Vijeće
Europske unije

Bruxelles, 20. travnja 2023.
(OR. en)

8512/23

Međuinstitucijski predmet:
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

PRIJEDLOG

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	19. travnja 2023.
Za:	Thérèse BLANCHET, glavna tajnica Vijeća Europske unije
Br. dok. Kom.:	COM(2023) 209 final
Predmet:	Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih

Za delegacije se u prilogu nalazi dokument COM(2023) 209 final.

Priloženo: COM(2023) 209 final

EUROPSKA
KOMISIJA

Strasbourg, 18.4.2023.
COM(2023) 209 final

2023/0109 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

• Razlozi i ciljevi prijedloga

Ovo obrazloženje priloženo je Prijedlogu akta o kibersolidarnosti. Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora gospodarstva jer su javne uprave, poduzeća i građani međusobno povezani i ovisni jedni o drugima u svim sektorima i prekogranično više nego ikada prije. S većom primjenom digitalnih tehnologija povećava se i izloženost incidentima u području kibersigurnosti i njihovim mogućim posljedicama. Istodobno se države članice suočavaju sa sve većim kibersigurnosnim rizicima i općenito složenim prijetnjama, uz očit rizik od brzog prelijevanja kiberincidenata iz jedne države članice na druge.

Osim toga, kiberoperacije sve se više integriraju u hibridne strategije i strategije ratovanja, sa znatnim posljedicama za metu. Konkretno, ruskoj vojnoj agresiji na Ukrajinu prethodila je i prati je strategija neprijateljskih kiberoperacija, što je prekretnica u percepciji i procjeni zajedničke pripravnosti EU-a za upravljanje kibersigurnosnim krizama te razlog za hitno djelovanje. Prijetnja mogućeg incidenta velikih razmjera koji bi uzrokovao znatne poremećaje i štetu na kritičnoj infrastrukturi zahtijeva povećanu pripravnost na svim razinama kibersigurnosnog ekosustava EU-a. Ta prijetnja nadilazi rusku vojnu agresiju na Ukrajinu i uključuje stalne kiberprijetnje državnih i nedržavnih aktera, koje će se vjerojatno nastaviti s obzirom na mnoštvo državi bliskih, kriminalnih i haktivističkih aktera umiješanih u trenutačne geopolitičke napetosti. Posljednjih se godina broj kibernapada drastično povećao, uključujući napade na lance opskrbe s ciljem kiberšpijunaže, napade ucjenjivačkim softverom ili izazivanje poremećaja. Napad na lanac opskrbe poduzeća SolarWinds 2020. pogodio je više od 18 000 organizacija u svijetu, uključujući vladine agencije i velika poduzeća. Značajni kibersigurnosni incidenti mogu izazvati prevelike poremećaje da bi se jedna ili više pogođenih država članica s njima mogle samostalno nositi. Zbog toga je potrebna pojačana solidarnost na razini Unije kako bi se bolje otkrile kibersigurnosne prijetnje i incidenti te kako bi se za njih bolje pripremilo i na njih odgovorilo.

Kad je riječ o otkrivanju kiberprijetnji i kiberincidenata, hitno je potrebno poboljšati razmjenu informacija i naše zajedničke kapacitete kako bi se drastično smanjilo vrijeme potrebno za otkrivanje kiberprijetnji prije nego što prouzroče veliku štetu i troškove[1]. Iako mnoge kibersigurnosne prijetnje i incidenti imaju potencijalnu prekograničnu dimenziju zbog međusobne povezanosti digitalnih infrastruktura, razmjena relevantnih informacija među državama članicama i dalje je ograničena. Taj se problem nastoji riješiti uspostavom mreže prekograničnih centara za sigurnosne operacije (SOC-ova) radi poboljšanja sposobnosti otkrivanja i odgovora.

[1] Prema izvješću organizacija Ponemon Institute i IBM Security, prosječno vrijeme potrebno za utvrđivanje povrede u 2022. bilo je 207 dana, uz dodatnih 70 dana za ograničavanje posljedica. Istodobno je 2022. prosječni trošak povreda privatnosti podataka sa životnim vijekom duljim od 200 dana iznosio 4,86 milijuna EUR, u usporedbi s 3,74 milijuna EUR za životni vijek kraći od 200 dana. („Cost of a data breach 2022”, https://www.ibm.com/reports/data-breach).

Kad je riječ o pripravnosti i odgovoru na kibersigurnosne incidente, potpora na razini Unije i solidarnost među državama članicama trenutno su ograničene. U Zaključcima Vijeća iz listopada 2021. istaknuta je potreba za uklanjanjem tih nedostataka i Komisija je pozvana da predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti[2].

Ovom se Uredbom provodi i Strategija EU-a za kibersigurnost donesena u prosincu 2020.[3] u kojoj je najavljena uspostava europskog kiberštita, kojim bi se ojačali kapaciteti za otkrivanje kiberprijetnji i razmjenu informacija u Europskoj uniji putem udruženja nacionalnih i prekograničnih SOC-ova.

Ova se Uredba temelji na prvim mjerama koje su već osmišljene u bliskoj suradnji s glavnim dionicima i koje se podupiru u okviru programa Digitalna Europa. Konkretno, kad je riječ o SOC-ovima, u okviru programa rada za kibersigurnost programa Digitalna Europa za razdoblje 2021.–2022. objavljen je poziv na iskaz interesa za zajedničku nabavu alata i infrastrukture za uspostavu prekograničnih SOC-ova i poziv za dodjelu bespovratnih sredstava za izgradnju kapaciteta SOC-ova koji služe javnim i privatnim organizacijama. Kad je riječ o pripravnosti i odgovoru na incidente, Komisija je uspostavila kratkoročni program za potporu državama članicama dodjelom dodatnih sredstava Agenciji Europske unije za kibersigurnost (ENISA) kako bi se hitno ojačali pripravnost i kapaciteti za odgovor na velike kiberincidente. Obje su mjere pripremljene u bliskoj suradnji s državama članicama. Ovom se Uredbom uklanjaju nedostaci tih mjera i uzimaju u obzir saznanja o njima.

Naposljetku, ovim se Prijedlogom ispunjava obveza iz Zajedničke komunikacije o kiberobrani[4] donesene 10. studenoga da se pripremi prijedlog inicijative EU-a za kibersolidarnost sa sljedećim ciljevima: jačanje zajedničkih sposobnosti EU-a za otkrivanje, informiranost o stanju i odgovor radi postupne izgradnje kibersigurnosne pričuve na razini EU-a s uslugama pouzdanih privatnih pružatelja usluga i radi potpore testiranju ključnih subjekata.

U tom kontekstu Komisija predlaže Akt o kibersolidarnosti kako bi se povećala solidarnost na razini Unije radi boljeg otkrivanja, pripreme i odgovora na kibersigurnosne prijetnje i incidenate postizanjem sljedećih posebnih ciljeva:

- unapređenja zajedničkog otkrivanja kiberprijetnji i kiberincidenata u EU-u i informiranosti o stanju u pogledu kiberprijetnji i kiberincidenata, čime bi se doprinijelo europskom tehnološkom suverenitetu u području kibersigurnosti,
- jačanja pripravnosti kritičnih subjekata u cijelom EU-u i jačanja solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore za

[2] Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje je Vijeće odobrilo na sastanku 23. svibnja 2022. (9364/22).

[3] Zajednička komunikacija Europskom parlamentu i Vijeću „Strategija EU-a za kibersigurnost za digitalno desetljeće”, JOIN(2020) 18 final.

[4] Zajednička komunikacija Europskom parlamentu i Vijeću „Politika kiberobrane EU-a”, JOIN(2022) 49 final.

odgovor na incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa,

- povećanja otpornosti Unije i djelotvornosti odgovora istraživanjem i procjenjivanjem značajnih incidenata ili incidenata velikih razmjera, među ostalim učenjem iz iskustva i, prema potrebi, davanjem preporuka.

Ti se ciljevi provode sljedećim mjerama:

- uvođenjem paneuropske infrastrukture SOC-ova (europski kiberštit) radi razvoja i poboljšanja zajedničkih sposobnosti za otkrivanje i informiranost o stanju,
- uspostavom mehanizma za izvanredne kibersigurnosne situacije kako bi se državama članicama pomoglo u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih. Potpora za odgovor na incidente stavlja se na raspolaganje i institucijama, tijelima, uredima i agencijama Unije.
- Uspostavom europskog mehanizma za istraživanje kibersigurnosnih incidenata radi istraživanja i procjene konkretnih značajnih incidenata ili incidenata velikih razmjera.

Europski kiberštit i mehanizam za izvanredne kibersigurnosne situacije poduprijet će se financiranjem iz programa Digitalna Europa, koji će se ovim zakonodavnim instrumentom izmijeniti kako bi se uspostavile prethodno navedene mjere, osigurala financijska potpora za njihov razvoj i pojasnili uvjeti za dobivanje financijske potpore.

- **Dosljednost s postojećim odredbama politike u tom području**

Okvir EU-a obuhvaća nekoliko zakonodavnih akata koji su već na snazi ili predloženi na razini Unije za smanjenje ranjivosti, povećanje otpornosti kritičnih subjekata na kibersigurnosne rizike i potporu koordiniranom upravljanju kibersigurnosnim incidentima i kibersigurnosnim krizama velikih razmjera, posebno Direktivu o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (NIS 2)[5], Akt o kibersigurnosti[6], Direktivu o napadima na informacijske sustave[7], Preporuku Komisije (EU) 2017/1584 o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera[8].

Mjere predložene u Aktu o kibersolidarnosti obuhvaćaju informiranost o stanju, dijeljenje informacija te potporu pripravnosti i odgovoru na kiberincidente. Te su mjere u skladu s

[5] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2).

[6] Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti).

[7] Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP.

[8] Prijedlog uredbe Europskog parlamenta i Vijeća o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020, COM(2022) 454 final.

ciljevima važećeg regulatornog okvira na razini Unije, posebno Direktive (EU) 2022/2555 („Direktiva NIS 2”), te ih podupiru. Akt o kibersolidarnosti posebno će se temeljiti na postojećim okvirima za operativnu suradnju i upravljanje krizama u području kibersigurnosti i podupirati ih, posebno na Europskoj mreži organizacija za vezu za kiberkrize (mreža EU-CyCLONe) i mreži timova za odgovor na računalne sigurnosne incidente (CSIRT-ovi).

