnost, je izmenjava ustreznih informacij

[1] Po podatkih iz poročila inštituta Ponemon in družbe IBM Security je bil povprečni čas za ugotovitev kršitve v letu 2022 207 dni, za obvladovanje pa je bilo potrebnih dodatnih 70 dni. Hkrati so leta 2022 povprečni stroški kršitev varstva podatkov z življenjskim ciklom, daljšim od 200 dni, znašali 4,86 milijona EUR v primerjavi s 3,74 milijona EUR pri življenjskem ciklu, krajšem od 200 dni („Cost of a data breach 2022“ (Stroški kršitve varstva podatkov v letu 2022), https://www.ibm.com/reports/data-breach).

med državami članicami še vedno omejena. Namen vzpostavitve mreže čezmejnih centrov za varnostne operacije za izboljšanje zmogljivosti za odkrivanje in odzivanje je pomoč pri reševanju tega vprašanja.

Kar zadeva pripravljenost in odzivanje na kibernetskovarnostne incidente, sta podpora na ravni Unije in solidarnost med državami članicami trenutno omejeni. Svet je v sklepih iz oktobra 2021 poudaril, da je treba te vrzeli odpraviti, in pozval Komisijo, naj predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere[2].

S to uredbo se izvaja tudi strategija EU za kibernetsko varnost, sprejeta decembra 2020[3], v kateri je bila napovedana vzpostavitev evropskega kibernetskega ščita, ki krepi zmogljivosti za odkrivanje kibernetskih groženj in izmenjavo informacij o njih v Evropski uniji z združevanjem nacionalnih in čezmejnih centrov za varnostne operacije.

Ta uredba temelji na prvih korakih, ki so že bili storjeni v tesnem sodelovanju z glavnimi deležniki in jih podpira program Digitalna Evropa. V okviru delovnega programa programa Digitalna Evropa za kibernetsko varnost za obdobje 2021–2022 sta bila v zvezi s centri za varnostne operacije organizirana zlasti razpis za prijavo interesa za skupno javno naročanje orodij in infrastrukture za ustanovitev čezmejnih centrov za varnostne operacije ter razpis za nepovratna sredstva za omogočanje krepitve zmogljivosti centrov za varnostne operacije, ki delujejo v javnih in zasebnih organizacijah. Kar zadeva pripravljenost in odzivanje na incidente, je Komisija vzpostavila kratkoročni program za podporo državam članicam z dodatnimi sredstvi, dodeljenimi Agenciji Evropske unije za kibernetsko varnost (ENISA), da bi se nemudoma okrepile pripravljenost in zmogljivosti za odzivanje na večje kibernetske incidente. Oba ukrepa sta bila pripravljena v tesnem sodelovanju z državami članicami. V tej uredbi so obravnavane pomanjkljivosti navedenih ukrepov in vanjo so vključena spoznanja, ki izhajajo iz teh ukrepov.

Ta predlog tudi izpolnjuje zavezo v skladu s skupnim sporočilom o kibernetski obrambi[4], sprejetim 10. novembra, za pripravo predloga za pobudo EU za kibernetsko solidarnost z naslednjimi cilji: okrepiti skupne zmogljivosti EU za odkrivanje, situacijsko zavedanje in odzivanje, postopno vzpostaviti kibernetsko rezervo na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in podpreti preskušanje kritičnih subjektov.

Glede na navedeno Komisija predlaga ta akt o kibernetski solidarnosti za okrepitev solidarnosti na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter boljšo pripravo in odzivanje nanje, pri čemer ima akt naslednje specifične cilje:

---

[2] Sklepi Sveta o oblikovanju kibernetske drže Evropske unije, ki jih je Svet odobril na seji 23. maja 2022 (9364/22).

[3] Skupno sporočilo Evropskemu parlamentu in Svetu, Strategija EU za kibernetsko varnost v digitalnem desetletju, JOIN(2020) 18 final.

[4] Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo, JOIN(2022) 49 final.

- okrepiti skupno odkrivanje kibernetskih groženj in incidentov v EU in situacijsko zavedanje o njih ter tako prispevati k evropski tehnološki suverenosti na področju kibernetske varnosti;
- okrepiti pripravljenost kritičnih subjektov po vsej EU in solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore pri odzivanju na incidente tretjim državam, pridruženim programu Digitalna Evropa;
- povečati odpornost Unije in prispevati k učinkovitemu odzivu s pregledovanjem in ocenjevanjem pomembnih incidentov ali incidentov velikih razsežnosti, med drugim z uporabo pridobljenih spoznanj in po potrebi priporočil.

Ti cilji se uresničujejo z naslednjimi ukrepi:

- vzpostavitvijo vseevropske infrastrukture centrov za varnostne operacije (evropskega kibernetskega ščita) za vzpostavitev in okrepitev skupnih zmogljivosti za odkrivanje in situacijsko zavedanje;
- vzpostavitvijo mehanizma za izredne kibernetske razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih. Podpora za odzivanje na incidente se omogoči tudi evropskim institucijam, organom, uradom in agencijam Unije;
- vzpostavitvijo evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih incidentov ali incidentov velikih razsežnosti.

Evropski kibernetski ščit in mehanizem za izredne kibernetske razmere bosta podprta s sredstvi iz programa Digitalna Evropa, ki bo s tem zakonodajnim instrumentom spremenjen, da se določijo zgoraj navedeni ukrepi, zagotovi finančna podpora za njihov razvoj in pojasnijo pogoji za upravičenost do finančne podpore.

• Skladnost z veljavnimi predpisi s področja zadevne politike

Okvir EU zajema več zakonodajnih aktov, ki so že vzpostavljeni ali so bili predlagani na ravni Unije za zmanjšanje ranljivosti, povečanje odpornosti kritičnih subjektov proti tveganjem za kibernetsko varnost in podporo usklajenemu obvladovanju kibernetskovarnostnih incidentov velikih razsežnosti in kriz, zlasti direktivo o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (NIS 2)[5], Akt o

[5] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2).

kibernetski varnosti[6], direktivo o napadih na informacijske sisteme[7] in Priporočilo Komisije (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize[8].

Ukrepi, predlagani v okviru akta o kibernetski solidarnosti, zajemajo situacijsko zavedanje, izmenjavo informacij ter podporo za pripravljenost in odzivanje na kibernetske incidente. Ti ukrepi so skladni s cilji regulativnega okvira, vzpostavljenega na ravni Unije, zlasti Direktivo (EU) 2022/2555 (v nadaljnjem besedilu: direktiva NIS 2), in jih podpirajo. Akt o kibernetski solidarnosti bo temeljil zlasti na obstoječih okvirih za operativno sodelovanje in krizno upravljanje na področju kibernetske varnosti, zlasti na Evropski organizacijski mreži za povezovanje v kibernetski krizi (EU-CyCLONe) in mreži skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT), ter jih bo podpiral.

Platforme čezmejnih centrov za varnostne operacije bi morale predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov o kibernetskovarnostnih grožnjah, povečevanjem vrednosti takih podatkov s strokovno analizo in najsodobnejšimi orodji ter prispevanjem k razvoju zmogljivosti in tehnološke suverenosti Unije.

Ta predlog je skladen s tudi priporočilom Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture[9], ki države članice poziva, naj sprejmejo nujne in učinkovite ukrepe ter zvesto, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se povečala odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

- **Skladnost z drugimi politikami Unije**

Predlog je skladen z drugimi mehanizmi in protokoli za izredne krizne razmere, kot je enotna ureditev za politično odzivanje na krize (IPCR). Akt o kibernetski solidarnosti bo te okvire in protokole za krizno upravljanje dopolnjeval z zagotavljanjem namenske podpore za pripravljenost in odzivanje na kibernetskovarnostne incidente. Predlog bo skladen tudi z zunanjim delovanjem EU v odziv na incidente velikih razsežnosti v okviru skupne zunanje in varnostne politike (SZVP), med drugim prek zbirke orodij EU za kibernetsko diplomacijo. Dopolnjeval bo ukrepe, ki se izvajajo v okviru člena 42(7) Pogodbe o Evropski uniji ali v primerih, opredeljenih v členu 222 Pogodbe o delovanju Evropske unije.

---

[6] Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti).

[7] Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ.

[8] Predlog uredbe Evropskega parlamenta in Sveta o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020, COM(2022) 454 final.

[9] Priporočilo Sveta z dne 8. decembra 2022 o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture (Besedilo velja za EGP), 2023/C 20/01.

Predlog dopolnjuje tudi mehanizem Unije na področju civilne zaščite[10], ki je bil vzpostavljen decembra 2013 in dopolnjen z novo zakonodajo, sprejeto maja 2021[11], s katero so okrepljeni stebri preprečevanja, pripravljenosti in odzivanja v okviru mehanizma Unije na področju civilne zaščite, EU pa zagotovljene dodatne zmogljivosti za odzivanje na nova tveganja v Evropi in po svetu ter okrepljene so zaloge v okviru rescEU.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

• Pravna podlaga

Pravna podlaga tega predloga sta člen 173(3) in člen 322(1), točka (a), Pogodbe o delovanju Evropske unije (PDEU). Člen 173 PDEU določa, da Unija in države članice skrbijo za zagotovitev pogojev, ki so potrebni za konkurenčnost industrije Unije. Namen te uredbe je okrepiti konkurenčni položaj industrijskega in storitvenega sektorja v Evropi v celotnem spletnem gospodarstvu ter podpreti njuno digitalno preobrazbo, in sicer z okrepitvijo ravni kibernetske varnosti na enotnem digitalnem trgu. Njen cilj je zlasti povečati odpornost državljanov, podjetij in subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice.

Predlog temelji tudi na členu 322(1), točka (a), PDEU, saj vsebuje posebna pravila o prenosu, ki odstopajo od načela enoletnosti iz Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta (v nadaljnjem besedilu: finančna uredba)[12]. Za namene dobrega finančnega poslovodenja ter ob upoštevanju nepredvidljive, izjemne in posebne narave kibernetskovarnostne krajine in kibernetskih groženj bi bilo treba mehanizmu za izredne kibernetske razmere omogočiti določeno stopnjo prožnosti v zvezi z upravljanjem proračuna, zlasti z omogočanjem samodejnega prenosa neporabljenih odobritev za prevzem obveznosti in odobritev plačil za ukrepe, namenjene izpolnjevanju ciljev iz Uredbe, v naslednje proračunsko leto. Ker se s tem novim pravilom odpirajo vprašanja v zvezi s finančno uredbo, bi se to vprašanje lahko obravnavalo v okviru sedanjih pogajanj o prenovitvi finančne uredbe.

• Subsidiarnost (za neizključno pristojnost)

Zaradi močne čezmejne narave kibernetskovarnostnih groženj ter vse večjega števila tveganj in incidentov, ki imajo učinke prelivanja prek meja, sektorjev in proizvodov, države članice ciljev tega ukrepanja ne morejo učinkovito doseči same, zato sta potrebna skupno ukrepanje in solidarnost na ravni Unije.

---

[10] Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (Besedilo velja za EGP).

[11] Uredba (EU) 2021/836 Evropskega parlamenta in Sveta z dne 20. maja 2021 o spremembi Sklepa št. 1313/2013/EU o mehanizmu Unije na področju civilne zaščite (Besedilo velja za EGP).

[12] Uredba (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije (UL L 193, 30.7.2018, str. 1).

Izkušnje z bojem proti kibernetskim grožnjam, ki izhajajo iz vojne proti Ukrajini, skupaj s spoznanji, pridobljenimi med vajo na področju kibernetske varnosti, ki se je izvajala med francoskim predsedovanjem (EU CyCLES), so pokazale, da bi bilo treba za dosego solidarnosti na ravni EU razviti konkretne mehanizme vzajemne podpore, zlasti sodelovanje z zasebnim sektorjem. Glede na navedeno Svet v sklepih z dne 23. maja 2022 o oblikovanju kibernetske drže Evropske unije Komisijo poziva, naj predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere.

Podpora in ukrepi na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj ter povečanje zmogljivosti za pripravljenost in odzivanje zagotavljajo dodano vrednost, saj preprečujejo podvajanje prizadevanj v Uniji in državah članicah. To bi omogočilo boljšo uporabo obstoječih sredstev ter večje usklajevanje in izmenjavo informacij o pridobljenih spoznanjih. Mehanizem za izredne kibernetske razmere predvideva tudi podporo tretjim državam, pridruženim programu Digitalna Evropa, iz kibernetskovarnostne rezerve EU.

Podpora, zagotovljena v okviru različnih pobud, ki bodo vzpostavljene in financirane na ravni Unije, bo dopolnila nacionalne zmogljivosti v zvezi z odkrivanjem kibernetskih groženj in incidentov, situacijskim zavedanjem o njih ter pripravljenostjo in odzivanjem nanje, ne bo pa jih podvojila.

• Sorazmernost

Ukrepi ne presegajo tistega, kar je potrebno za doseganje splošnih in specifičnih ciljev Uredbe. Ukrepi iz te uredbe ne vplivajo na odgovornosti držav članic na področju nacionalne varnosti, javne varnosti ter preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj. Prav tako ne vplivajo na pravne obveznosti subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih, glede sprejemanja ukrepov na področju kibernetske varnosti v skladu z direktivo NIS 2.

Taka prizadevanja in ukrepe dopolnjujejo ukrepi, ki jih zajema ta uredba, saj podpirajo vzpostavitev infrastruktur za boljše odkrivanje in analizo groženj ter zagotavljajo podporo za ukrepe pripravljenosti in odzivanja v primeru pomembnih incidentov ali incidentov velikih razsežnosti.

• Izbira instrumenta

Predlagani instrument je uredba Evropskega parlamenta in Sveta. To je najprimernejši pravni instrument, saj lahko le uredba s pravnimi določbami, ki se neposredno uporabljajo, zagotovi stopnjo enotnosti, ki je potrebna za vzpostavitev in delovanje evropskega kibernetskega ščita in mehanizma za izredne kibernetske razmere, in sicer z zagotavljanjem podpore iz programa Digitalna Evropa za njuno vzpostavitev ter določitvijo jasnih pogojev za uporabo in dodeljevanje te podpore.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z DELEŽNIKI IN OCEN UČINKA

- **Posvetovanja z deležniki**

Ukrepi iz te uredbe bodo podprti s programom Digitalna Evropa, o katerem so potekala obsežna posvetovanja. Poleg tega bodo temeljili na prvih korakih, ki so bili pripravljeni v tesnem sodelovanju z glavnimi deležniki. Kar zadeva centre za varnostne operacije, je Komisija v tesnem sodelovanju z državami članicami v okviru Evropskega kompetenčnega centra za kibernetsko varnost (ECCC) pripravila konceptni dokument o razvoju platform čezmejnih centrov za varnostne operacije in razpis za prijavo interesa. V zvezi s tem je bila izvedena raziskava o zmogljivostih nacionalnih centrov za varnostne operacije, v tehnični delovni skupini centra ECCC, ki združuje predstavnike držav članic, pa so bili obravnavani skupni pristopi in tehnične zahteve. Poleg tega so potekale izmenjave z industrijo, zlasti v okviru strokovne skupine o centrih za varnostne operacije, ki sta jo ustanovili agencija ENISA in Evropska organizacija za kibernetsko varnost (ECSO).

Kar zadeva pripravljenost in odzivanje na incidente, je Komisija vzpostavila kratkoročni program za podporo državam članicam z dodatnimi sredstvi, dodeljenimi agenciji ENISA iz programa Digitalna Evropa, da bi se nemudoma okrepile pripravljenost in zmogljivosti za odzivanje na večje kibernetske incidente. Povratne informacije držav članic in industrije, zbrane med izvajanjem tega kratkoročnega programa, že zagotavljajo dragocena spoznanja, ki so se upoštevala pri pripravi predlagane uredbe za odpravo ugotovljenih pomanjkljivosti. To je bil prvi korak v skladu s sklepi Sveta o kibernetski drži, v katerih je bila Komisija pozvana, naj pripravi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere.

Poleg tega je 16. februarja 2023 na podlagi dokumenta za razpravo potekala delavnica s strokovnjaki držav članic o mehanizmu za izredne kibernetske razmere. Na delavnici so sodelovale vse države članice, enajst držav članic pa je predložilo dodatne pisne prispevke.

- **Ocena učinka**

Zaradi nujnosti priprave predloga ocena učinka ni bila izvedena. Ukrepi iz te uredbe bodo podprti s programom Digitalna Evropa in so v skladu z ukrepi iz uredbe o programu Digitalna Evropa (PDE), za katero je bila izvedena namenska ocena učinka. Ta uredba ne bo imela večjih upravnih ali okoljskih učinkov, razen tistih, ki so bili že ocenjeni v oceni učinka uredbe o PDE.