Prekogranične platforme SOC-ova trebale bi nuditi nove mogućnosti komplementarne mreži CSIRT-ova objedinjavanjem i razmjenom podataka o kibersigurnosnim prijetnjama dobivenih od javnih i privatnih subjekata, povećanjem vrijednosti takvih podataka stručnim analizama i najsuvremenijim alatima te doprinosom razvoju sposobnosti i tehnološke suverenosti Unije.

Naposljetku, ovaj je Prijedlog u skladu s Preporukom Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture[9] u kojoj se države članice pozivaju da poduzmu hitne i učinkovite mjere te da lojalno, učinkovito, solidarno i koordinirano surađuju međusobno, s Komisijom i s drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se upotrebljava za pružanje osnovnih usluga na unutarnjem tržištu.

- **Dosljednost u odnosu na druge politike Unije**

Prijedlog je u skladu s drugim mehanizmima i protokolima za krizne situacije, kao što je mehanizam za integrirani politički odgovor na krizu (IPCR). Aktom o kibersolidarnosti ti će se okviri i protokoli za upravljanje krizama dopuniti pružanjem namjenske potpore za pripravnost i odgovor na kiberincidente. Prijedlog će biti usklađen i s vanjskim djelovanjem EU-a kao odgovor na incidente velikih razmjera u okviru zajedničke vanjske i sigurnosne politike (ZVSP), među ostalim s pomoću alata EU-a za kiberdiplomaciju. Prijedlogom će se dopuniti mjere koje se primjenjuju u kontekstu članka 42. stavka 7. Ugovora o Europskoj uniji ili u situacijama definiranima u članku 222. Ugovora o funkcioniranju Europske unije.

Njime se dopunjuje i Mehanizam Unije za civilnu zaštitu[10] uspostavljen u prosincu 2013. i dopunjen novim zakonodavstvom donesenim u svibnju 2021.[11], kojim se jačaju stupovi prevencije, pripravnosti i odgovora Mehanizma Unije za civilnu zaštitu te osiguravaju dodatni kapaciteti EU-a za odgovor na nove rizike u Europi i svijetu te povećava pričuva sustava rescEU.

---

[9] Preporuka Vijeća od 8. prosinca 2022. o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture (Tekst značajan za EGP), 2023/C 20/01.

[10] Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu (Tekst značajan za EGP).

[11] Uredba (EU) 2021/836 Europskog parlamenta i Vijeća od 20. svibnja 2021. o izmjeni Odluke br. 1313/2013/EU o Mehanizmu Unije za civilnu zaštitu (Tekst značajan za EGP).

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

• Pravna osnova

Pravna je osnova za ovaj Prijedlog članak 173. stavak 3. i članak 322. stavak 1. točka (a) Ugovora o funkcioniranju Europske unije (UFEU). Člankom 173. UFEU-a predviđeno je da Unija i države članice osiguravaju potrebne uvjete za konkurentnost industrije Unije. Cilj je ove Uredbe ojačati konkurentni položaj industrije i uslužnih sektora u Europi u digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Konkretno, cilj joj je povećati otpornost građana, poduzeća i subjekata koji djeluju u kritičnim i visokokritičnim sektorima na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice.

Prijedlog se temelji i na članku 322. stavku 1. točki (a) UFEU-a jer sadržava posebna pravila o prijenosu kojima se odstupa od načela jedne godine utvrđenog u Uredbi (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća („Financijska uredba")[12]. Za potrebe dobrog financijskog upravljanja i uzimajući u obzir nepredvidivu, iznimnu i specifičnu prirodu kibersigurnosnog okruženja i kiberprijetnji, mehanizam za izvanredne kibersigurnosne situacije trebao bi imati određeni stupanj fleksibilnosti u pogledu upravljanja proračunom, konkretno omogućivanjem automatskog prijenosa neiskorištenih odobrenih sredstava za preuzimanje obveza i odobrenih sredstava za plaćanje za mjere namijenjene ostvarivanju ciljeva iz Uredbe u sljedeću financijsku godinu. Budući da to novo pravilo otvara pitanja povezana s Financijskom uredbom, to bi se pitanje moglo riješiti u kontekstu aktualnih pregovora o preinaci Financijske uredbe.

• Supsidijarnost (za neisključivu nadležnost)

Zbog izražene prekogranične naravi kibersigurnosnih prijetnji i sve većeg broja rizika i incidenata, koji imaju učinke prelijevanja preko granica, sektora i proizvoda, države članice ne mogu same učinkovito ostvariti ciljeve ove intervencije te je potrebno zajedničko djelovanje i solidarnost na razini Unije.

Iskustvo u borbi protiv kiberprijetnji stečeno na temelju rata Rusije protiv Ukrajine te iskustva stečena vježbom u području kibersigurnosti provedenom tijekom francuskog predsjedanja (EU CyCLES), pokazali su da bi trebalo razviti konkretne mehanizme uzajamne potpore, posebno suradnju s privatnim sektorom, kako bi se postigla solidarnost na razini EU-a. U tom se kontekstu u Zaključcima Vijeća od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora Komisija poziva da predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti.

Potpora i mjere na razini Unije radi boljeg otkrivanja kibersigurnosnih prijetnji te povećanja kapaciteta za pripravnost i odgovor pružaju dodanu vrijednost jer se njima izbjegava udvostručavanje napora na razini Unije i u državama članicama. To bi omogućilo bolje

[12] Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije (SL L 193, 30.7.2018., str. 1.).

iskorištavanje postojećih sredstava te bolju koordinaciju i razmjenu informacija o stečenim iskustvima. U okviru mehanizma za izvanredne kibersigurnosne situacije predviđa se i pružanje potpore trećim zemljama pridruženima programu Digitalna Europa iz kibersigurnosne pričuve EU-a.

Potporom koja se pruža u okviru različitih inicijativa koje će se uspostaviti i financirati na razini Unije dopunit će se, a ne udvostručiti nacionalni kapaciteti za otkrivanje, informiranost o stanju, pripravnost i odgovor na kiberprijetnje i kiberincidente.

•Proporcionalnost

Mjere ne prelaze ono što je potrebno za ostvarivanje općih i posebnih ciljeva Uredbe. Mjere iz ove Uredbe ne utječu na odgovornosti država članica za nacionalnu sigurnost, javnu sigurnost, sprečavanje, istragu, otkrivanje i progon kaznenih djela. Ne utječu ni na pravne obveze subjekata koji posluju u kritičnim i visokokritičnim sektorima da uvedu kibersigurnosne mjere u skladu s Direktivom NIS 2.

Mjere obuhvaćene ovom Uredbom dopunjuju takva nastojanja i mjere jer doprinose stvaranju infrastrukture za bolje otkrivanje i analizu prijetnji te aktivnostima pripravnosti i odgovora u slučaju značajnih incidenata ili incidenata velikih razmjera.

- **Odabir instrumenta**

Prijedlog dolazi u obliku uredbe Europskog parlamenta i Vijeća. To je najprikladniji pravni instrument jer se samo uredbom i njezinim izravno primjenjivim pravnim odredbama može osigurati stupanj ujednačenosti koji je potreban za uspostavu i funkcioniranje europskog kiberštita i mehanizma za izvanredne kibersigurnosne situacije tako što se njome omogućuje potpora iz programa Digitalna Europa za njihovu uspostavu i predviđaju jasni uvjeti za korištenje i dodjelu te potpore.

3. REZULTATI *EX POST* EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

- **Savjetovanja s dionicima**

Mjere iz ove Uredbe poduprijet će se programom Digitalna Europa, o čemu se opsežno savjetovalo. Osim toga, temeljit će se na prvim koracima koji su osmišljeni u bliskoj suradnji s glavnim dionicima. Kad je riječ o SOC-ovima, Komisija je sastavila dokument za raspravu o razvoju prekograničnih platformi SOC-ova i poziv na iskaz interesa u bliskoj suradnji s državama članicama u okviru Europskog stručnog centra u području kibersigurnosti (ECCC). U tom je kontekstu provedena anketa o kapacitetima nacionalnih SOC-ova te se raspravljalo o zajedničkim pristupima i tehničkim zahtjevima u okviru tehničke radne skupine ECCC-a koja okuplja predstavnike država članica. Osim toga, razmijenjena su stajališta s industrijom,

prvenstveno u okviru stručne skupine za SOC-ove koju su osnovale ENISA i Europska organizacija za kibersigurnost (ECSO).

K tomu, kad je riječ o pripravnosti i odgovoru na incidente, Komisija je uspostavila kratkoročni program za potporu državama članicama dodjelom dodatnih sredstava ENISA-i u okviru programa Digitalna Europa kako bi se hitno ojačali pripravnost i kapaciteti za odgovor na velike kiberincidente. Povratne informacije država članica i industrije prikupljene tijekom provedbe ovog kratkoročnog programa već pružaju vrijedan uvid koji je uvršten u pripremu predložene uredbe kako bi se uklonili utvrđeni nedostaci. To je bio prvi korak u skladu sa Zaključcima Vijeća o razvoju položaja u pogledu kiberprostora, u kojem je od Komisije zatraženo da iznese prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti.

Osim toga, 16. veljače 2023. održana je radionica sa stručnjacima iz država članica o mehanizmu za izvanredne kibersigurnosne situacije na temelju dokumenta za raspravu. Sve države članice sudjelovale su na toj radionici, a jedanaest država članica dostavilo je dodatne doprinose u pisanom obliku.

- **Procjena učinka**

Procjena učinka nije provedena zbog žurnosti Prijedloga. Mjere iz ove uredbe podupirat će se programom Digitalna Europa te su one u skladu s mjerama utvrđenima u Uredbi o programu Digitalna Europa, koja je bila predmet posebne procjene učinka. Ova uredba neće imati znatne administrativne učinke ili učinke na okoliš osim onih koji su već utvrđeni u procjeni učinka Uredbe o programu Digitalna Europa.

Nadalje, temelji se na prvim mjerama razvijenima u bliskoj suradnji s glavnim dionicima, kako je prethodno navedeno, i na pozivu država članica Komisiji da do kraja trećeg tromjesečja 2022. predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti.

Konkretno, kad je riječ o informiranosti o stanju i otkrivanju u okviru europskog kiberštita, u okviru programa rada za kibersigurnost programa Digitalna Europa za razdoblje 2021.–2022. objavljen je poziv na iskaz interesa za zajedničku nabavu alata i infrastrukture za uspostavu prekograničnih SOC-ova te poziv za dodjelu bespovratnih sredstava za izgradnju kapaciteta SOC-ova koji služe javnim i privatnim organizacijama.

U području pripravnosti i odgovora na incidente, kako je prethodno navedeno, Komisija je uspostavila kratkoročni program za potporu državama članicama u okviru programa Digitalna Europa, koji provodi ENISA. Obuhvaćene usluge uključuju mjere pripravnosti, kao što su penetracijsko testiranje kritičnih subjekata kako bi se identificirale slabe točke. Povećavaju se i mogućnosti za pomoć državama članicama u slučaju velikog incidenta koji utječe na kritične subjekte. ENISA trenutačno provodi taj kratkoročni program, što je već omogućilo relevantne uvide koji su uzeti u obzir pri pripremi ove Uredbe.

- **Temeljna prava**

Budući da se ovim prijedlogom doprinosi sigurnosti digitalnih informacija, njime će se doprinijeti i zaštiti prava na slobodu i sigurnost u skladu s člankom 6. Povelje EU-a o temeljnim pravima te prava na poštovanje privatnog i obiteljskog života u skladu s člankom 7. Povelje. Prijedlogom će se doprinijeti i slobodi poduzetništva u skladu s člankom 16. Povelje EU-a o temeljnim pravima te zaštiti prava na vlasništvo u skladu s člankom 17. Povelje jer će se poduzeća zaštititi od ekonomski štetnih kibernapada. Naposljetku, prijedlogom će se zaštititi integritet kritične infrastrukture u slučaju kibernapada te će se na taj način doprinijeti zaštiti prava na zdravstvenu zaštitu u skladu s člankom 35. Povelje EU-a o temeljnim pravima i prava na pristup uslugama od općeg gospodarskog interesa u skladu s člankom 36. Povelje.

4. UTJECAJ NA PRORAČUN

Mjere iz ove uredbe podupirat će se financiranjem u okviru strateškog cilja „Kibersigurnost" programa Digitalna Europa.

Ukupni proračun uključuje povećanje od 100 milijuna EUR, a ovom se Uredbom predlaže da se taj iznos preraspodjeli iz drugih strateških ciljeva programa Digitalna Europa. Time će se novi ukupni iznos dostupan za mjere u području kibersigurnosti u okviru programa Digitalna Europa povećati na 842,8 milijuna EUR.

Jedan dio dodatnih 100 milijuna EUR iskoristit će se za povećanje proračuna kojim upravlja ECCC kako bi se provele mjere za SOC-ove i pripravnost u okviru njihovih programa rada. Nadalje, dodatna sredstva poslužit će za potporu uspostavi kibersigurnosne pričuve EU-a.

Njima se dopunjuje proračun koji je već predviđen za slična djelovanja u glavnom programu Digitalna Europa i programu rada u području kibersigurnosti programa Digitalna Europa za razdoblje 2023.–2027., čime bi se ukupni iznos mogao povećati na 551 milijun za razdoblje 2023.–2027., dok je iznos od 115 milijuna već bio izdvojen u obliku pilot-projekata za razdoblje 2021.–2022. Kad se pribroje doprinosi država članica, ukupni bi proračun mogao iznositi do 1 109 milijardi EUR.

Pregled uključenih troškova uključen je u „zakonodavni financijski izvještaj" priložen ovom Prijedlogu.

5. DRUGI ELEMENTI

- **Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja**

Komisija će pratiti provedbu, primjenu i sukladnost s tim novim odredbama kako bi procijenila njihovu djelotvornost. Komisija podnosi izvješće o evaluaciji i preispitivanju ove Uredbe Europskom parlamentu i Vijeću u roku od četiri godine od datuma njezine primjene.

- **Detaljno obrazloženje posebnih odredaba prijedloga**

Opći ciljevi, predmet i definicije (poglavlje I.)

U poglavlju I. utvrđuju se ciljevi Uredbe za jačanje solidarnosti na razini Unije radi boljeg otkrivanja, pripreme i odgovora na kibersigurnosne prijetnje i incidente, a posebno za unapređenje zajedničkog otkrivanja kiberprijetnji i kiberincidenata i informiranosti o stanju u Uniji, jačanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u cijeloj Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera te povećanje otpornosti Unije preispitivanjem i procjenom značajnih incidenata ili incidenata velikih razmjera. U ovom se poglavlju utvrđuju i mjere za postizanje tih ciljeva: uspostava europskog kiberštita, mehanizma za izvanredne kibersigurnosne situacije i mehanizma za istraživanje kibersigurnosnih incidenata. Utvrđuju se i definicije koje se upotrebljavaju u cijelom instrumentu.

Europski kiberštit (poglavlje II.)

U poglavlju II. uspostavlja se europski kiberštit i utvrđuju njegovi različiti elementi i uvjeti za sudjelovanje. Prvo, u njemu se navodi opći cilj europskog kiberštita, a to je razvoj naprednih sposobnosti Unije za otkrivanje, analizu i obradu podataka o kiberprijetnjama i kiberincidentima u Uniji, kao i posebni operativni ciljevi. U njemu se dalje navodi da Unija financira europski kiberštit u skladu s Uredbom o programu Digitalna Europa.

Nadalje, u poglavlju se opisuje vrsta subjekata koji će činiti europski kiberštit. Štit se sastoji od nacionalnih centara za sigurnosne operacije („nacionalnih SOC-ova”) i prekograničnih centara za sigurnosne operacije („prekograničnih SOC-ova”). Svaka država članica sudionica imenuje nacionalni SOC. On će služiti drugim javnim i privatnim organizacijama na nacionalnoj razini kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. Nakon poziva na iskaz interesa ECCC može odabrati nacionalni SOC koji će sudjelovati u zajedničkoj nabavi alata i infrastrukture s ECCC-om i kojem će se dodijeliti bespovratna sredstva za rad tih alata i infrastrukture. Ako nacionalni SOC ima koristi od potpore Unije, obvezuje se podnijeti zahtjev za sudjelovanje u prekograničnom SOC-u u roku od dvije godine.

Prekogranični SOC-ovi sastoje se od konzorcija koji čine najmanje tri države članice, koje predstavljaju nacionalni SOC-ovi, koje su se obvezale međusobno surađivati radi koordinacije svojih aktivnosti otkrivanja i praćenja kiberprijetnji. Nakon početnog poziva na iskaz interesa ECCC može odabrati konzorcija domaćina koji će sudjelovati u zajedničkoj nabavi alata i infrastrukture s ECCC-om i kojem će dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Članovi konzorcija domaćina sklapaju pisani ugovor o konzorciju kojim se utvrđuju njihovi interni aranžmani. U ovom se poglavlju zatim navode zahtjevi za razmjenu informacija među sudionicima u prekograničnom SOC-u i za razmjenu informacija

među prekograničnim SOC-ovima, kao i s relevantnim subjektima EU-a. Nacionalni SOC-ovi koji sudjeluju u prekograničnom SOC-u međusobno dijele relevantne informacije povezane s kiberprijetnjama, a pojedinosti, uključujući obvezu dijeljenja znatne količine podataka i uvjete za to, trebalo bi definirati u ugovoru o konzorciju. Prekogranični SOC-ovi osiguravaju visoku razinu međusobne interoperabilnosti. Isto tako, prekogranični SOC-ovi trebali bi s drugim prekograničnim SOC-ovima sklapati sporazume o suradnji u kojima se navode načela dijeljenja informacija. Ako prekogranični SOC-ovi dobiju informacije o potencijalnom ili aktualnom kibersigurnosnom incidentu velikih razmjera, dostavljaju relevantne informacije mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji u skladu sa svojim ulogama u upravljanju krizama na temelju Direktive (EU) 2022/2555. Na kraju poglavlja II. navode se sigurnosni uvjeti za sudjelovanje u europskom kiberštitu.

Mehanizam za izvanredne kibersigurnosne situacije (poglavlje III.)

U poglavlju III. uspostavlja se mehanizam za izvanredne kibersigurnosne situacije kako bi se poboljšala otpornost Unije na velike kibersigurnosne prijetnje te kako bi se na solidaran način pripremili za i ublažili kratkoročan učinak značajnih kibersigurnosnih incidenata ili kriza i kibersigurnosnih incidenata ili kriza velikih razmjera. Mjere za provedbu mehanizma za izvanredne kibersigurnosne situacije financiraju se u okviru programa Digitalna Europa. Mehanizmom se omogućuju mjere koje bi podupirale pripravnost, uključujući koordinirano testiranje subjekata koji djeluju u visokokritičnim sektorima, odgovor na značajne kiberincidente ili kiberincidente velikih razmjera i hitan oporavak od njih ili ublažavanje značajnih kiberprijetnji, te mjere uzajamne pomoći.

Mjere pripravnosti u okviru mehanizma za izvanredne kibersigurnosne situacije uključuju koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim sektorima. Komisija bi, nakon savjetovanja s ENISA-om i Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava, trebala među sektorima visokog stupnja kritičnosti navedenima u Prilogu I. Direktivi (EU) 2022/2555 redovito utvrđivati relevantne sektore ili podsektore iz kojih se subjekti mogu podvrgavati koordiniranom testiranju pripravnosti na razini EU-a.