Poleg tega uredba temelji na prvih ukrepih, oblikovanih v tesnem sodelovanju z glavnimi deležniki, kot je navedeno zgoraj, in nadaljnjih ukrepih na podlagi poziva držav članic, naj Komisija do konca 3. četrtletja 2022 predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere.

V okviru delovnega programa programa Digitalna Evropa za kibernetsko varnost za obdobje 2021–2022 sta bila v zvezi s situacijskim zavedanjem in odkrivanjem v okviru evropskega kibernetskega ščita organizirana zlasti razpis za prijavo interesa za skupno javno

naročanje orodij in infrastrukture za ustanovitev čezmejnih centrov za varnostne operacije ter razpis za nepovratna sredstva za krepitev zmogljivosti centrov za varnostne operacije, ki delujejo v javnih in zasebnih organizacijah.

Kot je navedeno zgoraj, je Komisija na področju pripravljenosti in odzivanja na incidente oblikovala kratkoročni program, ki ga izvaja agencija ENISA, za podporo državam članicam iz programa Digitalna Evropa. Zajete storitve vključujejo ukrepe pripravljenosti, kot je penetracijsko testiranje kritičnih subjektov za ugotavljanje ranljivosti. S programom so okrepljene tudi možnosti za pomoč državam članicam v primeru večjega incidenta, ki prizadene kritične subjekte. Ta kratkoročni program izvaja agencija ENISA, zagotovil pa je že ustrezna spoznanja, ki so bila upoštevana pri pripravi te uredbe.

- **Temeljne pravice**

Predlog bo s povečevanjem varnosti digitalnih informacij prispeval k zaščiti pravice do svobode in varnosti v skladu s členom 6 Listine EU o temeljnih pravicah ter pravice do spoštovanja zasebnega in družinskega življenja v skladu s členom 7 Listine EU o temeljnih pravicah. Z varovanjem podjetij pred gospodarsko škodljivimi kibernetskimi napadi bo prispeval tudi k svobodi gospodarske pobude v skladu s členom 16 Listine EU o temeljnih pravicah in lastninski pravici v skladu s členom 17 Listine EU o temeljnih pravicah. Nazadnje bo predlog z varovanjem celovitosti kritične infrastrukture pred kibernetskimi napadi prispeval k pravici do varovanja zdravja v skladu s členom 35 Listine EU o temeljnih pravicah in pravici do dostopa do storitev splošnega gospodarskega pomena v skladu s členom 36 Listine EU o temeljnih pravicah.

4. PRORAČUNSKE POSLEDICE

Ukrepi iz te uredbe bodo podprti s sredstvi, namenjenimi za strateški cilj kibernetske varnosti v okviru programa Digitalna Evropa.

Skupni proračun vključuje povečanje v višini 100 milijonov EUR, za katero se v tej uredbi predlaga, da se prerazporedi iz drugih strateških ciljev programa Digitalna Evropa. Tako se bo novi skupni znesek, ki je na voljo za ukrepe na področju kibernetske varnosti v okviru programa Digitalna Evropa, povečal na 842,8 milijona EUR.

Del dodatnih 100 milijonov EUR bo okrepil proračun, ki ga upravlja center ECCC, za izvajanje ukrepov v zvezi s centri za varnostne operacije in pripravljenostjo v okviru njihovih delovnih programov. Poleg tega bodo dodatna sredstva namenjena podpori vzpostavitve kibernetskovarnostne rezerve EU.

Ta sredstva dopolnjujejo proračun, ki je za podobne ukrepe že predviden v okviru delovnih programov osrednjega programa Digitalna Evropa in programa Digitalna Evropa za kibernetsko varnost za obdobje 2023–2027, s čimer bi se lahko skupni znesek za obdobje 2023–2027 povečal na 551 milijonov, pri čemer je bilo za obdobje 2021–2022 že

dodeljenih 115 milijonov v obliki pilotnih projektov. Vključno s prispevki držav članic bi lahko skupni proračun znašal do 1,109 milijarde EUR.

Pregled s tem povezanih stroškov je vključen v oceno finančnih posledic zakonodajnega predloga, ki je priložena temu predlogu.

5. DRUGI ELEMENTI

• Načrti za izvedbo ter ureditev spremljanja, ocenjevanja in poročanja

Komisija bo spremljala izvajanje in uporabo teh novih določb ter skladnost z njimi, da bi ocenila njihovo učinkovitost. Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe najpozneje štiri leta po datumu začetka njene uporabe.

• Natančnejša pojasnitev posameznih določb predloga

Splošni cilji, predmet urejanja in opredelitve pojmov (poglavje I)

V poglavju I so določeni cilji Uredbe za okrepitev solidarnosti na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje ter zlasti za krepitev skupnega odkrivanja kibernetskih groženj in incidentov ter situacijskega zavedanja o njih v Uniji, krepitev pripravljenosti subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, krepitev solidarnosti z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti ter povečanje odpornosti Unije s pregledovanjem in ocenjevanjem pomembnih incidentov ali incidentov velikih razsežnosti. V tem poglavju so določeni tudi ukrepi, s katerimi se bodo ti cilji dosegli, in sicer uvedba evropskega kibernetskega ščita, vzpostavitev mehanizma za izredne kibernetske razmere in vzpostavitev mehanizma za pregledovanje kibernetskovarnostnih incidentov. Prav tako so opredeljeni pojmi, ki se uporabljajo v celotnem instrumentu.

Evropski kibernetski ščit (poglavje II)

Poglavje II vzpostavlja evropski kibernetski ščit ter določa njegove različne elemente in pogoje za sodelovanje. V njem so najprej napovedani splošni cilj evropskega kibernetskega ščita, tj. razviti napredne zmogljivosti Unije za odkrivanje, analiziranje in obdelavo podatkov o kibernetskih grožnjah in incidentih v Uniji, ter specifični operativni cilji. Določeno je, da se sredstva Unije za evropski kibernetski ščit zagotavljajo v skladu z uredbo o PDE.

Poleg tega je v tem poglavju opisana vrsta subjektov, ki sestavljajo evropski kibernetski ščit. Ščit sestavljajo nacionalni centri za varnostne operacije in čezmejni centri za varnostne operacije. Nacionalni center za varnostne operacije imenuje vsaka država članica. Ta center deluje kot referenčna točka in točka dostopa do drugih javnih in zasebnih organizacij na nacionalni ravni za zbiranje in analiziranje informacij o kibernetskovarnostnih grožnjah in incidentih ter prispevanje k čezmejnemu centru za varnostne operacije. Center ECCC lahko na podlagi razpisa za prijavo interesa izbere nacionalni center za varnostne operacije, ki bo z

njim sodeloval pri skupnem javnem naročanju orodij in infrastruktur ter prejel nepovratna sredstva za upravljanje teh orodij in infrastruktur. Če nacionalni center za varnostne operacije prejme podporo Unije, se zaveže, da bo v dveh letih zaprosil za sodelovanje v čezmejnem centru za varnostne operacije.

Čezmejne centre za varnostne operacije sestavlja konzorcij vsaj treh držav članic, ki jih zastopajo nacionalni centri za varnostne operacije, ki so se zavezali sodelovanju pri usklajevanju svojih dejavnosti odkrivanja in spremljanja kibernetskih groženj. Center ECCC lahko po prvem razpisu za prijavo interesa izbere gostiteljski konzorcij, ki bo z njim sodeloval pri skupnem javnem naročanju orodij in infrastruktur ter prejel nepovratna sredstva za upravljanje teh orodij in infrastruktur. Članice gostiteljskega konzorcija sklenejo pisno konzorcijsko pogodbo, v kateri so določeni njihovi notranji dogovori. V tem poglavju so nato podrobno opisane zahteve glede izmenjave informacij med sodelujočimi v čezmejnem centru za varnostne operacije ter izmenjave informacij med enim čezmejnim centrom za varnostne operacije in drugimi čezmejnimi centri za varnostne operacije ter z ustreznimi subjekti EU. Nacionalni centri za varnostne operacije, ki sodelujejo v čezmejnem centru za varnostne operacije, si izmenjujejo ustrezne informacije v zvezi s kibernetskimi grožnjami, podrobnosti, med drugim zavezanost izmenjavi znatnih količin podatkov in pogoje te izmenjave, pa bi bilo treba opredeliti v konzorcijski pogodbi. Čezmejni centri za varnostne operacije zagotavljajo visoko raven medsebojne interoperabilnosti. Čezmejni centri za varnostne operacije bi morali tudi skleniti sporazume o sodelovanju z drugimi čezmejnimi centri za varnostne operacije, v njih pa bi morali določiti načela izmenjave informacij. Kadar čezmejni centri za varnostne operacije pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti, ustrezne informacije zagotovijo mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji glede na njihove vloge pri kriznem upravljanju v skladu z Direktivo (EU) 2022/2555. Poglavje II se zaključi z določitvijo varnostnih pogojev za sodelovanje v evropskem kibernetskem ščitu.

Mehanizem za izredne kibernetske razmere (poglavje III)

Poglavje III vzpostavlja mehanizem za izredne kibernetske razmere za povečanje odpornosti Unije proti večjim kibernetskovarnostnim grožnjam ter pripravo na kratkoročne posledice pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti ali kriz in njihovo ublažitev v duhu solidarnosti. Ukrepi za izvajanje mehanizma za izredne kibernetske razmere se podprejo s sredstvi iz programa Digitalna Evropa. Mehanizem določa ukrepe za podporo pripravljenosti, vključno z usklajenim preskušanjem subjektov, ki delujejo v visoko kritičnih sektorjih, in odzivanju na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti ter takojšnjemu okrevanju po njih ali ublažitvi pomembnih kibernetskih groženj ter ukrepe medsebojne pomoči.

Ukrepi pripravljenosti v okviru mehanizma za izredne kibernetske razmere vključujejo usklajeno preskušanje pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih. Komisija bi morala po posvetovanju z agencijo ENISA in skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov med visoko kritičnimi sektorji, navedenimi v

Prilogi I k Direktivi (EU) 2022/2555, redno določati ustrezne sektorje ali podsektorje, katerih subjekti so lahko predmet usklajenega preskušanja pripravljenosti na ravni EU.

S to uredbo se za namene izvajanja predlaganih ukrepov za odzivanje na incidente vzpostavi kibernetskovarnostna rezerva EU, ki vključuje storitve zaupanja vrednih ponudnikov za odzivanje na incidente, izbrane v skladu z merili iz te uredbe. Med uporabniki storitev iz kibernetskovarnostne rezerve EU so organi držav članic za obvladovanje kibernetskih kriz in skupine CSIRT ter institucije, organi, uradi in agencije Unije. Za izvajanje kibernetskovarnostne rezerve EU je v celoti odgovorna Komisija, pri čemer lahko delovanje in upravljanje te rezerve v celoti ali delno zaupa agenciji ENISA.

Da bi uporabniki prejeli podporo iz kibernetskovarnostne rezerve EU, bi morali sprejeti lastne ukrepe za ublažitev učinkov incidenta, za katerega se zahteva podpora. Zahtevki za podporo iz kibernetskovarnostne rezerve EU bi morali vključevati potrebne ustrezne informacije o incidentu in ukrepih, ki so jih uporabniki že sprejeli. V tem poglavju so prav tako opisane podrobnosti o izvajanju, vključno z oceno zahtevkov, predloženih kibernetskovarnostni rezervi EU.

V Uredbi so določena tudi načela javnega naročanja in merila za izbiro v zvezi z zaupanja vrednimi ponudniki kibernetskovarnostne rezerve EU.

Tretje države lahko zaprosijo za podporo iz kibernetskovarnostne rezerve EU, če je to določeno v pridružitvenih sporazumih, sklenjenih v zvezi z njihovim sodelovanjem v programu Digitalna Evropa. V tem poglavju so opisani nadaljnji pogoji takega sodelovanja in podrobnosti o njem.

Mehanizem za pregledovanje kibernetskovarnostnih incidentov (poglavje IV)

Agencija ENISA bi morala na zahtevo Komisije, mreže EU-CyCLONe ali mreže skupin CSIRT pregledati in oceniti grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Agencija ENISA bi morala mreži skupin CSIRT, mreži EU-CyCLONe in Komisiji pregled in oceno predložiti v obliki poročila o pregledu incidenta, da bi jih s tem podprla pri izvajanju njihovih nalog. Če se incident nanaša na tretjo državo, bi morala Komisija poročilo poslati visokemu predstavniku. Poročilo bi moralo vključevati pridobljena spoznanja in po potrebi priporočila za izboljšanje kibernetske drže EU.

Končne določbe (poglavje V)

Poglavje V vsebuje spremembe uredbe o PDE in obveznost Komisije, da za Evropski parlament in Svet redno pripravlja poročila za oceno in pregled Uredbe. Komisija je pooblaščena za sprejemanje izvedbenih aktov v skladu s postopkom pregleda iz člena 21, in sicer za določitev pogojev za to interoperabilnost med čezmejnimi centri za varnostne operacije; določitev postopkovnih ureditev za izmenjavo informacij v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti med čezmejnimi centri za varnostne operacije in subjekti Unije; določitev tehničnih zahtev za zagotovitev visoke ravni

varnosti podatkov in fizične varnosti infrastrukture ter za zaščito varnostnih interesov Unije pri izmenjavi informacij s subjekti, ki niso javni organi držav članic; določitev vrst in števila storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU, in natančnejšo opredelitev podrobnih ureditev za dodeljevanje storitev podpore iz kibernetskovarnostne rezerve EU.

2023/0109 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije ter zlasti člena 173(3) in člena 322(1), točka (a), Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Računskega sodišča[1],

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[2],

ob upoštevanju mnenja Odbora regij[3],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Uporaba informacijskih in komunikacijskih tehnologij ter odvisnost od njih sta postali ključna vidika v vseh sektorjih gospodarske dejavnosti, saj so naše javne uprave, podjetja in državljani v različnih sektorjih in prek meja tesneje medsebojno povezani in bolj odvisni drug od drugega kot kdaj koli prej.

(2) Obseg, pogostost in posledice kibernetskovarnostnih incidentov se povečujejo, vključno z napadi na oskrbovalno verigo, katerih cilj je kibernetsko vohunjenje, izsiljevalsko programje ali povzročanje motenj. Ti predstavljajo veliko grožnjo za delovanje omrežja in informacijskih sistemov. Glede na hitro razvijajočo se krajino groženj je treba zaradi nevarnosti morebitnih incidentov velikih razsežnosti, ki povzročajo velike motnje ali škodo na kritičnih infrastrukturah, povečati pripravljenost na vseh ravneh okvira Unije za kibernetsko varnost. Ta nevarnost presega rusko vojaško agresijo na Ukrajino in se bo verjetno nadaljevala, glede na številne na državni ravni usklajene, kriminalne in hektivistične akterje, vpletene v trenutne geopolitične napetosti. Taki incidenti lahko ovirajo zagotavljanje javnih storitev in opravljanje gospodarskih dejavnosti, tudi v kritičnih ali visoko kritičnih sektorjih, povzročijo znatne finančne izgube, spodkopljejo zaupanje uporabnikov, povzročijo veliko škodo gospodarstvu Unije in imajo lahko celo zdravstvene ali življenjsko nevarne posledice. Poleg tega so kibernetskovarnostni incidenti nepredvidljivi, saj pogosto nastanejo in se razvijejo v zelo kratkem času, niso omejeni na določeno geografsko območje in se zgodijo hkrati ali se takoj razširijo po številnih državah.

---

1 UL C , , str. .
2 UL C , , str. .
3 UL C , , str. .

(3) Okrepiti je treba konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter podpreti njuno digitalno preobrazbo, in sicer z okrepitvijo ravni kibernetske varnosti na enotnem digitalnem trgu. Kot je priporočeno v treh različnih predlogih Konference o prihodnosti Evrope[4], je treba povečati odpornost državljanov, podjetij in subjektov, ki upravljajo kritične infrastrukture, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. Zato so potrebne naložbe v infrastrukture in storitve, ki bodo podpirale hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, države članice pa potrebujejo pomoč pri boljši pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter odzivanju nanje. Unija bi tudi morala povečati svoje zmogljivosti na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih.

(4) Unija je že sprejela več ukrepov za zmanjšanje ranljivosti in povečanje odpornosti kritičnih infrastruktur in subjektov proti tveganjem za kibernetsko varnost, zlasti Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta[5], Priporočilo Komisije (EU) 2017/1584[6], Direktivo 2013/40/EU Evropskega parlamenta in Sveta[7] ter Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta[8]. Poleg tega so države članice v priporočilu Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture pozvane, naj sprejmejo nujne in učinkovite ukrepe ter zvesto, učinkovito, solidarno in usklajeno sodelujejo med seboj, s Komisijo in drugimi ustreznimi javnimi organi ter zadevnimi subjekti, da bi se okrepila odpornost kritične infrastrukture, ki se uporablja za zagotavljanje bistvenih storitev na notranjem trgu.