Za potrebe primjene predloženih mjera odgovora na incidente ovom se Uredbom uspostavlja kibersigurnosna pričuva EU-a, koja se sastoji od usluga odgovora na incidente pouzdanih pružatelja usluga, odabranih u skladu s kriterijima utvrđenima u ovoj Uredbi. Korisnici usluga kibersigurnosne pričuve EU-a uključuju tijela za upravljanje kiberkrizama i CSIRT-ove iz država članica te institucije, tijela i agencije Unije. Komisija je općenito odgovorna za primjenu kibersigurnosne pričuve EU-a te može rad i vođenje kibersigurnosne pričuve EU-a u cijelosti ili djelomično povjeriti ENISA-i.

Kako bi primili potporu iz kibersigurnosne pričuve EU-a, korisnici bi trebali poduzeti vlastite mjere za ublažavanje posljedica incidenta za koji se traži potpora. Zahtjevi za potporu iz kibersigurnosne pričuve EU-a trebali bi sadržavati odgovarajuće informacije o incidentu i mjerama koje su korisnici već poduzeli. U poglavlju se opisuju i načini provedbe, uključujući procjenu zahtjeva za potporu iz kibersigurnosne pričuve EU-a.

Uredbom se propisuju i načela nabave i kriteriji za odabir pouzdanih pružatelja usluga u okviru kibersigurnosne pričuve EU-a.

Treće zemlje mogu zatražiti potporu iz kibersigurnosne pričuve EU-a ako je tako uređeno sporazumima o pridruživanju sklopljenima u pogledu njihova sudjelovanja u programu Digitalna Europa. U ovom se poglavlju opisuju daljnji uvjeti i načini takvog sudjelovanja.

Mehanizam za istraživanje kibersigurnosnih incidenata (poglavlje IV.)

Na zahtjev Komisije, mreže EU-CyCLONe ili mreže CSIRT-ova ENISA bi trebala istražiti i procijeniti prijetnje, ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibersigurnosni incident ili kibersigurnosni incident velikih razmjera. ENISA bi rezultate istrage i procjene trebala dostaviti mreži CSIRT-ova, mreži EU-CyCLONe i Komisiji u obliku izvješća o istraživanju incidenta kako bi im pomogla u obavljanju njihovih zadaća. Ako se incident odnosi na treću zemlju, Komisija bi izvješće trebala poslati Visokom predstavniku. Izvješće bi trebalo uključivati stečena iskustva i, prema potrebi, preporuke za poboljšanje položaja Unije u pogledu kiberprostora.

Završne odredbe (poglavlje V.)

Poglavlje V. sadržava izmjene Uredbe o programu Digitalna Europa i obvezu Komisije da Europskom parlamentu i Vijeću podnosi redovita izvješća za evaluaciju i reviziju Uredbe. Komisija je ovlaštena za donošenje provedbenih akata u skladu s postupkom ispitivanja iz članka 21. kako bi: utvrdila uvjete za interoperabilnost među prekograničnim SOC-ovima; odredila postupovne aranžmane za dijeljenje informacija između prekograničnih SOC-ova i subjekata Unije koje su povezane s potencijalnim ili aktualnim kibersigurnosnim incidentima velikih razmjera; utvrdila tehničke zahtjeve kako bi se osigurala visoka razina sigurnosti podataka i fizičke sigurnosti infrastrukture te zaštitili sigurnosni interesi Unije pri dijeljenju informacija sa subjektima koji nisu javna tijela država članica; odredila vrste i broj usluga odgovora potrebnih za kibersigurnosnu pričuvu EU-a; i dodatno utvrdila detaljne aranžmane za dodjelu usluga potpore iz kibersigurnosne pričuve EU-a.

2023/0109 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 173. stavak 3. i članak 322. stavak 1. točku (a),

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Revizorskog suda[1],

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[2],

uzimajući u obzir mišljenje Odbora regija[3],

u skladu s redovnim zakonodavnim postupkom,

budući da:

(1) Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora gospodarstva jer su javne uprave, poduzeća i građani međusobno povezani i ovisni jedni o drugima u svim sektorima i prekogranično više nego ikada prije.

(2) Povećavaju se razmjeri i učestalost te pogoršavaju posljedice kiberincidenata, uključujući napade na lance opskrbe s ciljem kiberšpijunaže, napad ucjenjivačkim softverom ili izazivanje poremećaja. Oni predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava. S obzirom na to da se prijetnje brzo mijenjaju, mogući incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu na kritičnoj infrastrukturi zahtijevaju povećanu pripravnost na svim razinama okvira Unije za kibersigurnost. Ta prijetnja nadilazi rusku vojnu agresiju na Ukrajinu i vjerojatno će se nastaviti s obzirom na mnoštvo državi bliskih, kriminalnih i haktivističkih aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga i obavljanje gospodarskih djelatnosti, među ostalim u kritičnim ili visokokritičnim sektorima, uzrokovati znatne financijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu Unije te čak imati zdravstvene ili po život opasne posljedice. K tomu, kibersigurnosni incidenti su nepredvidivi jer se često pojavljuju i razvijaju u vrlo kratkim vremenskim razdobljima, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u mnogim zemljama ili se brzo šire na mnoge zemlje.

---

1 SL C […], […], str. […].
2 SL C , , str. .
3 SL C , , str. .

(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe[4], potrebno je povećati otpornost građana, poduzeća i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoć u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibersigurnosnim prijetnjama i incidentima.

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća[5], Preporuku Komisije (EU) 2017/1584[6], Direktivu 2013/40/EU Europskog parlamenta i Vijeća[7] i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[8]. Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

(5) Zbog sve većih kibersigurnosnih rizika i općenito složenih prijetnji te uz očit rizik od brzog prelijevanja kiberincidenata iz jedne države članice u druge i iz treće zemlje u Uniju, potrebna je snažnija solidarnost na razini Unije kako bi se bolje otkrile kibersigurnosne prijetnje i incidenti te kako bi se za njih bolje pripremilo i na njih bolje odgovorilo. Države članice pozvale su Komisiju i da predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti u Zaključcima Vijeća o položaju EU-a u pogledu kiberprostora[9].

(6) U Zajedničkoj komunikaciji o politici EU-a o kiberobrani[10] donesenoj 10. studenoga 2022. najavljena je inicijativa EU-a za kibersolidarnost sa sljedećim ciljevima: jačanje zajedničkih kapaciteta EU-a za otkrivanje, informiranost o stanju i

---

4 https://futureu.europa.eu/hr/?locale=hr

5 Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (SL L 333, 27.12.2022.).

6 Preporuka Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera (SL L 239, 19.9.2017., str. 36.).

7 Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP (SL L 218, 14.8.2013., str. 8.).

8 Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti), (SL L 151, 7.6.2019., str. 15.).

9 Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje je Vijeće odobrilo na sastanku 23. svibnja 2022. (9364/22).

10 Zajednička komunikacija Europskom parlamentu i Vijeću „Politika EU-a o kiberobrani”, JOIN/2022/49 final.

odgovor poticanjem uvođenja infrastrukture EU-a za centre za sigurnosne operacije (SOC-ove), podupiranje postupne izgradnje kibersigurnosne pričuve na razini EU-a s uslugama pouzdanih privatnih pružatelja usluga i testiranje kritičnih subjekata na moguće ranjivosti na temelju procjena rizika EU-a.

(7) Potrebno je poboljšati otkrivanje kiberprijetnji i kiberincidenata u cijeloj Uniji i informiranost o njihovu stanju te ojačati solidarnost unapređenjem pripravnosti država članica i Unije te njihove sposobnosti za odgovor na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera. Stoga je potrebno uvesti paneuropsku infrastrukturu SOC-ova (europski kiberštit) kako bi se izgradili i poboljšale zajedničke sposobnosti za otkrivanje i informiranost o stanju; trebalo bi uspostaviti mehanizam za izvanredne kibersigurnosne situacije kako bi se državama članicama pomoglo u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih; trebalo bi uspostaviti i mehanizam za istraživanje kibersigurnosnih incidenata kako bi se istražili i procijenili određeni značajni incidenti ili incidenti velikih razmjera. Tim se mjerama ne dovode u pitanje članci 107. i 108. Ugovora o funkcioniranju Europske unije (UFEU).

(8) Radi postizanja tih ciljeva neophodno je izmijeniti određene dijelove Uredbe (EU) 2021/694 Europskog parlamenta i Vijeća[11]. Konkretno, ovom bi se Uredbom trebala izmijeniti Uredba (EU) 2021/694 u dijelu koji se odnosi na dodavanje novih operativnih ciljeva povezanih s europskim kiberštitom i mehanizmom za izvanredne kibersigurnosne situacije u okviru specifičnog cilja 3 programa Digitalna Europa, kojim se nastoji zajamčiti otpornost, integritet i pouzdanost jedinstvenog digitalnog tržišta, ojačati kapacitete za praćenje kibernapada i prijetnji i odgovor na njih te ojačati prekograničnu suradnju u području kibersigurnosti. Osim toga, trebalo bi utvrditi posebne uvjete pod kojima se može dodijeliti financijska potpora za te mjere te bi trebalo definirati mehanizme upravljanja i koordinacije potrebne za postizanje predviđenih ciljeva. Druge izmjene Uredbe (EU) 2021/694 trebale bi uključivati opise predloženih mjera u okviru novih operativnih ciljeva, kao i mjerljive pokazatelje za praćenje provedbe tih ciljeva.

(9) Financiranje mjera u okviru ove Uredbe trebalo bi biti propisano Uredbom (EU) 2021/694, koja bi trebala ostati relevantni temeljni akt za te mjere obuhvaćene specifičnim ciljem 3 programa Digitalna Europa. Posebni uvjeti za sudjelovanje za svaku mjeru bit će definirani u relevantnim programima rada, u skladu s primjenjivom odredbom Uredbe (EU) 2021/694.

(10) Na ovu se Uredbu primjenjuju horizontalna financijska pravila koja su Europski parlament i Vijeće donijeli na temelju članka 322. UFEU-a. Ta su pravila utvrđena u Financijskoj uredbi i njima se osobito određuje postupak donošenja i izvršenja proračuna Unije te predviđaju provjere odgovornosti financijskih izvršitelja. Pravila donesena na temelju članka 322. UFEU-a uključuju i opći režim uvjetovanosti za zaštitu proračuna Unije kako je utvrđen u Uredbi (EU, Euratom) 2020/2092 Europskog parlamenta i Vijeća.

(11) U svrhu dobrog financijskog upravljanja trebalo bi utvrditi posebna pravila za prijenos neiskorištenih odobrenih sredstava za preuzete obveze i odobrenih sredstava za plaćanje. Uz poštovanje načela da se proračun Unije utvrđuje na godišnjoj razini,

[11] Uredba (EU) 2021/694 Europskog parlamenta i Vijeća od 29. travnja 2021. o uspostavi programa Digitalna Europa te o stavljanju izvan snage Odluke (EU) 2015/2240 (SL L 166, 11.5.2021., str. 1.).

ovom bi se Uredbom, zbog nepredvidive, neuobičajene i specifične prirode kibersigurnosnog okruženja, trebao omogućiti prijenos neiskorištenih sredstava koja premašuju ona utvrđena u Financijskoj uredbi, čime bi se maksimalno povećao kapacitet mehanizma za izvanredne kibersigurnosne situacije za potporu državama članicama u djelotvornoj borbi protiv kiberprijetnji.

(12) Kako bi se učinkovitije spriječile i procijenile kiberprijetnje i kiberincidenti te na njih odgovorilo, potrebno je steći sveobuhvatnije znanje o prijetnjama ključnim resursima i infrastrukturi na području Unije, uključujući njihovu geografsku raspoređenost, međusobnu povezanost i potencijalne posljedice u slučaju kibernapada koji pogađaju te infrastrukture. Trebalo bi uvesti opsežnu infrastrukturu EU-a za SOC-ove („europski kiberštit”), koja se sastoji od nekoliko interoperabilnih prekograničnih platformi, od kojih svaka okuplja nekoliko nacionalnih SOC-ova. Ta bi infrastruktura trebala služiti kibersigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijom tehnologijom za napredne alate za prikupljanje i analizu podataka, jačajući kapacitete otkrivanja i upravljanja kibertehnologijama i osiguravajući informiranost o stanju u stvarnom vremenu. Ta bi infrastruktura trebala služiti za bolje otkrivanje kibersigurnosnih prijetnji i incidenata te na taj način dopunjavati i podržavati subjekte i mreže Unije odgovorne za upravljanje krizama u Uniji, posebno Europsku mrežu organizacija za vezu za kiberkrize („EU-CyCLONe”), kako je definirana u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća[12].

(13) Svaka bi država članica trebala na nacionalnoj razini imenovati javnopravno tijelo zaduženo za koordinaciju aktivnosti otkrivanja kiberprijetnji u toj državi članici. Ti nacionalni SOC-ovi trebali bi djelovati kao referentna i pristupna točka na nacionalnoj razini za sudjelovanje u europskom kiberštitu te bi trebali osigurati da se informacije o kiberprijetnjama dobivene od javnih i privatnih subjekata dijele i prikupljaju na nacionalnoj razini na učinkovit i pojednostavnjen način.

(14) U okviru europskog kiberštita trebalo bi uspostaviti niz prekograničnih centara za sigurnosne operacije („prekograničnih SOC-ova”). U njima bi se trebali okupiti nacionalni SOC-ovi iz najmanje triju država članica kako bi se u potpunosti ostvarile koristi od otkrivanja prekograničnih prijetnji te dijeljenja informacija i upravljanja njima. Opći cilj prekograničnih SOC-ova trebao bi biti jačanje kapaciteta za analizu, sprečavanje i otkrivanje kibersigurnosnih prijetnji te podupiranje proizvodnje visokokvalitetnih obavještajnih podataka o kibersigurnosnim prijetnjama, osobito dijeljenjem podataka iz različitih izvora, javnih ili privatnih te dijeljenjem i zajedničkom uporabom najsuvremenijih alata i zajedničkim razvojem sposobnosti otkrivanja, analize i sprečavanja u pouzdanom okruženju. Njima bi se trebali osigurati dodatni kapaciteti, koji se temelje na postojećim SOC-ovima i timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovima) i drugim relevantnim akterima te ih nadopunjuju.

(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove

[12] Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsuvremenijim alatima te doprinosili razvoju sposobnosti i tehnološke suverenosti Unije.

(16) Prekogranični SOC-ovi trebali bi djelovati kao središnja točka koja omogućuje opsežno objedinjavanje relevantnih podataka i obavještajnih podataka o kiberprijetnjama, omogućiti širenje informacija o prijetnjama među velikim i različitim akterima (npr. timovima za hitne računalne intervencije (CERT-ovima), CSIRT-ovima, centrima za razmjenu i analizu informacija (ISAC-ima), operaterima ključnih infrastruktura). Informacije koje razmjenjuju sudionici u prekograničnom SOC-u mogle bi uključivati podatke iz mreža i senzora, obavještajne podatke o prijetnjama, pokazatelje ugroženosti i informacije o incidentima, prijetnjama i ranjivostima stavljene u kontekst. Osim toga, prekogranični SOC-ovi trebali bi sklapati sporazume o suradnji s drugim prekograničnim SOC-ovima.

(17) Nužan preduvjet za pripravnost i koordinaciju na razini Unije u pogledu značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera je da relevantna tijela budu jednako informirana o stanju. Direktivom (EU) 2022/2555 uspostavlja se EU-CyCLONe kako bi se omogućilo koordinirano upravljanje kibersigurnosnim incidentima i krizama velikih razmjera na operativnoj razini te kako bi se zajamčila redovita razmjena relevantnih informacija među državama članicama i institucijama, tijelima i agencijama Unije. U Preporuci (EU) 2017/1584 o koordiniranom odgovoru na kibersigurnosne incidente i krize velikih razmjera navedene su uloge svih relevantnih aktera. U Direktivi (EU) 2022/2555 se podsjeća i na odgovornosti Komisije u okviru Mehanizma Unije za civilnu zaštitu uspostavljenog Odlukom 1313/2013/EU Europskog parlamenta i Vijeća, kao i na odgovornost za dostavu analitičkih izvješća za aranžmane za integrirani politički odgovor na krizu (IPCR) na temelju Provedbene odluke (EU) 2018/1993. Kada dobiju informacije povezane s potencijalnim ili aktualnim kiberincidentima velikih razmjera, prekogranični SOC-ovi stoga bi trebali relevantne informacije proslijediti mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji. Konkretno, ovisno o situaciji, informacije koje se dijele mogle bi uključivati tehničke informacije, informacije o prirodi i motivima napadača ili potencijalnog napadača te netehničke informacije više razine o potencijalnom ili aktualnom kiberincidentu velikih razmjera. U tom bi kontekstu dužnu pozornost trebalo posvetiti načelu nužnosti pristupa podacima i potencijalno osjetljivoj prirodi informacija koje se dijele.

(18) Subjekti koji sudjeluju u europskom kiberštitu trebali bi osigurati visoku razinu međusobne interoperabilnosti, uključujući, prema potrebi, formata podataka, taksonomije, alata za obradu i analizu podataka te sigurnih komunikacijskih kanala, minimalne razine sigurnosti aplikacijskog sloja, pregleda informiranosti o stanju i pokazatelja. Pri donošenju zajedničke taksonomije i izradi predložaka za izvješća o stanju u kojima se opisuju tehnički uzroci i posljedice kibersigurnosnih incidenata trebalo bi uzeti u obzir aktualni rad na obavijestima o incidentima u kontekstu provedbe Direktive (EU) 2022/2555.

(19) Kako bi se omogućilo da se opsežna razmjena podataka o kibersigurnosnim prijetnjama iz različitih izvora odvija u pouzdanom okruženju, subjekti koji sudjeluju u europskom kiberštitu trebali bi biti opremljeni najsuvremenijim i vrlo sigurnim alatima, opremom i infrastrukturom. Time bi se trebalo omogućiti poboljšanje zajedničkih kapaciteta za otkrivanje i pravodobno upozoravanje nadležnih tijela i

relevantnih subjekata, posebno uporabom najnovijih tehnologija umjetne inteligencije i analitike podataka.

(20) Prikupljanjem, dijeljenjem i razmjenom podataka europski kiberštit trebao bi povećati tehnološku suverenost Unije. Objedinjavanje visokokvalitetnih prilagođenih podataka trebalo bi doprinijeti i razvoju naprednih tehnologija umjetne inteligencije i analitike podataka. To bi trebalo omogućiti povezivanjem europskog kiberštita s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom Uredbom Vijeća (EU) 2021/1173[13].

(21) Iako je europski kiberštit civilni projekt, zajednica za kiberobranu mogla bi imati koristi od bolje sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture. Prekogranični SOC-ovi, uz potporu Komisije i Europskog stručnog centra u području kibersigurnosti (ECCC) te u suradnji s Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”), trebali bi postupno razvijati namjenske protokole i standarde kako bi se omogućila suradnja sa zajednicom za kiberobranu, uključujući uvjete provjere i sigurnosti. Razvoj europskog kiberštita trebao bi biti popraćen razmatranjem načina na koji bi se omogućila buduća suradnja s mrežama i platformama odgovornima za dijeljenje informacija u zajednici za kiberobranu, u bliskoj suradnji s Visokim predstavnikom.

(22) Dijeljenje informacija među sudionicima europskog kiberštita trebalo bi biti u skladu s postojećim pravnim zahtjevima, a posebno s pravom Unije i nacionalnim pravom o zaštiti podataka, kao i s pravilima Unije o tržišnom natjecanju kojima se uređuje razmjena informacija. Primatelj informacija trebao bi, ako je obrada osobnih podataka potrebna, provesti tehničke i organizacijske mjere kojima se štite prava i slobode ispitanika te uništiti podatke čim ne budu potrebni za navedenu svrhu te obavijestiti tijelo koje je stavilo podatke na raspolaganje da su podaci uništeni.

(23) Ne dovodeći u pitanje članak 346. UFEU-a, razmjena povjerljivih informacija u skladu s pravilima Unije ili nacionalnim pravilima trebala bi biti ograničena na razmjenu informacija koja je relevantna i razmjerna svrsi. Prilikom razmjene takvih informacija trebala bi se očuvati povjerljivost informacija i zaštititi sigurnost i komercijalni interesi predmetnih subjekata te potpuno poštovati poslovne tajne.