(5) Zaradi vse večjih tveganj za kibernetsko varnost in na splošno zapletene krajine groženj, pa tudi jasnega tveganja hitrega prelivanja kibernetskih incidentov iz ene države članice v druge in iz tretje države v Unijo, je potrebna okrepljena solidarnost na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje. Države članice so Komisijo v sklepih Sveta o kibernetski drži EU pozvale tudi, naj [9] predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere.

(6) V skupnem sporočilu o politiki EU za kibernetsko obrambo[10], sprejetem 10. novembra 2022, je bila napovedana pobuda EU za kibernetsko solidarnost z naslednjimi cilji: okrepitev skupnih zmogljivosti EU za odkrivanje, situacijsko zavedanje in odzivanje s spodbujanjem uvedbe infrastrukture centrov za varnostne

---

4 https://futureu.europa.eu/sl/

5 Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (UL L 333, 27.12.2022).

6 Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

7 Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).

8 Uredba (EU) 2019/881 Evropskega parlamenta in Sveta z dne 17. aprila 2019 o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt o kibernetski varnosti) (UL L 151, 7.6.2019, str. 15).

9 Sklepi Sveta o oblikovanju kibernetske drže Evropske unije, ki jih je Svet odobril na seji 23. maja 2022 (9364/22).

10 Skupno sporočilo Evropskemu parlamentu in Svetu, Politika EU za kibernetsko obrambo, JOIN(2022) 49 final.

operacije v EU, podpiranje postopne vzpostavitve kibernetskovarnostne rezerve na ravni EU s storitvami zaupanja vrednih zasebnih ponudnikov in preskušanje kritičnih subjektov glede morebitnih ranljivosti na podlagi ocen tveganja EU.

(7) Izboljšati je treba odkrivanje kibernetskih groženj in incidentov ter situacijsko zavedanje o njih po vsej Uniji ter okrepiti solidarnost s povečanjem pripravljenosti in zmogljivosti držav članic in Unije za odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti. Zato bi bilo treba vzpostaviti vseevropsko infrastrukturo centrov za varnostne operacije (evropski kibernetski ščit), da bi se oblikovale in okrepile skupne zmogljivosti za odkrivanje in situacijsko zavedanje; vzpostaviti bi bilo treba mehanizem za izredne kibernetske razmere, da bi države članice podprli pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih; vzpostaviti bi bilo treba mehanizem za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje posameznih pomembnih kibernetskovarnostnih incidentov ali incidentov velikih razsežnosti. Ti ukrepi ne posegajo v člena 107 in 108 Pogodbe o delovanju Evropske unije (PDEU).

(8) Za dosego teh ciljev je treba na nekaterih področjih spremeniti tudi Uredbo (EU) 2021/694 Evropskega parlamenta in Sveta[11]. Zlasti bi bilo treba s to uredbo spremeniti Uredbo (EU) 2021/694, kar zadeva dodajanje novih operativnih ciljev v zvezi z evropskim kibernetskim ščitom in mehanizmom za izredne kibernetske razmere v okviru specifičnega cilja 3 programa Digitalna Evropa, katerega cilj je zagotoviti odpornost, celovitost in zanesljivost enotnega digitalnega trga, okrepiti zmogljivosti za spremljanje kibernetskih napadov in groženj in odzivanje nanje ter izboljšati čezmejno sodelovanje na področju kibernetske varnosti. To bo dopolnjeno s posebnimi pogoji, pod katerimi se lahko za te ukrepe dodeli finančna podpora, pri čemer bi bilo treba opredeliti mehanizme upravljanja in usklajevanja, ki so potrebni za doseganje zastavljenih ciljev. Druge spremembe Uredbe (EU) 2021/694 bi morale vključevati opise predlaganih ukrepov v okviru novih operativnih ciljev in merljive kazalnike za spremljanje izvajanja teh novih operativnih ciljev.

(9) Financiranje ukrepov na podlagi te uredbe bi bilo treba določiti v Uredbi (EU) 2021/694, ki bi morala biti še naprej ustrezen temeljni akt za te ukrepe, določene v okviru specifičnega cilja 3 programa Digitalna Evropa. Posebni pogoji za sodelovanje v zvezi z vsakim ukrepom bodo določeni v ustreznih delovnih programih v skladu z veljavno določbo Uredbe (EU) 2021/694.

(10) Za to uredbo se uporabljajo horizontalna finančna pravila, ki sta jih Evropski parlament in Svet sprejela na podlagi člena 322 PDEU. Ta pravila so navedena v finančni uredbi in določajo zlasti postopek za določitev in izvrševanje proračuna Unije ter urejajo nadzor nad odgovornostmi finančnih udeležencev. Pravila, sprejeta na podlagi člena 322 PDEU, vključujejo tudi splošni režim pogojenosti za zaščito proračuna Unije, kot je določen v Uredbi (EU, Euratom) 2020/2092 Evropskega parlamenta in Sveta.

(11) Za dobro finančno poslovodenje bi bilo treba določiti posebna pravila za prenos neporabljenih odobritev za prevzem obveznosti in odobritev plačil. Ob upoštevanju načela, da se proračun Unije določi vsako leto, bi bilo treba s to uredbo zaradi nepredvidljive, izjemne in posebne narave kibernetske krajine zagotoviti možnosti za

[11] Uredba (EU) 2021/694 Evropskega parlamenta in Sveta z dne 29. aprila 2021 o vzpostavitvi programa Digitalna Evropa in razveljavitvi Sklepa (EU) 2015/2240 (UL L 166, 11.5.2021, str. 1).

prenos neporabljenih sredstev, ki presegajo tiste iz finančne uredbe, s čimer bi se čim bolj povečala zmogljivost mehanizma za izredne kibernetske razmere za podporo državam članicam pri učinkovitem boju proti kibernetskim grožnjam.

(12) Za učinkovitejše preprečevanje in ocenjevanje kibernetskih groženj in incidentov ter odzivanje nanje je treba razviti celovitejše znanje o grožnjah za kritična sredstva in infrastrukture na ozemlju Unije, vključno z njihovo geografsko porazdelitvijo, medsebojno povezanostjo in morebitnimi učinki v primeru kibernetskih napadov na te infrastrukture. Vzpostaviti bi bilo treba obsežno infrastrukturo centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) v Uniji, ki bi jo sestavljalo več interoperabilnih čezmejnih platform, od katerih bi vsaka združevala več nacionalnih centrov za varnostne operacije. Ta infrastruktura bi morala služiti interesom in potrebam držav in Unije na področju kibernetske varnosti, spodbujati najsodobnejšo tehnologijo za napredno zbiranje podatkov in analitična orodja, okrepiti zmogljivosti kibernetskega odkrivanja in upravljanja ter zagotavljati situacijsko zavedanje v realnem času. Namenjena bi morala biti boljšemu odkrivanju kibernetskovarnostnih groženj in incidentov ter tako dopolnjevati in podpirati subjekte in omrežja Unije, odgovorne za krizno upravljanje v Uniji, zlasti organizacijsko mrežo EU za povezovanje v kibernetski krizi (v nadaljnjem besedilu: mreža EU-CyCLONe), kot je opredeljena v Direktivi (EU) 2022/2555 Evropskega parlamenta in Sveta[12].

(13) Vsaka država članica bi morala imenovati javni organ na nacionalni ravni, ki bi bil zadolžen za usklajevanje dejavnosti odkrivanja kibernetskih groženj v tej državi članici. Ti nacionalni centri za varnostne operacije bi morali delovati kot referenčna točka in točka dostopa na nacionalni ravni za sodelovanje v evropskem kibernetskem ščitu ter zagotoviti, da se informacije o kibernetskih grožnjah, ki jih predložijo javni in zasebni subjekti, na nacionalni ravni izmenjujejo in zbirajo na učinkovit in poenostavljen način.

(14) V okviru evropskega kibernetskega ščita bi bilo treba ustanoviti več čezmejnih centrov za varnostne operacije na področju kibernetske varnosti. Ti bi morali združevati nacionalne centre za varnostne operacije iz vsaj treh držav članic, da bi lahko v celoti izkoristili prednosti čezmejnega odkrivanja groženj ter izmenjave in upravljanja informacij. Splošna cilja čezmejnih centrov za varnostne operacije bi morala biti okrepitev zmogljivosti za analizo, preprečevanje in odkrivanje kibernetskovarnostnih groženj ter podpora pripravi visokokakovostnih obveščevalnih podatkov o kibernetskovarnostnih grožnjah, zlasti z izmenjavo podatkov iz različnih virov, javnih ali zasebnih, pa tudi izmenjavo in skupno uporabo najsodobnejših orodij ter skupnim razvojem zmogljivosti za odkrivanje, analizo in preprečevanje v zaupanja vrednem okolju. Ti centri bi morali zagotoviti nove dodatne zmogljivosti, ki bi temeljile na obstoječih centrih za varnostne operacije in skupinah za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) ter drugih ustreznih akterjih in jih dopolnjevale.

(15) Spremljanje, odkrivanje in analizo kibernetskih groženj na nacionalni ravni običajno zagotavljajo centri za varnostne operacije, ki jih sestavljajo javni in zasebni subjekti, v povezavi s skupinami CSIRT. Poleg tega si skupine CSIRT informacije izmenjujejo v

[12] Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).

okviru mreže skupin CSIRT v skladu z Direktivo (EU) 2022/2555. Čezmejni centri za varnostne operacije bi morali predstavljati novo zmogljivost, ki dopolnjuje mrežo skupin CSIRT, in sicer z zbiranjem in izmenjavo podatkov javnih in zasebnih subjektov o kibernetskovarnostnih grožnjah, povečevanjem vrednosti takih podatkov s strokovno analizo ter skupno pridobljenimi infrastrukturami in najsodobnejšimi orodji ter prispevanjem k razvoju zmogljivosti in tehnološke suverenosti Unije.

(16) Čezmejni centri za varnostne operacije bi morali delovati kot osrednja točka, ki bi omogočala obsežno zbiranje ustreznih podatkov in obveščevalnih podatkov o kibernetskih grožnjah ter širjenje informacij o grožnjah med velikim in raznolikim naborom akterjev (npr. skupinami za odzivanje na računalniške grožnje (v nadaljnjem besedilu: skupine CERT), skupinami CSIRT, centri za izmenjavo in analizo informacij, upravljavci kritičnih infrastruktur). Informacije, ki si jih izmenjujejo sodelujoči v čezmejnem centru za varnostne operacije, bi lahko vključevale podatke iz omrežij in senzorjev, obveščevalne podatke o grožnjah, kazalnike ogroženosti ter kontekstualizirane informacije o incidentih, grožnjah in ranljivostih. Poleg tega bi morali čezmejni centri za varnostne operacije skleniti tudi sporazume o sodelovanju z drugimi čezmejnimi centri za varnostne operacije.

(17) Skupno situacijsko zavedanje med ustreznimi organi je nujen osnovni pogoj za pripravljenost in usklajevanje na ravni Unije v zvezi s pomembnimi kibernetskovarnostnimi incidenti in takimi incidenti velikih razsežnosti. Z Direktivo (EU) 2022/2555 je ustanovljena mreža EU-CyCLONe za podporo usklajenemu obvladovanju kibernetskovarnostnih incidentov velikih razsežnosti in kriz na operativni ravni ter zagotovitev redne izmenjave ustreznih informacij med državami članicami ter institucijami, organi, uradi in agencijami Unije. V Priporočilu (EU) 2017/1584 o usklajenem odzivu na velike kibernetske incidente in krize je obravnavana vloga vseh ustreznih akterjev. V Direktivi (EU) 2022/2555 je tudi opozorjeno na odgovornosti Komisije v okviru mehanizma Unije na področju civilne zaščite, vzpostavljenega s Sklepom 1313/2013/EU Evropskega parlamenta in Sveta, ter za pripravo analitičnih poročil o enotni ureditvi za politično odzivanje na krize (IPCR) v skladu z Izvedbenim sklepom (EU) 2018/1993. Zato bi morali čezmejni centri za varnostne operacije v primerih, ko pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti, mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji zagotoviti ustrezne informacije. Glede na okoliščine bi lahko informacije, ki jih je treba izmenjati, vključevale zlasti tehnične informacije, informacije o naravi in motivih napadalca ali morebitnega napadalca ter netehnične informacije na višji ravni o morebitnem ali tekočem kibernetskovarnostnem incidentu velikih razsežnosti. V zvezi s tem bi bilo treba ustrezno upoštevati načelo potrebe po seznanitvi in morda občutljivo naravo izmenjanih informacij.

(18) Subjekti, ki sodelujejo v evropskem kibernetskem ščitu, bi morali zagotoviti visoko raven medsebojne interoperabilnosti, po potrebi tudi kar zadeva formate podatkov, taksonomijo ter orodja za obravnavanje in analizo podatkov, pa tudi varne komunikacijske kanale, minimalno raven varnosti aplikacijske plasti, pregled situacijskega zavedanja in kazalnike. Pri sprejetju skupne taksonomije in oblikovanju predloge za poročila o razmerah za opis tehničnega vzroka in posledic kibernetskovarnostnih incidentov bi bilo treba upoštevati tekoče delo v zvezi s priglasitvijo incidentov v okviru izvajanja Direktive (EU) 2022/2555.

(19) Da bi omogočili obsežno izmenjavo podatkov o kibernetskovarnostnih grožnjah iz različnih virov v zaupanja vrednem okolju, bi morali biti subjekti, ki sodelujejo v

evropskem kibernetskem ščitu, opremljeni z najsodobnejšimi in izjemno varnimi orodji, opremo in infrastrukturami. To bi moralo omogočiti izboljšanje skupnih zmogljivosti za odkrivanje in pravočasno opozarjanje organov in ustreznih subjektov, zlasti z uporabo najnovejših tehnologij umetne inteligence in podatkovne analitike.

(20) Evropski kibernetski ščit bi moral z zbiranjem, deljenjem in izmenjavanjem podatkov okrepiti tehnološko suverenost Unije. Zbiranje visokokakovostnih pripravljenih podatkov bi moralo prispevati tudi k razvoju naprednih tehnologij umetne inteligence in podatkovne analitike. Olajšati bi ga bilo treba tako, da se evropski kibernetski ščit poveže z infrastrukturo vseevropskega visokozmogljivostnega računalništva, vzpostavljenega z Uredbo Sveta (EU) 2021/1173[13].

(21) Čeprav je evropski kibernetski ščit civilni projekt, bi lahko imela skupnost za kibernetsko obrambo koristi od okrepljenih zmogljivosti civilnega odkrivanja in situacijskega zavedanja, ki so bile razvite za zaščito kritične infrastrukture. Čezmejni centri za varnostne operacije bi morali ob podpori Komisije in Evropskega kompetenčnega centra za kibernetsko varnost (v nadaljnjem besedilu: ECCC) ter v sodelovanju z visokim predstavnikom Unije za zunanje zadeve in varnostno politiko (v nadaljnjem besedilu: visoki predstavnik) postopoma razviti namenske protokole in standarde, da se omogoči sodelovanje s skupnostjo za kibernetsko obrambo, vključno s pogoji preverjanja in varnostnimi pogoji. Razvoj evropskega kibernetskega ščita bi moral spremljati razmislek, na podlagi katerega bi bilo v tesnem sodelovanju z visokim predstavnikom omogočeno prihodnje sodelovanje z mrežami in platformami, odgovornimi za izmenjavo informacij v skupnosti za kibernetsko obrambo.

(22) Izmenjava informacij med sodelujočimi v evropskem kibernetskem ščitu bi morala biti skladna z obstoječimi pravnimi zahtevami, zlasti s pravom Unije in nacionalnim pravom o varstvu podatkov, ter pravili Unije o konkurenci, ki urejajo izmenjavo informacij. Prejemnik informacij bi moral, če je potrebna obdelava osebnih podatkov, izvajati tehnične in organizacijske ukrepe, ki varujejo pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in podatke uničiti takoj, ko niso več potrebni za navedeni namen, ter organ, ki daje podatke na voljo, obvestiti, da so bili podatki uničeni.

(23) Brez poseganja v člen 346 PDEU bi morala biti izmenjava informacij, ki so zaupne v skladu s pravili Unije ali nacionalnimi pravili, omejena na to, kar je ustrezno za namen te izmenjave in sorazmerno z njim. Pri izmenjavi takih informacij bi bilo treba ohraniti njihovo zaupnost ter zaščititi varnostne in poslovne interese zadevnih subjektov ob polnem spoštovanju trgovinskih in poslovnih skrivnosti.