(24) S obzirom na sve veće rizike i sve veći broj kiberincidenata koji pogađaju države članice, potrebno je uspostaviti instrument za potporu u kriznim situacijama kako bi se poboljšala otpornost Unije na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera te dopunile mjere država članica hitnom financijskom potporom za pripravnost, odgovor i hitan oporavak osnovnih usluga. Tim bi se instrumentom trebalo omogućiti brzo pružanje pomoći u definiranim okolnostima i pod jasnim uvjetima te omogućiti pažljivo praćenje i evaluacija uporabe sredstava. Iako glavnu odgovornost za sprečavanje kibersigurnosnih incidenata i kriza te pripravnost i odgovor na njih snose države članice, mehanizmom za izvanredne kibersigurnosne situacije promiče se solidarnost među državama članicama u skladu s člankom 3. stavkom 3. Ugovora o Europskoj uniji (UEU).

[13] Uredba Vijeća (EU) 2021/1173 od 13. srpnja 2021. o osnivanju Zajedničkog poduzeća za europsko računalstvo visokih performansi te stavljanju izvan snage Uredbe (EU) 2018/1488 (SL L 256, 19.7.2021., str. 3.).

(25) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružiti potpora državama članicama te bi se trebale dopuniti njihove vlastite mjere i resursi te druge postojeće mogućnosti potpore u slučaju odgovora na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera i hitnog oporavka od njih, kao što su usluge koje pruža Agencija Europske unije za kibersigurnost (ENISA) u skladu sa svojim mandatom, koordinirani odgovor i pomoć mreže CSIRT-ova, potpora za ublažavanje posljedica koju pruža EU-CyCLONe, te uzajamna pomoć među državama članicama, među ostalim u kontekstu članka 42. stavka 7. UEU-a, timovi za brz odgovor na kiberincidente u okviru PESCO-a[14] i timovi za brz odgovor na hibridne prijetnje. Njime bi se trebalo odgovoriti na potrebu da se osigura dostupnost specijaliziranih sredstava za potporu pripravnosti i odgovoru na kibersigurnosne incidente u cijeloj Uniji i u trećim zemljama.

(26) Ovim se instrumentom ne dovode u pitanje postupci i okviri za koordinaciju odgovora na krizu na razini Unije, posebno Mehanizam Unije za civilnu zaštitu[15], IPCR[16,] i Direktiva (EU) 2022/2555. Može doprinijeti ili dopuniti mjere koje su donesene u kontekstu članka 42. stavka 7. UEU-a ili u situacijama definiranima u članku 222. UFEU-a. Uporabu ovog instrumenta trebalo bi, prema potrebi, koordinirati i s provedbom mjera u okviru alata za kiberdiplomaciju.

(27) Pomoć koja se pruža na temelju ove Uredbe trebala bi doprinositi mjerama koje države članice poduzimaju na nacionalnoj razini i nadopunjavati ih. U tu bi svrhu trebalo osigurati blisku suradnju i savjetovanje između Komisije i pogođene države članice. Pri podnošenju zahtjeva za potporu u okviru mehanizma za izvanredne kibersigurnosne situacije država članica trebala bi dostaviti relevantne informacije kojima se obrazlaže potreba za potporom.

(28) Prema Direktivi (EU) 2022/2555 države članice dužne su imenovati ili uspostaviti jedno ili više tijela za upravljanje kiberkrizama i osigurati da ta tijela imaju odgovarajuće resurse za učinkovito i efikasno obavljanje svojih zadaća. Isto su tako dužne utvrditi kapacitete, sredstva i postupke koji se mogu primijeniti u slučaju krize te donijeti nacionalni plan za odgovor na kibersigurnosne incidente velikih razmjera i krize u kojem su utvrđeni ciljevi i načini upravljanja kibersigurnosnim incidentima velikih razmjera i krizama. Od država članica zahtijeva se i da uspostave jedan ili više CSIRT-ova, koji će biti zaduženi za postupanje s incidentima u skladu s točno propisanim postupkom i obuhvaćati barem sektore, podsektore i vrste subjekata obuhvaćene područjem primjene navedene direktive, te im osigurati odgovarajuće resurse za učinkovito izvršavanje zadaća. Ovom se Uredbom ne dovodi u pitanje uloga Komisije u osiguravanju usklađenosti država članica s obvezama iz Direktive (EU) 2022/2555. Mehanizmom za kibersigurnost trebala bi se pružiti pomoć za djelovanja usmjerena na jačanje pripravnosti i djelovanja za odgovor na incidente kako bi se ublažile posljedice značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera, podržao hitan oporavak i/ili ponovno uspostavilo funkcioniranje osnovnih usluga.

---

14 ODLUKA VIJEĆA (ZVSP) 2017/2315 od 11. prosinca 2017. o uspostavi stalne strukturirane suradnje (PESCO) i utvrđivanju popisa država članica sudionica.

15 Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu (SL L 347, 20.12.2013., str. 924.).

16 Aranžmani za integrirani politički odgovor na krizu (IPCR) u skladu s Preporukom Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera.

(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti"). Koordinirane vježbe testiranja trebale bi se temeljiti na zajedničkim scenarijima i metodama procjene rizika. Pri odabiru sektora i razvoju scenarija rizika trebalo bi uzeti u obzir relevantne procjene rizika i scenarije rizika na razini Unije, uključujući potrebu za izbjegavanjem njihova udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje trebaju provesti Komisija, Visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za elektroničke komunikacije (BEREC), koordinirane procjene rizika koje treba provesti na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća[17]. Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

(30) Osim toga, mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružati potpora drugim mjerama pripravnosti i podupirati pripravnost u drugim sektorima koji nisu obuhvaćeni koordiniranim testiranjem subjekata koji djeluju u visokokritičnim sektorima. Te bi mjere mogle uključivati različite vrste aktivnosti za nacionalnu pripravnost.

(31) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružati potpora i mjerama za odgovor na incidente kako bi se ublažio učinak značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera, podržao hitan oporavak ili ponovno uspostavilo funkcioniranje ključnih usluga. Prema potrebi, njime bi se trebao dopuniti Mehanizam Unije za civilnu zaštitu kako bi se osigurao sveobuhvatan odgovor na učinke kiberincidenata na građane.

(32) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se podupirati pomoć koju države članice pružaju državi članici pogođenoj značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera, među ostalim u okviru mreže CSIRT-ova utvrđene u članku 15. Direktive (EU) 2022/2555. Državama članicama koje pružaju pomoć trebalo bi dopustiti podnošenje zahtjeva za pokrivanje troškova povezanih sa slanjem timova stručnjaka u okviru pružanja uzajamne pomoći. Prihvatljivi troškovi mogli bi uključivati putne troškove, troškove smještaja i dnevnice stručnjaka za kibersigurnost.

---

[17] Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011.

(33) Na razini Unije trebalo bi postupno uspostaviti kibersigurnosnu pričuvu koja bi se sastojala od usluga privatnih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i hitne mjere oporavka u slučajevima značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera. Kibersigurnosna pričuva EU-a trebala bi osigurati dostupnost i spremnost usluga. Usluge iz kibersigurnosne pričuve EU-a trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima koji djeluju u kritičnim ili visokokritičnim sektorima te nadopunjavati njihovo djelovanje na nacionalnoj razini. Pri podnošenju zahtjeva za potporu iz kibersigurnosne pričuve EU-a države članice trebale bi navesti vrstu potpore pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni zahtjeva države članice. Usluge iz kibersigurnosne pričuve EU-a mogu služiti i za potporu institucijama, tijelima i agencijama Unije pod sličnim uvjetima.

(34) U svrhu odabira privatnih pružatelja usluga koji će pružati usluge u kontekstu kibersigurnosne pričuve EU-a potrebno je utvrditi skup minimalnih kriterija koje bi trebalo uključiti u poziv na podnošenje ponuda za odabir tih pružatelja, kako bi se ispunile potrebe tijela i subjekata država članica koji djeluju u kritičnim ili visokokritičnim sektorima.

(35) Kako bi pridonijela uspostavi kibersigurnosne pričuve EU-a, Komisija bi mogla razmotriti mogućnost da od ENISA-e zatraži izradu prijedloga programa certifikacije u skladu s Uredbom (EU) 2019/881 za upravljane sigurnosne usluge u područjima obuhvaćenima mehanizmom za izvanredne kibersigurnosne situacije.

(36) Kako bi se poduprli ciljevi ove Uredbe koji se odnose na promicanje zajedničke informiranosti o stanju, jačanje otpornosti Unije i omogućivanje djelotvornog odgovora na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, mreža EU-CyCLONe, mreža CSIRT-ova ili Komisija trebali bi moći zatražiti od ENISA-e da istraži i procijeni prijetnje, ranjivosti i mjere ublažavanja povezane s određenim značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera. Nakon dovršetka istraživanja i procjene incidenta ENISA bi trebala pripremiti izvješće o istraživanju incidenta u suradnji s relevantnim dionicima, uključujući predstavnike iz privatnog sektora, države članice, Komisiju i druge relevantne institucije, tijela i agencije EU-a. Kad je riječ o privatnom sektoru, ENISA razvija kanale za razmjenu informacija sa specijaliziranim pružateljima usluga, uključujući pružatelje upravljanih sigurnosnih rješenja i dobavljače, kako bi ostvarila svoju misiju postizanja visoke zajedničke razine kibersigurnosti u Uniji. Na temelju suradnje s dionicima, uključujući privatni sektor, izvješće o istraživanju određenih incidenata trebalo bi biti usmjereno na procjenu uzroka, učinaka i mjera ublažavanja posljedica incidenta nakon što se on dogodio. Posebnu pozornost trebalo bi posvetiti informacijama i iskustvima koje dijele pružatelji upravljanih sigurnosnih usluga koji ispunjavaju uvjete najvišeg profesionalnog integriteta, nepristranosti i potrebnog tehničkog stručnog znanja u skladu s ovom Uredbom. Izvješće bi trebalo dostaviti i mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji te bi ga oni trebali uzeti u obzir u svom radu. Ako se incident odnosi na treću zemlju, Komisija bi izvješće trebala poslati Visokom predstavniku.

(37) S obzirom na nepredvidivu prirodu kibernapada i činjenicu da ti napadi često nisu ograničeni na određeno zemljopisno područje te da postoji visok rizik od prelijevanja, jačanje otpornosti susjednih zemalja i njihove sposobnosti da učinkovito odgovore na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera doprinosi zaštiti Unije u cjelini. Stoga treće zemlje pridružene programu Digitalna

Europa mogu primiti potporu iz kibersigurnosne pričuve EU-a, ako je to predviđeno odgovarajućim sporazumom o pridruživanju programu Digitalna Europa. Unija bi trebala podupirati financiranje pridruženih trećih zemalja u okviru relevantnih partnerstava i instrumenata financiranja za te zemlje. Potpora bi trebala obuhvaćati usluge za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera te hitnog oporavka od njih. Uvjeti za kibersigurnosnu pričuvu EU-a i pouzdane pružatelje usluga utvrđeni u ovoj Uredbi trebali bi se primjenjivati pri pružanju potpore trećim zemljama pridruženima programu Digitalna Europa.

(38) Radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe, Komisiji bi trebalo dodijeliti provedbene ovlasti za određivanje uvjeta za interoperabilnost prekograničnih SOC-ova; za određivanje postupovnih aranžmana za dijeljenje informacija između prekograničnih SOC-ova i subjekata Unije koje su povezane s potencijalnim ili aktualnim kibersigurnosnim incidentima velikih razmjera; za utvrđivanje tehničkih zahtjeva za osiguravanje sigurnosti europskog kiberštita; za određivanje vrste i broja usluga odgovora potrebnih za kibersigurnosnu pričuvu EU-a; i za dodatno utvrđivanje detaljnih aranžmana za dodjelu usluga potpore iz kibersigurnosne pričuve EU-a. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća.

(39) Cilj ove Uredbe može se bolje ostvariti na razini Unije nego na razini država članica. Stoga Unija može donijeti mjere u skladu s načelima supsidijarnosti i proporcionalnosti utvrđenima u članku 5. Ugovora o Europskoj uniji. Ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

DONIJELI SU OVU UREDBU:

Poglavlje I.

OPĆI CILJEVI, PREDMET I DEFINICIJE

Članak 1.

Predmet i ciljevi

1. Ovom se Uredbom utvrđuju mjere za jačanje kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih, prije svega sljedećim djelovanjima:

(a) uvođenjem paneuropske infrastrukture centara za sigurnosne operacije („europski kiberštit”) radi razvoja i poboljšanja zajedničkih sposobnosti za otkrivanje i informiranost o stanju;

(b) uspostavom mehanizma za izvanredne kibersigurnosne situacije kako bi se državama članicama pružila potpora u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih;

(c) uspostavom europskog mehanizma za istraživanje kibersigurnosnih incidenata radi istraživanja i procjenjivanja značajnih incidenata ili incidenata velikih razmjera.

2. Cilj je ove Uredbe ojačati solidarnost na razini Unije ostvarivanjem sljedećih specifičnih ciljeva:

(a) poboljšanje zajedničkog otkrivanja kiberprijetnji i kiberincidenata te zajedničke informiranosti o njihovu stanju u Uniji da bi se omogućilo učvršćivanje konkurentnog položaja industrijskog i uslužnog sektora u Uniji u cijelom digitalnom gospodarstvu te doprinijelo tehnološkom suverenitetu Unije u području kibersigurnosti;

(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa („DEP”);

(c) povećanje otpornosti Unije i djelotvornosti odgovora istraživanjem i procjenjivanjem značajnih incidenata ili incidenata velikih razmjera, među ostalim učenjem iz iskustva i, prema potrebi, davanjem preporuka.

3. Ovom se Uredbom ne dovodi u pitanje primarna odgovornost država članica za nacionalnu sigurnost, javnu sigurnost te sprečavanje, istragu, otkrivanje i progon kaznenih djela.

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. **„prekogranični centar za sigurnosne operacije” ili „prekogranični SOC”** znači višedržavna platforma na kojoj su, u koordiniranoj mrežnoj strukturi, okupljeni nacionalni SOC-ovi iz najmanje triju država članica koji čine konzorcij domaćin i koja je namijenjena za sprečavanje kiberprijetnji i kiberincidenata, pružanje potpore u pripremi visokokvalitetnih relevantnih informacija, ponajprije razmjenom podataka iz raznih izvora, javnih i privatnih, te pružanjem najsuvremenijih alata i zajedničkim razvojem kibersigurnosnih sposobnosti otkrivanja, analize, prevencije i zaštite u pouzdanom okruženju;

2. **„javnopravno tijelo”** znači javnopravno tijelo kako je definirano u članku 2. stavku 1. točki 4. Direktive 2014/24/EU Europskog parlamenta i Vijeća[18];

3. **„konzorcij domaćin”** znači konzorcij sastavljen od država sudionica, koje predstavljaju nacionalni SOC-ovi, koje su se sporazumjele pokrenuti nabavu alata i infrastrukture za prekogranični SOC i njegov rad te joj doprinositi;

4. **„subjekt”** znači subjekt kako je definiran u članku 6. točki 38. Direktive (EU) 2022/2555;

[18] Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

5. **„subjekti koji djeluju u kritičnim ili visokokritičnim sektorima”** znači subjekti vrsta navedenih u prilozima I. i II. Direktivi (EU) 2022/2555;

6. **„kiberprijetnja”** znači kiberprijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;

7. **„značajan kibersigurnosni incident”** znači kiberincident koji ispunjava kriterije utvrđene u članku 23. stavku 3. Direktive (EU) 2022/2555;

8. **„kibersigurnosni incident velikih razmjera”** znači incident kako je definiran u članku 6. točki 7. Direktive (EU) 2022/2555;

9. **„pripravnost”** znači stanje spremnosti i sposobnost da se osigura učinkovit i brz odgovor na značajan kibersigurnosni incident ili kibersigurnosni incident velikih razmjera ostvareno kao rezultat unaprijed poduzetih aktivnosti procjenjivanja i praćenja rizika;

10. **„odgovor”** znači postupanje u slučaju značajnog kibersigurnosnog incidenta ili kibersigurnosnog incidenta velikih razmjera, ili tijekom ili nakon takvog incidenta, radi saniranja njegovih neposrednih i kratkoročnih štetnih posljedica;

11. **„pouzdani pružatelji”** znači pružatelji upravljanih sigurnosnih usluga kako su definirani u članku 6. točki 40. Direktive (EU) 2022/2555 i odabrani u skladu s člankom 16. ove Uredbe.

Poglavlje II.

EUROPSKI KIBERŠTIT

Članak 3.

Uspostava europskog kiberštita

1. Uspostavlja se međusobno povezana paneuropska infrastruktura centara za sigurnosne operacije („europski kiberštit”) radi razvoja naprednih sposobnosti Unije za otkrivanje, analizu i obradu podataka o kiberprijetnjama i kiberincidentima u Uniji. Sastoji se od svih nacionalnih centara za sigurnosne operacije („nacionalni SOC-ovi”) i prekograničnih centara za sigurnosne operacije („prekogranični SOC-ovi”).

Djelovanja radi implementacije europskog kiberštita podupiru se sredstvima iz programa Digitalna Europa i provode u skladu s Uredbom (EU) 2021/694, osobito njezinim specifičnim ciljem 3.

2. Europski kiberštit:

(a) objedinjuje i dijeli podatke o kiberprijetnjama i kiberincidentima iz raznih izvora putem prekograničnih SOC-ova;

(b) priprema visokokvalitetne i upotrebljive informacije te relevantne podatke o kiberprijetnjama upotrebom najsuvremenijih alata, osobito tehnologija umjetne inteligencije i analitike podataka;

(c) doprinosi boljoj zaštiti i odgovoru na kiberprijetnje;

(d) doprinosi bržem otkrivanju kiberprijetnji i informiranosti o stanju u cijeloj Uniji;

(e) pruža usluge i provodi aktivnosti zajednici za kibersigurnost u Uniji, što uključuje doprinos razvoju naprednih alata koji se temelje na umjetnoj inteligenciji i naprednih alata za analitiku podataka.

Razvija se u suradnji s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom na temelju Uredbe (EU) 2021/1173.

Članak 4.

Nacionalni centri za sigurnosne operacije

1. Kako bi sudjelovala u europskom kiberštitu, svaka država članica imenuje barem jedan nacionalni SOC. Nacionalni SOC mora biti javnopravno tijelo.

Mora moći služiti drugim javnim i privatnim organizacijama na nacionalnoj razini kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. Mora biti opremljen najsuvremenijim tehnologijama za otkrivanje, agregiranje i analiziranje podataka relevantnih za kibersigurnosne prijetnje i incidente.

2. Nakon poziva na iskaz interesa Europski stručni centar u području kibersigurnosti („ECCC”) odabire nacionalne SOC-ove za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može odabranim nacionalnim SOC-ovima dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski doprinos Unije pokriva do 50 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva država članica. Prije pokretanja postupka nabave alata i infrastrukture ECCC i nacionalni SOC sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.

3. Nacionalni SOC odabran u skladu sa stavkom 2. obvezuje se podnijeti zahtjev za sudjelovanje u prekograničnom SOC-u u roku od dvije godine od datuma nabave alata i infrastrukture ili datuma na koji primi bespovratna sredstva, ovisno o tome što nastupi prije. Ako nacionalni SOC do tog roka nije postao sudionik prekograničnog SOC-a, nema pravo na dodatnu potporu Unije na temelju ove Uredbe.

Članak 5.

Prekogranični centri za sigurnosne operacije

1. Konzorcij domaćin koji čine najmanje tri države članice, koje predstavljaju nacionalni SOC-ovi, koje su se obvezale međusobno surađivati radi koordinacije svojih aktivnosti otkrivanja i praćenja kiberprijetnji ima pravo sudjelovati u aktivnostima za uspostavu prekograničnog SOC-a.

2. Nakon poziva na iskaz interesa ECCC odabire konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski

doprinos Unije pokriva do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva konzorcij domaćin. Prije pokretanja postupka nabave alata i infrastrukture ECCC i konzorcij domaćin sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.