(24) Glede na vse večja tveganja in število kibernetskovarnostnih incidentov, ki prizadenejo države članice, je treba vzpostaviti instrument podpore ob krizi, da se izboljša odpornost Unije proti pomembnim kibernetskovarnostnim incidentom in takim incidentom velikih razsežnosti ter da se ukrepi držav članic dopolnijo z nujno finančno podporo za pripravljenost, odzivanje in takojšnje okrevanje bistvenih storitev. Ta instrument bi moral omogočiti hitro zagotavljanje pomoči v določenih okoliščinah in pod jasnimi pogoji ter skrbno spremljanje in ocenjevanje porabe sredstev. Čeprav so za preprečevanje kibernetskovarnostnih incidentov in kriz ter pripravo in odzivanje nanje v prvi vrsti odgovorne države članice, mehanizem za

[13] Uredba Sveta (EU) 2021/1173 z dne 13. julija 2021 o ustanovitvi Skupnega podjetja za evropsko visokozmogljivostno računalništvo in razveljavitvi Uredbe (EU) 2018/1488 (UL L 256, 19.7.2021, str. 3).

izredne kibernetske razmere spodbuja solidarnost med državami članicami v skladu s členom 3(3) Pogodbe o Evropski uniji (PEU).

(25) Mehanizem za izredne kibernetske razmere bi moral državam članicam zagotoviti podporo z dopolnjevanjem njihovih ukrepov in virov ter druge obstoječe možnosti podpore v primeru odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter takojšnjega okrevanja po njih, kot so storitve, ki jih zagotavlja Agencija Evropske unije za kibernetsko varnost (ENISA) v skladu s svojim mandatom, usklajen odziv in pomoč mreže skupin CSIRT, podpora mreže EU-CyCLONe pri ublažitvi posledic ter medsebojna pomoč med državami članicami, med drugim v okviru člena 42(7) PEU, enot za hitro odzivanje na kibernetske grožnje v okviru stalnega strukturnega sodelovanja (PESCO)[14] in skupin za hitro odzivanje na hibridne grožnje. Obravnavati bi moral potrebo po zagotavljanju razpoložljivosti specializiranih sredstev za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente po vsej Uniji in v tretjih državah.

(26) Ta instrument ne posega v postopke in okvire za usklajevanje odzivanja na krize na ravni Unije, zlasti mehanizem Unije na področju civilne zaščite[15], enotno ureditev za politično odzivanje na krize[16,] in Direktivo (EU) 2022/2555. Prispeva lahko k ukrepom, ki se izvajajo v okviru člena 42(7) PEU ali v primerih, opredeljenih v členu 222 PDEU, ali jih dopolnjuje. Uporabo tega instrumenta bi bilo treba po potrebi uskladiti tudi z izvajanjem ukrepov iz zbirke orodij za kibernetsko diplomacijo.

(27) Pomoč, zagotovljena na podlagi te uredbe, bi morala podpirati in dopolnjevati ukrepe, ki jih države članice sprejmejo na nacionalni ravni. V ta namen bi bilo treba zagotoviti tesno sodelovanje in posvetovanje med Komisijo in prizadeto državo članico. Kadar država članica zaprosi za podporo v okviru mehanizma za izredne kibernetske razmere, bi morala predložiti ustrezne informacije, s katerimi utemelji potrebo po podpori.

(28) V skladu z Direktivo (EU) 2022/2555 morajo države članice imenovati ali ustanoviti enega ali več organov za obvladovanje kibernetskih kriz ter jim zagotoviti ustrezna sredstva za učinkovito in uspešno izvajanje nalog. Države članice morajo tudi določiti zmogljivosti, sredstva in postopke, ki se lahko uporabijo v primeru krize, ter sprejeti nacionalni načrt za odzivanje na kibernetskovarnostne incidente velikih razsežnosti in krize, v katerem so opredeljeni cilji in ureditve obvladovanja kibernetskovarnostnih incidentov velikih razsežnosti in kriz. Prav tako morajo ustanoviti eno ali več skupin CSIRT, ki bodo pristojne za obvladovanje incidentov v skladu z natančno določenim postopkom in bodo zajemale vsaj sektorje, podsektorje in vrste subjektov, ki spadajo na področje uporabe navedene direktive, ter jim zagotoviti ustrezna sredstva za učinkovito izvajanje nalog. Ta uredba ne posega v vlogo Komisije pri zagotavljanju skladnosti držav članic z obveznostmi iz Direktive (EU) 2022/2555. Mehanizem za izredne kibernetske razmere bi moral zagotavljati pomoč za ukrepe, namenjene krepitvi pripravljenosti, in ukrepe za odzivanje na incidente, da bi ublažili posledice pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti, podprli takojšnje okrevanje in/ali ponovno vzpostavili delovanje bistvenih storitev.

---

14 Sklep Sveta (SZVP) 2017/2315 z dne 11. decembra 2017 o vzpostavitvi stalnega strukturnega sodelovanja (PESCO) in določitvi seznama sodelujočih držav članic.

15 Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924).

16 Enotna ureditev za politično odzivanje na krize (IPCR) in v skladu s Priporočilom Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize.

(29) V okviru ukrepov pripravljenosti bi bilo treba za spodbujanje doslednega pristopa ter krepitev varnosti po vsej Uniji in na njenem notranjem trgu zagotoviti podporo za usklajeno preskušanje in ocenjevanje kibernetske varnosti subjektov, ki delujejo v visoko kritičnih sektorjih, opredeljenih v skladu z Direktivo (EU) 2022/2555. V ta namen bi morala Komisija ob podpori agencije ENISA in v sodelovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov, ustanovljeno z Direktivo (EU) 2022/2555, redno določati ustrezne sektorje ali podsektorje, ki bi morali biti upravičeni do finančne podpore za usklajeno preskušanje na ravni Unije. Sektorje ali podsektorje bi bilo treba izbrati iz Priloge I k Direktivi (EU) 2022/2555 (v nadaljnjem besedilu: visoko kritični sektorji). Usklajeno preskušanje bi moralo temeljiti na skupnih scenarijih tveganja in metodologijah. Pri izbiri sektorjev in razvoju scenarijev tveganja bi bilo treba upoštevati ustrezne ocene tveganja in scenarije tveganja po vsej Uniji, vključno s potrebo po preprečevanju podvajanja, kot so ocena tveganja in scenariji tveganja, h katerim poziva Svet v svojih sklepih o oblikovanju kibernetske drže Evropske unije in ki jih morajo izvesti Komisija, visoki predstavnik in skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju z ustreznimi civilnimi in vojaškimi organi in agencijami ter vzpostavljenimi mrežami, med drugim mrežo EU-CyCLONe, pa tudi ocena tveganja komunikacijskih omrežij in infrastruktur, ki se zahteva na podlagi skupnega ministrskega poziva iz Neversa ter jo izvede skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov ob podpori Komisije in agencije ENISA ter v sodelovanju z Organom evropskih regulatorjev za elektronske komunikacije (BEREC), usklajene ocene tveganja, ki se izvedejo v skladu s členom 22 Direktive (EU) 2022/2555, in testiranje digitalne operativne odpornosti, kot je določeno v Uredbi (EU) 2022/2554 Evropskega parlamenta in Sveta[17]. Pri izbiri sektorjev bi bilo treba upoštevati tudi priporočilo Sveta o usklajenem vseevropskem pristopu za krepitev odpornosti kritične infrastrukture.

(30) Poleg tega bi moral mehanizem za izredne kibernetske razmere zagotavljati podporo za druge ukrepe pripravljenosti in podpirati pripravljenost v drugih sektorjih, ki jih usklajeno preskušanje subjektov, ki delujejo v visoko kritičnih sektorjih, ne zajema. Ti ukrepi bi lahko vključevali različne vrste nacionalnih dejavnosti na področju pripravljenosti.

(31) Mehanizem za izredne kibernetske razmere bi moral zagotavljati tudi podporo za ukrepe za odzivanje na incidente za ublažitev posledic pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti, da bi se podprlo takojšnje okrevanje ali ponovna vzpostavitev delovanja bistvenih storitev. Kjer je ustrezno, bi moral dopolnjevati mehanizem Unije na področju civilne zaščite, da se zagotovi celovit pristop k odzivanju na posledice kibernetskih incidentov za državljane.

(32) Mehanizem za izredne kibernetske razmere bi moral podpreti pomoč, ki jo države članice zagotovijo državi članici, ki jo je prizadel pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, med drugim pomoč mreže skupin CSIRT iz člena 15 Direktive (EU) 2022/2555. Državam članicam, ki zagotovijo pomoč, bi bilo treba dovoliti, da vložijo zahtevke za kritje stroškov, povezanih s pošiljanjem strokovnih skupin v okviru medsebojne pomoči. Upravičeni stroški bi lahko

[17] Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011.

vključevali potne stroške, stroške nastanitve in dnevnice strokovnjakov na področju kibernetske varnosti.

(33) Postopno bi bilo treba vzpostaviti kibernetskovarnostno rezervo na ravni Unije, ki bi zajemala storitve zasebnih ponudnikov upravljanih varnostnih storitev za podporo ukrepom odzivanja in takojšnjega okrevanja v primeru pomembnih kibernetskovarnostnih incidentov ali takih incidentov velikih razsežnosti. Kibernetskovarnostna rezerva EU bi morala zagotoviti razpoložljivost in pripravljenost storitev. Storitve iz kibernetskovarnostne rezerve EU bi morale biti namenjene podpori nacionalnim organom pri zagotavljanju pomoči prizadetim subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih, kot dopolnitev njihovih ukrepov na nacionalni ravni. Države članice bi morale ob vložitvi zahtevka za podporo iz kibernetskovarnostne rezerve EU opredeliti podporo, zagotovljeno prizadetemu subjektu na nacionalni ravni, ki bi jo bilo treba upoštevati pri oceni zahtevka države članice. Storitve iz kibernetskovarnostne rezerve EU se lahko pod podobnimi pogoji uporabljajo tudi za podporo institucijam, organom, uradom in agencijam Unije.

(34) Za izbor zasebnih ponudnikov storitev, ki bi storitve zagotavljali v okviru kibernetskovarnostne rezerve EU, je treba določiti sklop minimalnih meril, ki bi jih bilo treba vključiti v razpis za zbiranje ponudb za izbor teh ponudnikov, da se lahko izpolnijo potrebe organov držav članic in subjektov, ki delujejo v kritičnih ali visoko kritičnih sektorjih.

(35) Komisija bi lahko za podporo vzpostavitvi kibernetskovarnostne rezerve EU preučila možnost, da od agencije ENISA zahteva, naj pripravi predlog certifikacijske sheme v skladu z Uredbo (EU) 2019/881 za upravljane varnostne storitve na področjih, ki jih zajema mehanizem za izredne kibernetske razmere.

(36) Za podporo ciljem te uredbe glede spodbujanja skupnega situacijskega zavedanja, krepitve odpornosti Unije ter omogočanja učinkovitega odziva na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti bi bilo treba mreži EU-CyCLONe, mreži skupin CSIRT ali Komisiji omogočiti, da agencijo ENISA zaprosijo, naj pregleda in oceni grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Po zaključku pregleda in ocene incidenta bi morala agencija ENISA v sodelovanju z ustreznimi deležniki, vključno s predstavniki iz zasebnega sektorja, držav članic, Komisije in drugih ustreznih institucij, organov, uradov in agencij EU, pripraviti poročilo o pregledu incidenta. Kar zadeva zasebni sektor, agencija ENISA razvija kanale za izmenjavo informacij s specializiranimi ponudniki, vključno s ponudniki upravljanih varnostnih rešitev in prodajalci, da bi prispevala k svojemu poslanstvu doseganja visoke skupne ravni kibernetske varnosti po vsej Uniji. Cilj poročila o pregledu posameznih incidentov, ki temelji na sodelovanju z deležniki, vključno z zasebnim sektorjem, bi moral biti ocena vzrokov, posledic in blažitev incidenta po njegovem nastanku. Posebno pozornost bi bilo treba nameniti prispevku in spoznanjem, ki si jih izmenjujejo ponudniki upravljanih varnostnih storitev, ki izpolnjujejo pogoje največje poklicne integritete, nepristranskosti in potrebnega tehničnega strokovnega znanja, kot se zahtevajo s to uredbo. Poročilo bi bilo treba predložiti mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji, pri čemer bi ga te morale upoštevati pri svojem delu. Če je incident povezan s tretjo državo, bo Komisija poročilo poslala tudi visokemu predstavniku.

(37) Ob upoštevanju nepredvidljive narave kibernetskih napadov in dejstva, da ti pogosto niso omejeni na določeno geografsko območje in da predstavljajo veliko tveganje

prelivanja, krepitev odpornosti sosednjih držav in njihove zmogljivosti za učinkovito odzivanje na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti prispeva k zaščiti Unije kot celote. Zato lahko podporo iz kibernetskovarnostne rezerve EU prejmejo tretje države, pridružene programu Digitalna Evropa, če je to določeno v ustreznih sporazumih o pridružitvi programu Digitalna Evropa. Unija bi morala financiranje za pridružene tretje države podpreti v okviru ustreznih partnerstev in instrumentov financiranja za te države. Podpora bi morala zajemati storitve na področju odzivanja na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnjega okrevanja po njih. Pri zagotavljanju podpore tretjim državam, pridruženim programu Digitalna Evropa, bi se morali uporabljati pogoji, določeni za kibernetskovarnostno rezervo EU in zaupanja vredne ponudnike v tej uredbi.

(38) Za zagotovitev enotnih pogojev za izvajanje te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila za določitev pogojev za interoperabilnost med čezmejnimi centri za varnostne operacije; določitev postopkovnih ureditev za izmenjavo informacij v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti med čezmejnimi centri za varnostne operacije in subjekti Unije; določitev tehničnih zahtev za zagotovitev varnosti evropskega kibernetskega ščita; določitev vrst in števila storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU, in natančnejšo opredelitev podrobnih ureditev za dodeljevanje storitev podpore iz kibernetskovarnostne rezerve EU. Navedena pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta.

(39) Cilj te uredbe je lažje doseči na ravni Unije kot na ravni držav članic. Zato lahko Unija sprejme ukrepe v skladu z načeloma subsidiarnosti in sorazmernosti iz člena 5 Pogodbe o Evropski uniji. Ta uredba ne presega tistega, kar je nujno za dosego tega cilja –

SPREJELA NASLEDNJO UREDBO:

Poglavje I

SPLOŠNI CILJI, PREDMET UREJANJA IN OPREDELITVE POJMOV

Člen 1

Predmet urejanja in cilji

1. Ta uredba določa ukrepe za okrepitev zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje, ki se uresničujejo zlasti z naslednjimi ukrepi:

(a) vzpostavitvijo vseevropske infrastrukture centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) za vzpostavitev in okrepitev skupnih zmogljivosti za odkrivanje in situacijsko zavedanje;

(b) vzpostavitvijo mehanizma za izredne kibernetske razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih;

(c) vzpostavitvijo evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov za pregledovanje in ocenjevanje pomembnih incidentov ali incidentov velikih razsežnosti.

2. Cilj te uredbe je okrepiti solidarnost na ravni Unije z naslednjimi specifičnimi cilji:

(a) okrepiti skupno odkrivanje kibernetskih groženj in incidentov v Uniji ter situacijsko zavedanje o njih, da se tako okrepi konkurenčni položaj industrijskega in storitvenega sektorja v Uniji v celotnem spletnem gospodarstvu ter prispeva k tehnološki suverenosti Unije na področju kibernetske varnosti;

(b) okrepiti pripravljenost subjektov, ki delujejo v kritičnih in visoko kritičnih sektorjih po vsej Uniji, ter solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore Unije pri odzivanju na kibernetskovarnostne incidente tretjim državam, pridruženim programu Digitalna Evropa;

(c) povečati odpornost Unije in prispevati k učinkovitemu odzivanju s pregledovanjem in ocenjevanjem pomembnih kibernetskovarnostnih incidentov ali takih incidentov velikih razsežnosti, med drugim na podlagi pridobljenih spoznanj in po potrebi priporočil.

3. Ta uredba ne posega v primarno odgovornost držav članic za nacionalno varnost, javno varnost ter preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

Člen 2

Opredelitve pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „**čezmejni center za varnostne operacije**“ pomeni večdržavno platformo, ki v usklajeni mrežni strukturi združuje nacionalne centre za varnostne operacije iz vsaj treh držav članic, ki sestavljajo gostiteljski konzorcij, in je namenjena preprečevanju kibernetskih groženj in incidentov ter podpiranju priprave visokokakovostnih obveščevalnih podatkov, zlasti z izmenjavanjem podatkov iz različnih virov, javnih in zasebnih, pa tudi z izmenjavanjem najsodobnejših orodij in skupnim razvijanjem kibernetskih zmogljivosti za odkrivanje, analizo ter preprečevanje in zaščito v zaupanja vrednem okolju;

(2) „**javni organ**“ pomeni osebo javnega prava, kot je opredeljena v členu 2(1), točka 4, Direktive 2014/24/EU Evropskega parlamenta in Sveta[18];

(3) „**gostiteljski konzorcij**“ pomeni konzorcij sodelujočih držav, ki jih zastopajo nacionalni centri za varnostne operacije in ki so se dogovorile, da bodo vzpostavile

[18] Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

orodja in infrastrukturo ter prispevale k pridobivanju teh orodij in infrastrukture za čezmejni center za varnostne operacije in njegovo delovanje;

(4) „**subjekt**“ pomeni subjekt, kot je opredeljen v členu 6, točka 38, Direktive (EU) 2022/2555;

(5) „**subjekti, ki delujejo v kritičnih ali visoko kritičnih sektorjih**“, pomeni vrsto subjektov s seznamov v prilogah I in II k Direktivi (EU) 2022/2555;

(6) „**kibernetska grožnja**“ pomeni kibernetsko grožnjo, kot je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(7) „**pomemben kibernetskovarnostni incident**“ pomeni kibernetskovarnostni incident, ki izpolnjuje merila iz člena 23(3) Direktive (EU) 2022/2555;

(8) „**kibernetskovarnostni incident velikih razsežnosti**“ pomeni incident, kot je opredeljen v členu 6, točka 7, Direktive (EU)2022/2555;

(9) „**pripravljenost**“ pomeni stanje pripravljenosti in zmogljivost za zagotovitev učinkovitega hitrega odziva na pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, ki se doseže na podlagi vnaprej izvedene ocene tveganja in vnaprej sprejetih ukrepov za spremljanje;

(10) „**odziv**“ pomeni ukrepanje v primeru pomembnega kibernetskovarnostnega incidenta ali takega incidenta velikih razsežnosti oziroma med takim incidentom ali po njem za odpravo njegovih takojšnjih in kratkoročnih negativnih posledic;

(11) „**zaupanja vredni ponudniki**“ pomeni ponudnike upravljanih varnostnih storitev, kot so opredeljeni v členu 6, točka 40, Direktive (EU) 2022/2555, izbrane v skladu s členom 16 te uredbe.

Poglavje II

EVROPSKI KIBERNETSKI ŠČIT

Člen 3

Vzpostavitev evropskega kibernetskega ščita

1. Vzpostavi se medsebojno povezana vseevropska infrastruktura centrov za varnostne operacije (v nadaljnjem besedilu: evropski kibernetski ščit) za razvoj naprednih zmogljivosti Unije za odkrivanje, analiziranje in obdelavo podatkov o kibernetskih grožnjah in incidentih v Uniji. Ščit sestavljajo vsi nacionalni centri za varnostne operacije in čezmejni centri za varnostne operacije.

Ukrepi za izvajanje evropskega kibernetskega ščita se podprejo s sredstvi iz programa Digitalna Evropa, izvajajo pa se v skladu z Uredbo (EU) 2021/694 in zlasti specifičnim ciljem 3 Uredbe.

2. Evropski kibernetski ščit:

(a) prek čezmejnih centrov za varnostne operacije zbira in izmenjuje podatke o kibernetskih grožnjah in incidentih iz različnih virov;

(b) z uporabo najsodobnejših orodij, zlasti tehnologij umetne inteligence in podatkovne analitike, zagotavlja visokokakovostne, uporabne informacije in obveščevalne podatke o kibernetskih grožnjah;

(c) prispeva k boljši zaščiti proti kibernetskim grožnjam in k boljšemu odzivanju nanje;

(d) prispeva k hitrejšemu odkrivanju kibernetskih groženj in situacijskemu zavedanju o njih po vsej Uniji;

(e) skupnosti za kibernetsko varnost v Uniji zagotavlja storitve in dejavnosti, med drugim s prispevanjem k razvoju naprednih orodij umetne inteligence in podatkovne analitike.

Razvije se v sodelovanju z infrastrukturo za vseevropsko visokozmogljivostno računalništvo, vzpostavljeno v skladu z Uredbo (EU) 2021/1173.

Člen 4

Nacionalni centri za varnostne operacije

1. Za sodelovanje v evropskem kibernetskem ščitu vsaka država članica imenuje vsaj en nacionalni center za varnostne operacije. Nacionalni center za varnostne operacije je javni organ.

Lahko deluje kot referenčna točka in točka dostopa do drugih javnih in zasebnih organizacij na nacionalni ravni za zbiranje in analiziranje informacij o kibernetskovarnostnih grožnjah in incidentih ter prispevanje k čezmejnim centrom za varnostne operacije. Opremljen je z najsodobnejšimi tehnologijami, ki so zmožne odkrivanja, združevanja in analiziranja podatkov v zvezi s kibernetskovarnostnimi grožnjami in incidenti.

2. Evropski kompetenčni center za kibernetsko varnost (v nadaljnjem besedilu: ECCC) na podlagi razpisa za prijavo interesa izbere nacionalne centre za varnostne operacije, ki z njim sodelujejo pri skupnem javnem naročanju orodij in infrastruktur. Center ECCC lahko izbranim nacionalnim centrom za varnostne operacije dodeli nepovratna sredstva za financiranje delovanja teh orodij in infrastruktur. Finančni prispevek Unije krije do 50 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije država članica. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in nacionalni center za varnostne operacije skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.

3. Nacionalni center za varnostne operacije, izbran v skladu z odstavkom 2, se zaveže, da bo za sodelovanje v čezmejnem centru za varnostne operacije zaprosil v dveh letih od datuma pridobitve orodij in infrastruktur ali datuma prejema nepovratnih sredstev, kateri koli nastopi prej. Če nacionalni center za varnostne operacije do takrat ne sodeluje v čezmejnem centru za varnostne operacije, ni upravičen do dodatne podpore Unije v skladu s to uredbo.

Člen 5

Čezmejni centri za varnostne operacije

1. Gostiteljski konzorcij, ki ga sestavljajo vsaj tri države članice, ki jih zastopajo nacionalni centri za varnostne operacije, ki so se zavezali skupnemu usklajevanju dejavnosti odkrivanja in spremljanja kibernetskih groženj, je upravičen do sodelovanja pri ukrepih za ustanovitev čezmejnega centra za varnostne operacije.

2. Center ECCC na podlagi razpisa za prijavo interesa izbere gostiteljski konzorcij, ki z njim sodeluje pri skupnem javnem naročanju orodij in infrastruktur. Gostiteljskemu konzorciju lahko dodeli nepovratna sredstva za financiranje delovanja orodij in infrastruktur. Finančni prispevek Unije krije do 75 % stroškov pridobitve orodij in infrastruktur ter do 50 % operativnih stroškov, preostale stroške pa krije gostiteljski konzorcij. Pred začetkom postopka za pridobitev orodij in infrastruktur center ECCC in gostiteljski konzorcij skleneta sporazum o gostiteljstvu in uporabi, ki ureja uporabo orodij in infrastruktur.

3. Članice gostiteljskega konzorcija sklenejo pisno konzorcijsko pogodbo, v kateri so določene njihove notranje ureditve za izvajanje sporazuma o gostiteljstvu in uporabi.

4. Čezmejni center za varnostne operacije za pravne namene zastopa nacionalni center za varnostne operacije, ki deluje kot usklajevalni center za varnostne operacije, ali gostiteljski konzorcij, če je ta pravna oseba. Usklajevalni center za varnostne operacije je odgovoren za zagotavljanje skladnosti z zahtevami iz sporazuma o gostiteljstvu in uporabi ter te uredbe.

Člen 6

Sodelovanje in izmenjava informacij v čezmejnih centrih za varnostne operacije in med njimi

1. Članice gostiteljskega konzorcija si v okviru čezmejnega centra za varnostne operacije izmenjujejo ustrezne informacije, vključno z informacijami, ki se nanašajo na kibernetske grožnje, skorajšnje incidente, ranljivosti, tehnike in postopke, kazalnike ogroženosti, sovražne taktike, specifične informacije o grožnji in akterju, opozorila glede kibernetske varnosti in priporočila glede konfiguracije orodij za kibernetsko varnost za zaznavo kibernetskih napadov, kadar taka izmenjava informacij:

(a) stremi k preprečevanju in odkrivanju incidentov, odzivanju nanje ali okrevanju po njih ali k ublažitvi njihovih posledic;

(b) zvišuje raven kibernetske varnosti, zlasti z ozaveščanjem v zvezi s kibernetskimi grožnjami, omejevanjem ali oviranjem zmožnosti širjenja takih groženj, podpiranjem vrste obrambnih zmogljivosti, odpravljanjem in razkrivanjem ranljivosti, tehnikami odkrivanja, omejevanja in preprečevanja groženj, strategijami za zmanjšanje tveganja ali fazami odzivanja in okrevanja ali spodbujanjem sodelovanja med javnimi in zasebnimi subjekti pri raziskovanju kibernetskih groženj.

2. V pisni konzorcijski pogodbi iz člena 5(3) se določijo:

(a) zaveza souporabi znatne količine podatkov iz odstavka 1 in pogoji, pod katerimi se te informacije izmenjujejo;

(b) okvir upravljanja, ki spodbuja izmenjavo informacij med vsemi sodelujočimi;

(c) cilji za prispevek k razvoju naprednih orodij umetne inteligence in podatkovne analitike.

3. Da bi spodbudili izmenjavo informacij med čezmejnimi centri za varnostne operacije, ti zagotovijo visoko raven medsebojne interoperabilnosti. Za spodbujanje interoperabilnosti med čezmejnimi centri za varnostne operacije lahko Komisija z izvedbenimi akti in po posvetovanju s centrom ECCC določi pogoje za to interoperabilnost. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2) te uredbe.

4. Čezmejni centri za varnostne operacije med seboj sklenejo sporazume o sodelovanju, v katerih določijo načela izmenjave informacij med čezmejnimi platformami.

Člen 7

Sodelovanje in izmenjava informacij s subjekti Unije

1. Kadar čezmejni centri za varnostne operacije pridobijo informacije v zvezi z morebitnim ali tekočim kibernetskovarnostnim incidentom velikih razsežnosti, ustrezne informacije nemudoma zagotovijo mreži EU-CyCLONe, mreži skupin CSIRT in Komisiji glede na njihove vloge pri kriznem upravljanju v skladu z Direktivo (EU) 2022/2555.

2. Komisija lahko z izvedbenimi akti določi postopkovne ureditve za izmenjavo informacij iz odstavka 1. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2) te uredbe.

Člen 8

Varnost

1. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo visoko raven varnosti podatkov in fizične varnosti infrastrukture evropskega kibernetskega ščita ter ustrezno upravljanje in nadzor infrastrukture, tako da je ta zaščitena pred grožnjami ter da sta zagotovljeni njena varnost in varnost sistemov, med drugim varnost podatkov, ki se izmenjujejo prek infrastrukture.

2. Države članice, ki sodelujejo v evropskem kibernetskem ščitu, zagotovijo, da izmenjava informacij v okviru evropskega kibernetskega ščita s subjekti, ki niso javni organi držav članic, nima negativnih posledic za varnostne interese Unije.

3. Komisija lahko sprejme izvedbene akte, s katerimi določi tehnične zahteve za države članice glede izpolnjevanja njihove obveznosti iz odstavkov 1 in 2. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2) te uredbe. Pri tem Komisija ob podpori visokega predstavnika upošteva ustrezne varnostne standarde na ravni obrambe, da bi se olajšalo sodelovanje z vojaškimi akterji.

Poglavje III

MEHANIZEM ZA IZREDNE KIBERNETSKE RAZMERE

Člen 9

Vzpostavitev mehanizma za izredne kibernetske razmere

1. Vzpostavi se mehanizem za izredne kibernetske razmere za povečanje odpornosti Unije proti večjim kibernetskovarnostnim grožnjam ter pripravo na kratkoročne posledice pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti in njihovo ublažitev v duhu solidarnosti (v nadaljnjem besedilu: mehanizem).

2. Ukrepi za izvajanje mehanizma za izredne kibernetske razmere se podprejo s sredstvi iz programa Digitalna Evropa, izvajajo pa se v skladu z Uredbo (EU) 2021/694 in zlasti specifičnim ciljem 3 Uredbe.

Člen 10

Vrsta ukrepov

1. Mehanizem podpira naslednje vrste ukrepov:

(a) ukrepe pripravljenosti, vključno z usklajenim preskušanjem pripravljenosti subjektov, ki delujejo v visoko kritičnih sektorjih po vsej Uniji;

(b) ukrepe za odzivanje za podporo odzivu in takojšnjemu okrevanju po pomembnih kibernetskovarnostnih incidentih in takih incidentih velikih razsežnosti, pri čemer ukrepe zagotovijo zaupanja vredni ponudniki, ki sodelujejo v kibernetskovarnostni rezervi EU, vzpostavljeni v skladu s členom 12;

(c) ukrepe medsebojne pomoči, ki vključujejo pomoč, ki jo nacionalni organi ene države članice zagotovijo drugi državi članici, zlasti kot je določeno v členu 11(3), točka (f), Direktive (EU) 2022/2555.

Člen 11

Usklajeno preskušanje pripravljenosti subjektov

1. Da bi Komisija podprla usklajeno preskušanje pripravljenosti subjektov iz člena 10(1), točka (a), po vsej Uniji, po posvetovanju s skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov in agencijo ENISA med visoko kritičnimi sektorji, navedenimi v Prilogi I k Direktivi (EU) 2022/2555, opredeli zadevne sektorje ali podsektorje, katerih subjekti so lahko predmet usklajenega preskušanja pripravljenosti, ob upoštevanju obstoječih in načrtovanih usklajenih ocen tveganja in testiranja odpornosti na ravni Unije.

2. Skupina za sodelovanje na področju varnosti omrežnih in informacijskih sistemov v sodelovanju s Komisijo, agencijo ENISA in visokim predstavnikom razvije skupne scenarije tveganja in metodologije za usklajeno preskušanje.

Člen 12

Vzpostavitev kibernetskovarnostne rezerve EU

1. Vzpostavi se kibernetskovarnostna rezerva EU za pomoč uporabnikom iz odstavka 3 pri odzivanju ali zagotavljanju podpore pri odzivanju na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti ter pri takojšnjem okrevanju po takih incidentih.

2. Kibernetskovarnostno rezervo EU sestavljajo storitve za odzivanje na incidente, ki jih zagotovijo zaupanja vredni ponudniki, izbrani v skladu z merili iz člena 16. Rezerva vključuje storitve, k zagotavljanju katerih se ponudniki zavežejo vnaprej. Storitve se lahko uporabljajo v vseh državah članicah.

3. Uporabniki storitev iz kibernetskovarnostne rezerve EU so:

(a) organi držav članic za obvladovanje kibernetskih kriz in skupine CSIRT iz člena 9(1) in (2) oziroma člena 10 Direktive (EU) 2022/2555;

(b) institucije, organi, uradi in agencije Unije.

4. Uporabniki iz odstavka 3, točka (a), storitve iz kibernetskovarnostne rezerve EU uporabljajo za odzivanje na pomembne incidente ali incidente velikih razsežnosti, ki prizadenejo subjekte, ki delujejo v kritičnih ali visoko kritičnih sektorjih, ali za podporo odzivanju nanje in takojšnjemu okrevanju po njih.

5. Za izvajanje kibernetskovarnostne rezerve EU je v celoti odgovorna Komisija. Komisija določi prednostne naloge in razvoj kibernetskovarnostne rezerve EU v skladu z zahtevami uporabnikov iz odstavka 3, nadzoruje njeno izvajanje ter zagotovi dopolnjevanje, doslednost, sinergije in povezave z drugimi podpornimi ukrepi na podlagi te uredbe, pa tudi drugimi ukrepi in programi Unije.

6. Komisija lahko delovanje in upravljanje kibernetskovarnostne rezerve EU s sporazumi o prispevku v celoti ali delno zaupa agenciji ENISA.

7. Da bi agencija ENISA podprla Komisijo pri vzpostavitvi kibernetskovarnostne rezerve EU, po posvetovanju z državami članicami in Komisijo pripravi pregled potrebnih storitev. Po posvetovanju s Komisijo pripravi podoben pregled za opredelitev potreb tretjih držav, upravičenih do podpore iz kibernetskovarnostne rezerve EU v skladu s členom 17. Komisija se po potrebi posvetuje z visokim predstavnikom.

8. Komisija lahko z izvedbenimi akti določi vrste in število storitev za odzivanje, potrebnih za kibernetskovarnostno rezervo EU. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2).

Člen 13

Zahtevki za podporo iz kibernetskovarnostne rezerve EU

1. Uporabniki iz člena 12(3) lahko zahtevajo storitve iz kibernetskovarnostne rezerve EU, da bi podprli odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti in takojšnje okrevanje po njih.

2. Da bi uporabniki iz člena 12(3) prejeli podporo iz kibernetskovarnostne rezerve EU, sprejmejo ukrepe za ublažitev učinkov incidenta, v zvezi s katerim zahtevajo podporo, med drugim lahko zagotovijo neposredno tehnično pomoč in druge vire za pomoč pri odzivanju na incident ter si prizadevajo za takojšnje okrevanje.

3. Zahtevki za podporo uporabnikov iz člena 12(3), točka (a), te uredbe se Komisiji in agenciji ENISA pošljejo prek enotne kontaktne točke, ki jo država članica imenuje ali vzpostavi v skladu s členom 8(3) Direktive (EU) 2022/2555.

4. Države članice o zahtevkih za podporo pri odzivanju na incidente in takojšnjem okrevanju po njih v skladu s tem členom obvestijo mrežo skupin CSIRT in po potrebi mrežo EU-CyCLONe.

5. Zahtevki za podporo pri odzivanju na incidente in takojšnjem okrevanju po njih vključujejo:

(a) ustrezne informacije o prizadetem subjektu in morebitnih posledicah incidenta ter načrtovani uporabi zahtevane podpore, vključno z navedbo ocenjenih potreb;

(b) informacije o ukrepih, sprejetih za ublažitev incidenta, v zvezi s katerim se zahteva podpora, kot je navedeno v odstavku 2;

(c) informacije o drugih oblikah podpore, ki so na voljo prizadetemu subjektu, vključno s pogodbenimi dogovori, vzpostavljenimi za storitve odzivanja na incidente in takojšnjega okrevanja po njih, ter zavarovalnimi pogodbami, ki bi lahko krile tovrstne incidente.

6. Agencija ENISA v sodelovanju s Komisijo in skupino za sodelovanje na področju varnosti omrežnih in informacijskih sistemov pripravi predlogo za lažjo predložitev zahtevkov za podporo iz kibernetskovarnostne rezerve EU.

7. Komisija lahko z izvedbenimi akti natančneje določi podrobne ureditve za dodeljevanje storitev podpore iz kibernetskovarnostne rezerve EU. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 21(2).

Člen 14

Izvajanje podpore iz kibernetskovarnostne rezerve EU

1. Zahtevke za podporo iz kibernetskovarnostne rezerve EU oceni Komisija ob podpori agencije ENISA ali kot je opredeljeno v sporazumih o prispevku iz člena 12(6), odgovor pa se nemudoma pošlje uporabnikom iz člena 12(3).

2. V primeru več hkratnih zahtevkov se za njihovo prednostno razvrstitev po potrebi upoštevajo naslednja merila:

(a) resnost kibernetskovarnostnega incidenta;

(b) vrsta prizadetega subjekta, pri čemer imajo prednost incidenti, ki prizadenejo bistvene subjekte, kot so opredeljeni v členu 3(1) Direktive (EU) 2022/2555;

(c) morebitne posledice za prizadete države članice ali uporabnike;

(d) morebitna čezmejna narava incidenta in tveganje prelivanja na druge države članice ali uporabnike;

(e) ukrepi, ki jih je uporabnik sprejel za pomoč pri prizadevanjih za odziv in takojšnje okrevanje, kot je navedeno v členu 13(2) in členu 13(5), točka (b).

3. Storitve kibernetskovarnostne rezerve EU se zagotovijo v skladu s posebnimi sporazumi med ponudnikom storitev in uporabnikom, ki mu je zagotovljena podpora v okviru kibernetskovarnostne rezerve EU. Ti sporazumi vključujejo pogoje glede odgovornosti.

4. Sporazumi iz odstavka 3 lahko temeljijo na predlogah, ki jih po posvetovanju z državami članicami pripravi agencija ENISA.

5. Komisija in agencija ENISA ne prevzameta pogodbene odgovornosti za škodo, ki jo tretjim osebam povzročijo storitve, zagotovljene v okviru izvajanja kibernetskovarnostne rezerve EU.

6. Uporabniki v enem mesecu po koncu ukrepa podpore Komisiji in agenciji ENISA predložijo zbirno poročilo o zagotovljeni storitvi, doseženih rezultatih in pridobljenih spoznanjih. Če je uporabnik iz tretje države, kot je določeno v členu 17, se tako poročilo pošlje visokemu predstavniku.

7. Komisija skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov redno poroča o uporabi podpore in njenih rezultatih.

Člen 15

Usklajevanje z mehanizmi kriznega upravljanja

1. Kadar pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti izvirajo iz nesreč, kot so opredeljene v Sklepu št. 1313/2013/EU[19], ali povzročijo take nesreče, podpora za odzivanje na take incidente na podlagi te uredbe dopolnjuje ukrepe na podlagi Sklepa št. 1313/2013/EU in brez poseganja vanj.

2. V primeru čezmejnega kibernetskovarnostnega incidenta velikih razsežnosti, pri katerem se uporabi enotna ureditev za politično odzivanje na krize (IPCR), se podpora iz te uredbe za odziv na tak incident obravnava v skladu z ustreznimi protokoli in postopki iz ureditve IPCR.

3. Na podlagi posvetovanja z visokim predstavnikom lahko podpora v okviru mehanizma za izredne kibernetske razmere dopolnjuje pomoč, zagotovljeno v okviru skupne zunanje in varnostne politike ter skupne varnostne in obrambne politike, med drugim prek enot za hitro odzivanje na kibernetske grožnje. Prav tako lahko dopolnjuje pomoč, ki jo ena država članica zagotavlja drugi državi članici, ali k njej prispeva v okviru člena 42(7) Pogodbe o Evropski uniji.

4. Podpora v okviru mehanizma za izredne kibernetske razmere je lahko del skupnega odziva Unije in držav članic v primerih iz člena 222 Pogodbe o delovanju Evropske unije.

Člen 16

Zaupanja vredni ponudniki

[19] Sklep št. 1313/2013/EU Evropskega parlamenta in Sveta z dne 17. decembra 2013 o mehanizmu Unije na področju civilne zaščite (UL L 347, 20.12.2013, str. 924).

1. Javni naročnik v postopkih javnega naročanja za namene vzpostavitve kibernetskovarnostne rezerve EU ravna v skladu z načeli iz Uredbe (EU, Euratom) 2018/1046 in naslednjimi načeli:

(a) zagotovi, da kibernetskovarnostna rezerva EU vključuje storitve, ki se lahko uvedejo v vseh državah članicah, ob upoštevanju zlasti nacionalnih zahtev za zagotavljanje takih storitev, vključno s certificiranjem ali akreditacijo;

(b) zagotovi zaščito bistvenih varnostnih interesov Unije in njenih držav članic;

(c) zagotovi, da kibernetskovarnostna rezerva EU prinaša dodano vrednost EU s prispevanjem k ciljem iz člena 3 Uredbe (EU) 2021/694, med drugim s spodbujanjem razvoja kibernetskovarnostnih veščin v EU.

2. Javni naročnik pri javnem naročanju storitev za kibernetskovarnostno rezervo EU v dokumente v zvezi z oddajo javnega naročila vključi naslednja merila za izbiro:

(a) ponudnik dokaže, da ima njegovo osebje najvišjo stopnjo poklicne integritete, neodvisnosti, odgovornosti in potrebne tehnične usposobljenosti za izvajanje dejavnosti na specifičnem področju, ter zagotovi stalnost/kontinuiteto strokovnega znanja in potrebne tehnične vire;

(b) ponudnik, njegova odvisna podjetja in podizvajalci imajo vzpostavljen okvir za varovanje občutljivih informacij v zvezi s storitvijo, zlasti dokazov, ugotovitev in poročil, pri čemer je okvir skladen z varnostnimi pravili Unije o varovanju tajnih podatkov EU;

(c) ponudnik predloži zadostne dokaze, da je njegova struktura upravljanja pregledna ter da ne bo ogrozila njegove nepristranskosti in kakovosti njegovih storitev ali povzročila navzkrižja interesov;

(d) ponudnik ima ustrezno varnostno preverjanje, vsaj za osebje, namenjeno uvedbi storitev;

(e) ponudnik zagotavlja ustrezno raven varnosti svojih informacijskih sistemov;

(f) ponudnik je opremljen s tehnično strojno in programsko opremo, potrebno za podporo zahtevani storitvi;

(g) ponudnik je sposoben dokazati, da ima izkušnje z zagotavljanjem podobnih storitev ustreznim nacionalnim organom ali subjektom, ki delujejo v kritičnih ali visoko kritičnih sektorjih;

(h) ponudnik lahko v državah članicah, v katerih lahko opravi storitev, to zagotovi v kratkem času;

(i) ponudnik lahko storitev zagotovi v lokalnem jeziku države članice, v kateri lahko opravi storitev;

(j) ko je vzpostavljena certifikacijska shema EU za upravljane varnostne storitve (Uredba (EU) 2019/881), se ponudnik certificira v skladu z navedeno shemo.

Člen 17

Podpora tretjim državam

1. Tretje države lahko zaprosijo za podporo iz kibernetskovarnostne rezerve EU, če je to določeno v pridružitvenih sporazumih, sklenjenih v zvezi z njihovim sodelovanjem v programu Digitalna Evropa.

2. Podpora iz kibernetskovarnostne rezerve EU je v skladu s to uredbo in izpolnjuje vse posebne pogoje, določene v pridružitvenih sporazumih iz odstavka 1.

3. Uporabniki iz pridruženih tretjih držav, ki so upravičeni do storitev iz kibernetskovarnostne rezerve EU, vključujejo pristojne organe, kot so skupine CSIRT in organi za obvladovanje kibernetskih kriz.

4. Vsaka tretja država, ki je upravičena do podpore iz kibernetskovarnostne rezerve EU, imenuje organ, ki deluje kot enotna kontaktna točka za namene te uredbe.

5. Preden tretje države prejmejo podporo iz kibernetskovarnostne rezerve EU, Komisiji in visokemu predstavniku predložijo informacije o svoji kibernetski odpornosti in zmogljivostih za obvladovanje tveganj, med drugim vsaj informacije o nacionalnih ukrepih, ki so jih sprejele za pripravo na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, ter informacije o odgovornih nacionalnih subjektih, vključno s skupinami CSIRT ali enakovrednimi subjekti, njihovih zmogljivostih in virih, ki so jim dodeljeni. Kadar se določbe členov 13 in 14 te uredbe nanašajo na države članice, se uporabljajo tudi za tretje države, kot je določeno v odstavku 1.

6. Komisija se z visokim predstavnikom uskladi glede prejetih zahtevkov in izvajanja podpore, dodeljene tretjim državam iz kibernetskovarnostne rezerve EU.

Poglavje IV

MEHANIZEM ZA PREGLEDOVANJE KIBERNETSKOVARNOSTNIH INCIDENTOV

Člen 18

Mehanizem za pregledovanje kibernetskovarnostnih incidentov

1. Agencija ENISA na zahtevo Komisije, mreže EU-CyCLONe ali mreže skupin CSIRT pregleda in oceni grožnje, ranljivosti in blažitvene ukrepe v zvezi s posameznim pomembnim kibernetskovarnostnim incidentom ali takim incidentom velikih razsežnosti. Agencija ENISA po zaključku pregleda in ocene incidenta mreži skupin CSIRT, mreži EU-CyCLONe in Komisiji predloži poročilo o pregledu incidenta, da bi jih podprla pri izvajanju njihovih nalog, zlasti nalog iz členov 15 in 16 Direktive (EU) 2022/2555. Komisija poročilo po potrebi posreduje visokemu predstavniku.

2. Agencija ENISA pri pripravi poročila o pregledu incidenta iz odstavka 1 sodeluje z vsemi ustreznimi deležniki, vključno s predstavniki držav članic, Komisijo, drugimi ustreznimi institucijami, organi, uradi in agencijami EU, ponudniki upravljanih varnostnih storitev in uporabniki kibernetskih storitev. Po potrebi sodeluje tudi s subjekti, ki so jih prizadeli pomembni kibernetskovarnostni incidenti ali taki incidenti velikih razsežnosti. Za podporo pregledu se lahko posvetuje tudi z drugimi vrstami deležnikov. Predstavniki, s katerimi se opravi posvetovanje, razkrijejo vsako morebitno navzkrižje interesov.

3. Poročilo zajema pregled in analizo posameznega pomembnega kibernetskovarnostnega incidenta ali takega incidenta velikih razsežnosti, vključno z glavnimi vzroki, ranljivostmi in pridobljenimi spoznanji. V njem so zaupne informacije zavarovane v skladu s pravom Unije ali nacionalnim pravom v zvezi z varstvom občutljivih ali tajnih podatkov.

4. Poročilo po potrebi vsebuje priporočila za izboljšanje kibernetske drže Unije.

5. Kadar je mogoče, se različica poročila javno objavi. Ta različica vključuje samo informacije javnega značaja.

Poglavje V

KONČNE DOLOČBE

Člen 19

Spremembe Uredbe (EU) 2021/694

Uredba (EU) 2021/694 se spremeni:

(1) člen 6 se spremeni:

(a) odstavek 1 se spremeni:

(1) vstavi se naslednja točka (aa):

„(aa) podpora razvoju kibernetskega ščita EU, vključno z razvojem, uvedbo in delovanjem platform nacionalnih in čezmejnih centrov za varnostne operacije, ki prispevajo k situacijskemu zavedanju v Uniji in krepitvi zmogljivosti Unije za pridobivanje obveščevalnih podatkov o kibernetskih grožnjah;“;

(2) doda se naslednja točka (g):

„(g) vzpostavitev in upravljanje mehanizma za izredne kibernetske razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in odzivanju nanje, pri čemer mehanizem dopolnjuje nacionalne vire in zmogljivosti ter druge oblike podpore, ki so na voljo na ravni Unije, vključno z vzpostavitvijo kibernetskovarnostne rezerve EU.“;

(a) odstavek 2 se nadomesti z naslednjim:

„2. Ukrepi v okviru specifičnega cilja 3 se izvajajo predvsem prek Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter mreže nacionalnih koordinacijskih centrov v skladu z Uredbo (EU) 2021/887 Evropskega parlamenta in Sveta[20], razen ukrepov za izvajanje kibernetskovarnostne rezerve EU, ki jih izvajata Komisija in agencija ENISA.“;

[20] Uredba (EU) 2021/887 Evropskega parlamenta in Sveta z dne 20. maja 2021 o vzpostavitvi Evropskega industrijskega, tehnološkega in raziskovalnega kompetenčnega centra za kibernetsko varnost ter Mreže nacionalnih koordinacijskih centrov (UL L 202, 8.6.2021, str. 1).

(2) člen 9 se spremeni:

(a) v odstavku 2 se točke (b), (c) in (d) nadomestijo z naslednjim:

„(b) 1 776 956 000 EUR za specifični cilj 2 – umetna inteligenca;

(c) 1 629 566 000 EUR za specifični cilj 3 – kibernetska varnost in zaupanje;

(d) 482 347 000 EUR za specifični cilj 4 – napredne digitalne veščine;“;

(b) doda se naslednji odstavek 8:

„8. Z odstopanjem od člena 12(4) Uredbe (EU, Euratom) 2018/1046 se neporabljene odobritve za prevzem obveznosti in odobritve plačil za ukrepe, s katerimi se uresničujejo cilji iz člena 6(1), točka (g), te uredbe, samodejno prenesejo ter se lahko prevzamejo in izplačajo do 31. decembra naslednjega proračunskega leta.“;

(3) v členu 14 se odstavek 2 nadomesti z naslednjim:

„2. Program lahko zagotovi financiranje v kateri koli obliki, določeni v finančni uredbi, v osnovni obliki zlasti kot javna naročila, ali v obliki nepovratnih sredstev in nagrad.

Kadar je za doseganje cilja ukrepa potrebno javno naročanje inovativnega blaga in storitev, se lahko nepovratna sredstva dodelijo le upravičencem, ki so javni naročniki ali naročniki, kot so opredeljeni v direktivah 2014/24/EU[27] in 2014/25/EU[28] Evropskega parlamenta in Sveta.

Kadar je za doseganje ciljev ukrepa treba dobaviti inovativno blago ali opraviti digitalne storitve, ki še niso na voljo v večjem komercialnem obsegu, lahko javni naročnik ali naročnik odobri oddajo več naročil v okviru istega postopka javnega naročanja.

Javni naročnik ali naročnik lahko iz ustrezno utemeljenih razlogov javne varnosti zahteva, da mora biti kraj izvajanja pogodbe znotraj ozemlja Unije.

Komisija in agencija ENISA lahko pri izvajanju postopkov javnega naročanja za kibernetskovarnostno rezervo EU, vzpostavljeno s členom 12 Uredbe (EU) 2023/XX, delujeta kot osrednji nabavni organ za javno naročanje v imenu tretjih držav, pridruženih Programu v skladu s členom 10. Delujeta lahko tudi kot trgovec na debelo, tako da kupujeta, skladiščita in nadalje prodajata ali darujeta blago in storitve, vključno z najemi, navedenim tretjim državam. Z odstopanjem od člena 169(3) Uredbe (EU) XXX/XXXX [prenovitev] za pooblastilo Komisije ali agencije ENISA za ukrepanje zadostuje zahtevek ene same tretje države.

Komisija in agencija ENISA lahko pri izvajanju postopkov javnega naročanja za kibernetskovarnostno rezervo EU, vzpostavljeno s členom 12 Uredbe (EU) 2023/XX, delujeta kot osrednji nabavni organ za javno naročanje v imenu institucij, organov, uradov in agencij Unije. Delujeta lahko tudi kot trgovec na debelo, tako da kupujeta,

skladiščita in nadalje prodajata ali darujeta blago in storitve, vključno z najemi, institucijam, organom, uradom in agencijam Unije. Z odstopanjem od člena 169(3) Uredbe (EU) XXX/XXXX [prenovitev] za pooblastilo Komisije ali agencije ENISA za ukrepanje zadostuje zahtevek ene same institucije, organa, urada ali agencije Unije.

Program lahko zagotovi tudi financiranje v obliki finančnih instrumentov v okviru operacij mešanega financiranja.“;

(4) doda se naslednji člen 16a:

„V primeru ukrepov za izvajanje evropskega kibernetskega ščita, vzpostavljenega s členom 3 Uredbe (EU) 2023/XX, se uporabljajo pravila iz členov 4 in 5 Uredbe (EU) 2023/XX. V primeru neskladja med določbami te uredbe ter členoma 4 in 5 Uredbe (EU) 2023/XX imata prednost navedena člena, ki se uporabljata za te specifične ukrepe.“;

(5) člen 19 se nadomesti z naslednjim:

„Nepovratna sredstva v okviru Programa se dodeljujejo in upravljajo v skladu z naslovom VIII finančne uredbe ter lahko krijejo do 100 % upravičenih stroškov brez poseganja v načelo sofinanciranja, kot je določeno v členu 190 finančne uredbe. Taka nepovratna sredstva se dodeljujejo in upravljajo, kot je določeno za vsak specifičen cilj.

Podporo v obliki nepovratnih sredstev lahko center ECCC dodeli neposredno, brez razpisa za zbiranje predlogov, nacionalnim centrom za varnostne operacije iz člena 4 Uredbe XXXX in gostiteljskemu konzorciju iz člena 5 Uredbe XXXX v skladu s členom 195(1), točka (d), finančne uredbe.

Podporo v obliki nepovratnih sredstev za mehanizem za izredne kibernetske razmere iz člena 10 Uredbe XXXX lahko center ECCC dodeli neposredno, brez razpisa za zbiranje predlogov, državam članicam v skladu s členom 195(1), točka (d), finančne uredbe.

Kar zadeva ukrepe iz člena 10(1), točka (c), Uredbe 202X/XXXX, center ECCC Komisijo in agencijo ENISA obvesti o zahtevkih držav članic za neposredna nepovratna sredstva, ki se dodelijo brez razpisa za zbiranje predlogov.

Za podporo v obliki medsebojne pomoči pri odzivanju na pomemben kibernetskovarnostni incident ali tak incident velikih razsežnosti, kot je opredeljen v členu 10, točka (c), Uredbe XXXX, in v skladu s členom 193(2), drugi pododstavek, točka (a), finančne uredbe se lahko v ustrezno utemeljenih primerih stroški štejejo za upravičene, tudi če so nastali pred vložitvijo zahtevka za nepovratna sredstva.“;

(6) prilogi I in II se spremenita v skladu s Prilogo k tej uredbi.

Člen 20

Ocena

Komisija do [štiri leta po datumu začetka uporabe te uredbe] Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe.

Člen 21

Postopek v odboru

1. Komisiji pomaga odbor za usklajevanje programa Digitalna Evropa, ustanovljen z Uredbo (EU) 2021/694. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Člen 22

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 Strasbourgu,

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

1.2. Zadevna področja

1.3. Ukrep, na katerega se predlog/pobuda nanaša

1.4. Cilji

1.4.1. Splošni cilji

1.4.2. Specifični cilji

1.4.3. Pričakovani rezultati in posledice

1.4.4. Kazalniki smotrnosti

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

1.6. Trajanje predloga/pobude in finančnih posledic

1.7. Načrtovani način(i) izvrševanja proračuna

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Uredba Evropskega parlamenta in Sveta o določitvi ukrepov za okrepitev solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje

1.2. Zadevna področja

Evropa, pripravljena na digitalno dobo Evropske strateške naložbe Dejavnost: oblikovanje digitalne prihodnosti Evrope.

1.3. Ukrep, na katerega se predlog/pobuda nanaša

☒ **Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[33]

☐ **Podaljšanje obstoječega ukrepa**

☐ **Združitev ali preusmeritev enega ali več ukrepov v drug/nov ukrep**

1.4. Cilji

1.4.1. Splošni cilji

Z aktom o kibernetski solidarnosti bo okrepljena solidarnost na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje. Njegovi cilji so: (a) okrepiti skupno odkrivanje kibernetskovarnostnih groženj in incidentov v EU ter situacijsko zavedanje o njih; (b) okrepiti pripravljenost kritičnih subjektov po vsej EU in solidarnost z razvijanjem skupnih zmogljivosti za odzivanje na pomembne kibernetskovarnostne incidente ali take incidente velikih razsežnosti, med drugim z omogočanjem podpore pri odzivanju na incidente tretjim državam, pridruženim programu Digitalna Evropa; (c) povečati odpornost Unije in prispevati k učinkovitemu odzivu s pregledovanjem in ocenjevanjem pomembnih incidentov ali incidentov velikih razsežnosti, med drugim na podlagi pridobljenih spoznanj in po potrebi priporočil.

1.4.2. Specifični cilji

Akt o kibernetski solidarnosti bo sklop ciljev dosegel z:

(a) vzpostavitvijo vseevropske infrastrukture centrov za varnostne operacije (evropskega kibernetskega ščita) za vzpostavitev in okrepitev skupnih zmogljivosti za odkrivanje in situacijsko zavedanje;

[33] Po členu 58(2)(a) oz. (b) finančne uredbe.

(b) vzpostavitvijo mehanizma za izredne kibernetske razmere za podporo državam članicam pri pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti, odzivanju nanje in takojšnjem okrevanju po njih. Podpora za odzivanje na incidente se omogoči tudi evropskim institucijam, organom, uradom in agencijam Unije.

Ti ukrepi bodo podprti s sredstvi iz programa Digitalna Evropa, ki bo s tem zakonodajnim instrumentom spremenjen, da se določijo zgoraj navedeni ukrepi, zagotovi finančna podpora za njihov razvoj in pojasnijo pogoji za upravičenost do finančne podpore;

(c) vzpostavitvijo evropskega mehanizma za pregledovanje kibernetskovarnostnih incidentov za pregled in oceno pomembnih incidentov ali incidentov velikih razsežnosti.

1.4.3. Pričakovani rezultati in posledice

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

Predlog bi prinesel znatne koristi za različne deležnike. Evropski kibernetski ščit bo izboljšal zmogljivosti držav članic za odkrivanje kibernetskih groženj. Mehanizem za izredne kibernetske razmere bo dopolnjeval ukrepe držav članic z nujno pomočjo za pripravljenost, odzivanje in takojšnje okrevanje/ponovno vzpostavitev delovanja bistvenih storitev.

Ti ukrepi bodo okrepili konkurenčni položaj industrije in podjetij v Evropi v celotnem spletnem gospodarstvu ter podprli njihovo digitalno preobrazbo, in sicer z okrepitvijo ravni kibernetske varnosti na enotnem digitalnem trgu. Cilj predloga je zlasti povečati odpornost državljanov, podjetij in subjektov, ki delujejo v kritičnih ali visoko kritičnih sektorjih, proti vse večjim kibernetskovarnostnim grožnjam, ki imajo lahko uničujoče družbene in gospodarske posledice. To se bo doseglo z vlaganjem v orodja, ki bodo podpirala hitrejše odkrivanje kibernetskovarnostnih groženj in incidentov ter odzivanje nanje, državam članicam pa bodo pomagala pri boljši pripravi na pomembne kibernetskovarnostne incidente in take incidente velikih razsežnosti ter pri odzivanju nanje. S tem bi se morala podpreti tudi krepitev zmogljivosti Evrope na teh področjih, zlasti kar zadeva zbiranje in analizo podatkov o kibernetskovarnostnih grožnjah in incidentih.

1.4.4. Kazalniki smotrnosti

Navedite, s katerimi kazalniki se bodo spremljali napredek in dosežki.

Za spodbujanje solidarnosti na ravni Unije bi bilo mogoče upoštevati več kazalnikov:

(1) število skupno naročenih infrastruktur ali orodij za kibernetsko varnost ali obojega;

(2) število ukrepov za podporo pripravljenosti in odzivanju na kibernetskovarnostne incidente v okviru mehanizma za izredne kibernetske razmere.

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Uredba bi se morala v celoti začeti uporabljati kmalu po sprejetju, tj. dvajseti dan po objavi v *Uradnem listu Evropske unije*.

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Zaradi močne čezmejne narave kibernetskovarnostnih groženj na splošno ter vse večjega števila tveganj in incidentov, ki imajo učinke prelivanja prek meja, sektorjev in proizvodov, države članice ciljev tega ukrepanja ne morejo učinkovito doseči same, zato sta potrebna skupno ukrepanje in solidarnost na ravni Unije. Izkušnje z bojem proti kibernetskim grožnjam, ki izhajajo iz vojne proti Ukrajini, skupaj s spoznanji, pridobljenimi med vajo na področju kibernetske varnosti, ki se je izvajala med francoskim predsedovanjem (EU CyCLES), so pokazale, da bi bilo treba za dosego solidarnosti na ravni EU razviti konkretne mehanizme vzajemne podpore, zlasti sodelovanje z zasebnim sektorjem. Glede na navedeno Svet v sklepih z dne 23. maja 2022 o oblikovanju kibernetske drže Evropske unije Komisijo poziva, naj predstavi predlog o novem skladu za odzivanje na izredne kibernetskovarnostne razmere. Podpora in ukrepi na ravni Unije za boljše odkrivanje kibernetskovarnostnih groženj ter povečanje zmogljivosti za pripravljenost in odzivanje zagotavljajo dodano vrednost, saj preprečujejo podvajanje prizadevanj v Uniji in državah članicah. To bi omogočilo boljšo uporabo obstoječih sredstev ter večje usklajevanje in izmenjavo informacij o pridobljenih spoznanjih.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

V okviru delovnega programa programa Digitalna Evropa za kibernetsko varnost za obdobje 2021–2022 sta bila v zvezi s situacijskim zavedanjem in odkrivanjem v okviru evropskega kibernetskega ščita organizirana razpis za prijavo interesa za skupno javno naročanje orodij in infrastrukture za ustanovitev čezmejnih centrov za varnostne operacije ter razpis za nepovratna sredstva za krepitev zmogljivosti centrov za varnostne operacije, ki delujejo v javnih in zasebnih organizacijah.

Kar zadeva pripravljenost in odzivanje na incidente, je Komisija vzpostavila kratkoročni program za podporo državam članicam z dodatnimi sredstvi, dodeljenimi agenciji ENISA, da bi se nemudoma okrepile pripravljenost in zmogljivosti za odzivanje na večji kibernetski incident. Zajete storitve vključujejo ukrepe pripravljenosti, kot je penetracijsko testiranje kritičnih subjektov za ugotavljanje ranljivosti. S programom so okrepljene tudi možnosti za pomoč državam članicam v primeru večjega incidenta, ki prizadene kritične subjekte. Ta kratkoročni program izvaja agencija ENISA, zagotovil pa je že dragocena spoznanja, ki so bila upoštevana pri pripravi te uredbe.

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

Akt o kibernetski solidarnosti bo temeljil na ukrepih, ki jih trenutno podpirajo Unija in države članice, za izboljšanje situacijskega zavedanja in odkrivanja kibernetskih groženj ter za odzivanje na incidente velikih razsežnosti in čezmejne kibernetskovarnostne incidente. Poleg tega je instrument skladen z drugimi okviri kriznega upravljanja, med drugim z ureditvijo IPCR, skupno varnostno in obrambno politiko, vključno z enotami za hitro odzivanje na kibernetske grožnje, in pomočjo, ki jo ena država članica zagotovi drugi državi članici v okviru člena 42(7) Pogodbe o Evropski uniji. Novi predlog bi dopolnjeval in podpiral tudi strukture, razvite v

okviru drugih instrumentov za kibernetsko varnost, kot sta Direktiva (EU) 2022/2555 (direktiva NIS 2) ali Uredba 2019/881 (Akt o kibernetski varnosti).

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

Upravljanje področij ukrepanja, dodeljenih agenciji ENISA, ustreza njenemu sedanjemu mandatu in splošnim nalogam. Za ta področja ukrepanja so lahko potrebni posebni profili ali nove naloge, vendar je te mogoče izvesti tudi z obstoječimi viri agencije ENISA ter s premestitvami ali povezovanjem različnih nalog. Agencija ENISA trenutno izvaja kratkoročni program, ki ga je Komisija vzpostavila leta 2022, da bi se nemudoma okrepile pripravljenost in zmogljivosti za odzivanje na večji kibernetski incident. Zajete storitve vključujejo možnosti za pomoč državam članicam v primeru večjega incidenta, ki prizadene kritične subjekte. Ta kratkoročni program izvaja agencija ENISA, zagotovil pa je že dragocena spoznanja, ki so bila upoštevana pri pripravi te uredbe. Vire, dodeljene kratkoročnemu programu, bi bilo mogoče uporabiti tudi v okviru te uredbe.

1.6. Trajanje predloga/pobude in finančnih posledic

☒ **Časovno omejeno**

– ☒ Z učinkom od datuma sprejetja predloga uredbe Evropskega parlamenta in Sveta o okrepitvi solidarnosti in zmogljivosti v Uniji za odkrivanje kibernetskovarnostnih groženj in incidentov ter pripravo in odzivanje nanje (v nadaljnjem besedilu: akt o kibernetski solidarnosti).

– ☒ Finančne posledice od leta 2023 do leta 2027 za odobritve za prevzem obveznosti ter od leta 2023 do leta 2031 za odobritve plačil[34].

☐ **Časovno neomejeno**

– izvajanje z obdobjem uvajanja med letoma LLLL in LLLL,

– ki mu sledi izvajanje v celoti.

1.7. Načrtovani način(i) izvrševanja proračuna[35]

☒ **Neposredno upravljanje** – Komisija:

– ☒ z lastnimi službami, vključno s svojim osebjem v delegacijah Unije,

– ☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☒ **Posredno upravljanje**, tako da se naloge izvrševanja proračuna poverijo:

– ☐ 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 imajo ti subjekti ustrezna finančna jamstva,

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

– ☐ organom ali osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

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

Opombe

Ukrepe v zvezi z evropskim kibernetskim ščitom bo izvajal center ECCC. Dokler je center ECCC zmožen izvrševati lastni proračun, bo Evropska komisija ukrepe izvajala z neposrednim upravljanjem v imenu tega centra. Center ECCC lahko na podlagi razpisov za prijavo interesa izbere subjekte, ki bodo sodelovali pri skupnem javnem naročanju orodij. Za uporabo teh orodij lahko dodeli nepovratna sredstva.

---

34 Ukrepi iz akta bi morali biti podprti z naslednjim večletnim finančnim okvirom.

35 Pojasnila o načinih izvrševanja proračuna in sklici na finančno uredbo so na voljo na spletišču BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx.

Poleg tega lahko center ECCC nepovratna sredstva za ukrepe pripravljenosti dodeli v okviru mehanizma za izredne kibernetske razmere.

Za izvajanje kibernetskovarnostne rezerve EU je v celoti odgovorna Komisija. Komisija lahko delovanje in upravljanje kibernetskovarnostne rezerve EU s sporazumi o prispevku v celoti ali delno zaupa agenciji ENISA. Ukrepi iz te uredbe, dodeljeni agenciji ENISA, so v skladu z njenim sedanjim mandatom. Ti ukrepi vključujejo: (i) podporo skupini za sodelovanje na področju varnosti omrežnih in informacijskih sistemov pri razvijanju ukrepov pripravljenosti v skladu z ocenami tveganja; (ii) podporo Komisiji pri vzpostavitvi in nadzoru izvajanja kibernetskovarnostne rezerve EU, med drugim s prejemanjem in obdelavo zahtevkov za podporo; (iii) oblikovanje predlog za lažjo predložitev zahtevkov za podporo in posebnih sporazumov, ki jih skleneta ponudnik storitev in uporabnik, ki mu je zagotovljena podpora v okviru kibernetskovarnostne rezerve EU; (iv) pregledovanje in ocenjevanje groženj, ranljivosti in blažitvenih ukrepov v zvezi s posameznimi pomembnimi kibernetskovarnostnimi incidenti ali takimi incidenti velikih razsežnosti ter pripravo poročil o njih.

Vse te naloge so ocenjene na približno sedem EPDČ iz obstoječih virov agencije ENISA, pri čemer te že temeljijo na strokovnem znanju in pripravljalnem delu, ki ga agencija ENISA trenutno opravlja v okviru pilotnega projekta nujne pomoči za pripravljenost in odzivanje na incidente.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Komisija bo spremljala izvajanje in uporabo teh novih določb ter skladnost z njimi, da bi ocenila njihovo učinkovitost. Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe najpozneje štiri leta po datumu začetka njene uporabe.

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

Uredba uvaja okvir za izvajanje financiranja EU z namenom povečanja kibernetske odpornosti z ukrepi za izboljšanje zmogljivosti za odkrivanje, odzivanje in okrevanje v primeru pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti. Izvajanje Direktive bodo upravljale enote v okviru GD za komunikacijska omrežja, vsebine in tehnologijo, ki so pristojne za zadevno področje politike.

Za izpolnjevanje novih nalog je treba službam Komisije zagotoviti ustrezne vire. Ocenjuje se, da bo za izvrševanje nove uredbe potrebnih šest EPDČ (trije uradniki in trije pogodbeni uslužbenci), in sicer za izvajanje naslednjih nalog:

- določanje ukrepov pripravljenosti v skladu z ocenami tveganja;
- zagotavljanje interoperabilnosti med platformami čezmejnih centrov za varnostne operacije;
- priprava morebitnih izvedbenih aktov (dveh za centre za varnostne operacije in dveh za mehanizem za izredne kibernetske razmere);
- upravljanje sporazumov o gostiteljstvu in uporabi za centre za varnostne operacije;
- vzpostavitev in upravljanje kibernetskovarnostne rezerve EU, neposredno ali s sporazumom o prispevku za agencijo ENISA. V primeru sporazuma o prispevku za agencijo ENISA naloge vključujejo tudi pripravo in nadzor izvajanja sporazuma o prispevku za naloge, dodeljene agenciji ENISA;
- sodelovanje v posvetovalnih skupinah, ki jih agencija ENISA skliče za pregled in oceno pomembnih kibernetskovarnostnih incidentov in takih incidentov velikih razsežnosti, ter priprava poročil.

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

Tveganje, ugotovljeno za evropski kibernetski ščit, je, da si države članice na platformah čezmejnih centrov za varnostne operacije ali med čezmejnimi platformami in drugimi ustreznimi subjekti na ravni EU ne izmenjujejo zadostne količine ustreznih informacij o kibernetskih grožnjah. Za ublažitev teh tveganj bodo sredstva dodeljena po razpisu za prijavo interesa, v katerem se države članice zavežejo, da bodo določeno količino informacij delile s subjekti na ravni EU. Ta zaveza bo nato formalizirana s sporazumom o gostiteljstvu in uporabi, s katerim bo

center ECCC pooblaščen za izvajanje revizij za zagotovitev, da se skupno naročena orodja in infrastruktura uporabljajo v skladu s sporazumom. Zaveze k visoki ravni izmenjave informacij znotraj čezmejnih centrov za varnostne operacije bodo formalizirane v konzorcijski pogodbi.

Tveganje, ugotovljeno za mehanizem za izredne kibernetske razmere, je, da uporabniki, ki sodelujejo v mehanizmu, ne sprejmejo zadostnih ukrepov za zagotovitev pripravljenosti na kibernetske napade. Zato morajo uporabniki sprejeti take ukrepe pripravljenosti, da bi lahko prejeli podporo iz kibernetskovarnostne rezerve EU. Ob predložitvi zahtevkov za podporo iz kibernetskovarnostne rezerve EU morajo uporabniki pojasniti, kateri ukrepi za odziv na incident so bili že sprejeti, saj se bo to upoštevalo pri oceni zahtevkov, predloženih kibernetskovarnostni rezervi EU.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

Ker so pravila sodelovanja v programu Digitalna Evropa, ki se uporablja za podporo v okviru akta o kibernetski solidarnosti, podobna pravilom, ki jih bo Komisija uporabila v svojih delovnih programih, in ker imajo upravičenci podoben profil tveganja kot upravičenci pri programih v okviru neposrednega upravljanja, je mogoče pričakovati, da bo stopnja napake podobna stopnji napake, ki jo je Komisija predvidela za program Digitalna Evropa, tj. razumno je treba zagotoviti, da tveganje napake v večletnem odhodkovnem obdobju na letni ravni ostaja med 2 % in 5 %, pri čemer je končni cilj, da se preostala stopnja napake ob zaključku večletnih programov, ko so upoštevane finančne posledice vseh revizij, popravkov in sanacijskih ukrepov, čim bolj približa 2 %.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

V primeru evropskega kibernetskega ščita bo imel center ECCC pooblastilo, da na podlagi dostopa do informacij in pregledov na kraju samem revidira skupno naročena orodja in infrastrukture v skladu s sporazumom o gostiteljstvu in uporabi, ki ga podpišeta gostiteljski konzorcij in center ECCC.

Obstoječi ukrepi za preprečevanje goljufij, ki se uporabljajo za institucije, organe, urade in agencije Unije, bodo zajemali dodatne odobritve, potrebne za to uredbo.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
	številka	dif./nedif.[36]	držav Efte[37]	držav kandidatk in potencialnih kandidatk[38]	drugih tretjih držav	drugi namenski prejemki
1	02 04 01 10 – program Digitalna Evropa – kibernetska varnost	dif.	DA	DA	NE	NE
1	02 04 01 11 – program Digitalna Evropa – Evropski industrijski, tehnološki in raziskovalni kompetenčni center za kibernetsko varnost	dif.	DA	DA	NE	NE
1	02 04 03 – program Digitalna Evropa – umetna inteligenca	dif.	DA	DA	NE	NE
1	02 04 04 – program Digitalna Evropa – znanja in spretnosti	dif.	DA	DA	NE	NE
1	02 01 30 – odhodki za podporo programu Digitalna Evropa	nedif.	DA	DA	NE	NE

[36] Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.
[37] Efta: Evropsko združenje za prosto trgovino.
[38] Države kandidatke in po potrebi potencialne države kandidatke.

3.2. Ocenjene finančne posledice predloga za odobritve

3.2.1. Povzetek ocenjenih posledic za odobritve za poslovanje

– ☐ Za predlog/pobudo niso potrebne odobritve za poslovanje.

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

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	Številka	1 **Enotni trg, inovacije in digitalni sektor**

S predlogom se skupna raven obveznosti v okviru programa Digitalna Evropa ne bo povišala. Prispevek k tej pobudi je namreč prerazporeditev obveznosti, ki izhajajo iz SC2 in SC4, za okrepitev proračuna SC3 in centra ECCC. Za namene te pobude bi bilo mogoče uporabiti vsako povečanje obveznosti v okviru programa Digitalna Evropa, ki izhaja iz revizije večletnega finančnega okvira.

GD CONNECT			Leto **2025**	Leto **2026**	Leto **2027**	Leto **2028+**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			**SKUPAJ**
○ Odobritve za poslovanje										
Proračunska vrstica[39] 02 04 01 10 (prerazporeditev iz vrstic 02 04 03 in 02 04 04)	obveznosti	(1a)	15,000	15,000	6,000	p. m.				**36,000**
	plačila	(2a)	15,000	15,000	6,000					**36,000**
Proračunska vrstica 02 04 01 11 02 (prerazporeditev iz 02 04 03 in 02 04 04)	obveznosti	(1b)	13,000	23,000	28,000	p. m.				**64,000**
	plačila	(2b)	8,450	18,200	25,250	12,100				**64,000**
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov[40]										
Proračunska vrstica 02 01 30		(3)	0,150	0,150	0,150	p. m.				0,450

[39] Po uradni proračunski nomenklaturi.

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

Odobritve iz RAZDELKA 7 za GD CONNECT	obveznosti	= 1a + 1b + 3	**28,150**	**38,150**	**34,150**	**p. m.**				**100,450**
	plačila	= 2a + 2b + 3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ Odobritve za poslovanje SKUPAJ	obveznosti	(4)	28,000	38,000	34,000	p. m.				**100,000**
	plačila	(5)	23,450	33,200	31,250	12,100				**100,000**
○ Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ		(6)	0,150	0,150	0,150	p. m.				**0,450**
Odobritve iz RAZDELKA 1 večletnega finančnega okvira **SKUPAJ**	obveznosti	= 4 + 6	**28,150**	**38,150**	**34,150**	**p. m.**				**100,450**
	plačila	= 5 + 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

<u>Če ima predlog/pobuda posledice za več razdelkov za poslovanje, ponovite zgornji odsek:</u>

○ Odobritve za poslovanje SKUPAJ (vsi razdelki za poslovanje)	obveznosti	(4)	28,000	38,000	34,000	p. m.				**100,000**
	plačila	(5)	23,450	33,200	31,250	12,100				**100,000**
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ (vsi razdelki za poslovanje)		(6)	0,150	0,150	0,150					**0,450**
Odobritve iz RAZDELKOV od 1 do 6 večletnega finančnega okvira **SKUPAJ** (referenčni znesek)	obveznosti	= 4 + 6	**28,150**	**38,150**	**34,150**	**p. m.**				**100,450**
	plačila	= 5 + 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Razdelek večletnega finančnega okvira	**7**	„Upravni odhodki“

Ta oddelek se izpolni s „proračunskimi podatki upravne narave“, ki jih je treba najprej vnesti v Prilogo k oceni finančnih posledic zakonodajnega predloga (Priloga 5 k Sklepu Komisije o notranjih pravilih za izvrševanje oddelka splošnega proračuna Evropske unije za Komisijo), ki se prenese v sistem DECIDE za namene posvetovanj med službami.

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2025**	Leto **2026**	Leto **2027**	Leto **2028+**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			**SKUPAJ**
GD CONNECT									
○ Človeški viri		0,786	0,786	0,786	p. m.				**2,358**
○ Drugi upravni odhodki		0,035	0,035	0,035	p. m.				**0,105**
GD CONNECT SKUPAJ	odobritve	**0,821**	**0,821**	**0,821**					**2,463**

Odobritve iz RAZDELKA 7 večletnega finančnega okvira **SKUPAJ**	(obveznosti skupaj = plačila skupaj)	**0,821**	**0,821**	**0,821**					**2,463**

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2025**	Leto **2026**	Leto **2027**	Leto **2028+**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			**SKUPAJ**
Odobritve iz RAZDELKOV od 1 do 7 večletnega finančnega okvira **SKUPAJ**	obveznosti	**28,971**	**38,971**	**34,971**	**p. m.**				**102,913**
	plačila	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Ocenjene realizacije, financirane z odobritvami za poslovanje

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

Cilji in realizacije			Leto **N**		Leto **N+1**		Leto **N+2**		Leto **N+3**		Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)						**SKUPAJ**	
	REALIZACIJE																	
⇩	vrsta[41]	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[42] …																		
– realizacija																		
– realizacija																		
– realizacija																		
Seštevek za specifični cilj št. 1																		
SPECIFIČNI CILJ št. 2 …																		
– realizacija																		
Seštevek za specifični cilj št. 2																		
SKUPAJ																		

[41] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[42] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

3.2.3. Povzetek ocenjenih posledic za upravne odobritve

– ☐ 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 2025	Leto 2026	Leto 2027	Leto N+3	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			**SKUPAJ**
RAZDELEK 7 večletnega finančnega okvira								
Človeški viri	0,786	0,786	0,786					**2,358**
Drugi upravni odhodki	0,035	0,035	0,035					**0,105**
Seštevek za RAZDELEK 7 večletnega finančnega okvira	**0,821**	**0,821**	**0,821**					**2,463**

Odobritve zunaj RAZDELKA 7[43] večletnega finančnega okvira								
Človeški viri								
Drugi upravni odhodki	0,150	0,150	0,150					**0,450**
Seštevek za odobritve zunaj RAZDELKA 7 večletnega finančnega okvira	**0,150**	**0,150**	**0,150**					**0,450**

SKUPAJ	**0,971**	**0,971**	**0,971**					**2,913**

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 postopku letne dodelitve virov glede na proračunske omejitve.

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

3.2.3.1. Ocenjene potrebe po človeških virih

– ☐ 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 **2025**	Leto **2026**	Leto 20 27	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)		
O Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)							
20 01 02 01 (sedež in predstavništva Komisije)	3	3	3				
20 01 02 03 (delegacije)							
01 01 01 01 (posredne raziskave)							
01 01 01 11 (neposredne raziskave)							
Druge proračunske vrstice (navedite)							
O Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)[44]							
20 02 01 (PU, NNS, ZU iz splošnih sredstev)	3	3	3				
20 02 03 (PU, LU, NNS, ZU in MSD na delegacijah)							
XX 01 xx **yy zz** [45] – na sedežu							
XX 01 xx **yy zz** [45] – na delegacijah							
01 01 01 02 (PU, NNS, ZU za posredne raziskave)							
01 01 01 12 (PU, NNS, ZU za neposredne raziskave)							
Druge proračunske vrstice (navedite)							
SKUPAJ	**6**	**6**	**6**				

XX je zadevno področje ali naslov v proračunu.

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 postopku letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci	- določanje ukrepov pripravljenosti v skladu z ocenami tveganja (člen 11) - priprava morebitnih izvedbenih aktov (dveh za centre za varnostne operacije in dveh za mehanizem za izredne kibernetske razmere) - upravljanje sporazumov o gostiteljstvu in uporabi za centre za varnostne operacije - vzpostavitev in upravljanje kibernetskovarnostne rezerve EU, neposredno ali s sporazumom o prispevku za agencijo ENISA
Zunanji sodelavci	Pod nadzorom uradnika: - določanje ukrepov pripravljenosti v skladu z ocenami tveganja (člen 11) - priprava morebitnih izvedbenih aktov (dveh za centre za varnostne operacije in dveh za mehanizem za izredne kibernetske razmere) - upravljanje sporazumov o gostiteljstvu in uporabi za centre za varnostne operacije - vzpostavitev in upravljanje kibernetskovarnostne rezerve EU, neposredno ali s sporazumom o prispevku za agencijo ENISA

[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).

3.2.4. *Skladnost z veljavnim večletnim finančnim okvirom*

Predlog/pobuda:

– [X] se lahko v celoti financira s prerazporeditvijo znotraj zadevnega razdelka večletnega finančnega okvira.

Pojasnite zahtevano spremembo ter navedite zadevne proračunske vrstice in ustrezne zneske. V primeru pomembnejših sprememb med programi predložite Excelovo tabelo.

	23	24	25	26	27	skupaj
SC1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
Prvotni znesek za SC2	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1185 449 819
Za kibernetsko pobudo			18 000 000	28 000 000	19 000 000	65 000 000
NOVI ZA SC2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1120 449 819**
Predlog proračuna 24 za SC3	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
Iz SC2–SC4			15 000 000	15 000 000	6 000 000	36 000 000
Novi za SC3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
Prvotni znesek za ECCC	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
Iz SC2–SC4			13 000 000	23 000 000	28 000 000	64 000 000
Novi za ECCC	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
Prvotni znesek za SC4	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Za kibernetsko pobudo			10 000 000	10 000 000	15 000 000	35 000 000
NOVI za SC4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] zahteva uporabo nedodeljene razlike do zgornje meje v zadevnem razdelku večletnega finančnega okvira in/ali uporabo posebnih instrumentov, kot so opredeljeni v uredbi o večletnem finančnem okviru;

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice, ustrezne zneske in instrumente, ki naj bi bili uporabljeni.

– [ ] zahteva spremembo večletnega finančnega okvira.

Pojasnite te zahteve ter navedite zadevne razdelke in proračunske vrstice ter ustrezne zneske.

3.2.5. *Udeležba tretjih oseb pri financiranju*

V predlogu/pobudi:

– [X] ni načrtovano sofinanciranje tretjih oseb;

– [ ] je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

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

	Leto **N**[46]	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)	Skupaj

[46] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Naredite isto za naslednja leta.

Navedite organ, ki bo sofinanciral predlog/pobudo								
Sofinancirane odobritve SKUPAJ								

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	Odobritve na voljo za tekoče proračunsko leto	Posledice predloga/pobude[47]						
		Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)		
Člen …….								

Za namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

[…]

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

[…]

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