3. Članovi konzorcija domaćina sklapaju pisani ugovor o konzorciju u kojem se utvrđuju njihovi interni aranžmani za provedbu ugovora o korištenju i upotrebi.

4. Prekogranični SOC za pravne potrebe zastupa nacionalni SOC koji djeluje kao koordinacijski SOC ili, ako ima pravnu osobnost, konzorcij domaćin. Koordinacijski SOC odgovoran je za usklađenost sa zahtjevima iz ugovora o smještaju i korištenju te iz ove Uredbe.

Članak 6.

Suradnja i dijeljenje informacija unutar prekograničnih SOC-ova i među njima

1. Članovi konzorcija domaćina unutar prekograničnog SOC-a međusobno razmjenjuju relevantne informacije kao što su informacije o kiberprijetnjama, izbjegnutim incidentima, ranjivostima, tehnikama i postupcima, pokazateljima ugroženosti, neprijateljskim taktikama i počiniteljima prijetnji, kibersigurnosna upozorenja te preporuke za konfiguriranje kibersigurnosnih alata za otkrivanje kibernapada ako takva razmjena informacija:

(a) ima za cilj sprečavanje ili otkrivanje incidenata, odgovaranje na njih, oporavljanje od incidenata ili ublažavanje njihova učinka;

(b) povećava razinu kibersigurnosti, posebno povećanjem informiranosti o kiberprijetnjama, ograničavanjem ili ometanjem mogućnosti širenja takvih prijetnji, podupiranjem niza obrambenih sposobnosti, otklanjanjem i otkrivanjem ranjivosti, tehnikama otkrivanja, zaustavljanja i sprečavanja prijetnji, strategijama ublažavanja ili fazama odgovora i oporavka ili promicanjem suradnje na istraživanju prijetnji između javnih i privatnih subjekata.

2. Pisanim ugovorom o konzorciju iz članka 5. stavka 3. utvrđuju se:

(a) obveza dijeljenja znatne količine podataka iz stavka 1. i uvjeti pod kojima se te informacije trebaju razmjenjivati;

(b) upravljački okvir kojim se svi sudionici potiču da dijele informacije;

(c) ciljevi doprinosa razvoju naprednih alata koji se temelje na umjetnoj inteligenciji i naprednih alata za analitiku podataka.

3. Kako bi potaknuli međusobnu razmjenu informacija, prekogranični SOC-ovi osiguravaju visoku razinu međusobne interoperabilnosti. Kako bi olakšala interoperabilnost prekograničnih SOC-ova, Komisija može, nakon savjetovanja s ECCC-om, provedbenim aktima odrediti uvjete te interoperabilnosti. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2. ove Uredbe.

4. Prekogranični SOC-ovi međusobno sklapaju sporazume o suradnji u kojima se utvrđuju načela razmjene informacija među prekograničnim platformama.

Članak 7.

Suradnja i dijeljenje informacija sa subjektima Unije

1. Ako prekogranični SOC-ovi dobiju informacije o potencijalnom ili aktualnom kibersigurnosnom incidentu velikih razmjera, oni bez nepotrebne odgode dostavljaju relevantne informacije mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji prema njihovim ulogama u upravljanju krizama u skladu s Direktivom (EU) 2022/2555.

2. Komisija može provedbenim aktima utvrditi postupovne aranžmane za dijeljenje informacija iz stavka 1. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2. ove Uredbe.

Članak 8.

Sigurnost

1. Države članice koje sudjeluju u europskom kiberštitu osiguravaju visoku razinu sigurnosti podataka i fizičke sigurnosti infrastrukture europskog kiberštita te primjereno upravljanje i kontrolu nad tom infrastrukturom kako bi je se zaštitilo od prijetnji i kako bi bila zajamčena njezina sigurnost i sigurnost sustava, uključujući podatke koji se razmjenjuju s pomoću te infrastrukture.

2. Države članice koje sudjeluju u europskom kiberštitu osiguravaju da dijeljenje informacija u okviru europskog kiberštita sa subjektima koji nisu javna tijela države članice ne šteti sigurnosnim interesima Unije.

3. Komisija može donijeti provedbene akte kojima se utvrđuju tehnički zahtjevi za ispunjavanje obveze država članica propisane u stavcima 1. i 2. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2. ove Uredbe. Kako bi se olakšala suradnja s vojnim akterima, Komisija pritom, uz podršku Visokog predstavnika, uzima u obzir relevantne obrambene sigurnosne standarde.

Poglavlje III.

MEHANIZAM ZA IZVANREDNE KIBERSIGURNOSNE SITUACIJE

Članak 9.

Uspostava mehanizma za izvanredne kibersigurnosne situacije

1. Uspostavlja se mehanizam za izvanredne kibersigurnosne situacije radi povećanja otpornosti Unije na velike kibersigurnosne prijetnje te radi pripreme za kratkoročne posljedice značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera i njegovo ublažavanje u duhu solidarnosti („mehanizam”).

2. Djelovanja radi primjene mehanizma za izvanredne kibersigurnosne situacije podupiru se sredstvima iz programa Digitalna Europa i provode u skladu s Uredbom (EU) 2021/694, osobito njezinim specifičnim ciljem 3.

Članak 10.

Vrste mjera

1. Mehanizmom se podupiru sljedeće vrste mjera:

(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim sektorima u Uniji;

(b) mjere odgovora, kojima se doprinosi odgovoru na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i hitnom oporavku od njih, koje trebaju poduzeti pouzdani pružatelji koji sudjeluju u kibersigurnosnoj pričuvi EU-a uspostavljenoj člankom 12.;

(c) mjere uzajamne pomoći koje se sastoje od pomoći nacionalnih tijela jedne države članice drugoj državi članici, osobito kako je utvrđeno u članku 11. stavku 3. točki (f) Direktive (EU) 2022/2555.

Članak 11.

Koordinirano testiranje pripravnosti subjekata

1. Za potrebe podupiranja koordiniranog testiranja pripravnosti subjekata iz članka 10. stavka 1. točke (a) u cijeloj Uniji Komisija, nakon savjetovanja sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava i ENISA-om, među sektorima visokog stupnja kritičnosti navedenima u Prilogu I. Direktivi (EU) 2022/2555 utvrđuje relevantne sektore ili podsektore iz kojih se subjekti mogu podvrgavati koordiniranom testiranju pripravnosti, uzimajući u obzir postojeće i planirane koordinirane procjene rizika i testiranja otpornosti na razini Unije.

2. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava izrađuje, u suradnji s Komisijom, ENISA-om i Visokim predstavnikom, zajedničke scenarije rizika i metodologije za koordinirana testiranja.

Članak 12.

Uspostava kibersigurnosne pričuve EU-a

1. Uspostavlja se kibersigurnosna pričuva EU-a radi pomaganja korisnicima iz stavka 3. pri odgovaranju ili pružanju potpore za odgovaranje na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i hitan oporavak od takvih incidenata.

2. Kibersigurnosnu pričuvu EU-a čine usluge odgovora na incidente koje pružaju pouzdani pružatelji odabrani u skladu s kriterijima iz članka 16. Pričuva obuhvaća unaprijed dogovorene usluge. Pružanje tih usluga mora biti moguće u svim državama članicama.

3. Korisnici usluga iz kibersigurnosne pričuve EU-a uključuju:

(a) tijela za upravljanje kiberkrizama i CSIRT-ove iz država članica navedene u članku 9. stavcima 1. i 2. odnosno članku 10. Direktive (EU) 2022/2555;

(b) institucije, tijela i agencije Unije.

4. Korisnici iz stavka 3. točke (a) usluge iz kibersigurnosne pričuve EU-a koriste za odgovor ili potporu odgovoru na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera koji utječu na subjekte koji djeluju u kritičnim ili visokokritičnim sektorima te za hitan oporavak od njih.

5. Komisija je općenito odgovorna za primjenu kibersigurnosne pričuve EU-a. Komisija određuje prioritete i razvoj kibersigurnosne pričuve EU-a u skladu sa zahtjevima korisnika iz stavka 3. i nadzire njezinu primjenu te se brine za komplementarnost, dosljednost, sinergije i veze s drugim mjerama potpore na temelju ove Uredbe, kao i s drugim mjerama i programima Unije.

6. Komisija može sporazumima o doprinosu rad i vođenje kibersigurnosne pričuve EU-a u cijelosti ili djelomično povjeriti ENISA-i.

7. Kako bi pomogla Komisiji u uspostavi kibersigurnosne pričuve EU-a, ENISA, nakon savjetovanja s državama članicama i Komisijom, izrađuje pregled potrebnih usluga. ENISA, nakon savjetovanja s Komisijom, sličan pregled izrađuje i kako bi utvrdila potrebe trećih zemalja koje ispunjavaju uvjete za potporu iz kibersigurnosne pričuve EU-a na temelju članka 17. Komisija se prema potrebi savjetuje s Visokim predstavnikom.

8. Komisija može provedbenim aktima utvrditi vrste i broj usluga odgovora potrebnih za kibersigurnosnu pričuvu EU-a. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2.

Članak 13.

Zahtjevi za potporu iz kibersigurnosne pričuve EU-a

1. Korisnici iz članka 12. stavka 3. mogu zatražiti usluge iz kibersigurnosne pričuve EU-a radi potpore odgovoru na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i hitnom oporavku od njih.

2. Da bi primili potporu iz kibersigurnosne pričuve EU-a, korisnici iz članka 12. stavka 3. dužni su poduzeti mjere za ublažavanje učinaka incidenta za koji se traži potpora, uključujući pružanje izravne tehničke pomoći i drugih resursa za pomoć u odgovoru na incident, te korake za hitan oporavak.

3. Zahtjevi za potporu koje podnesu korisnici iz članka 12. stavka 3. točke (a) ove Uredbe dostavljaju se Komisiji i ENISA-i putem jedinstvene kontaktne točke koju je država članica imenovala ili uspostavila u skladu s člankom 8. stavkom 3. Direktive (EU) 2022/2555.

4. Države članice obavješćuju mrežu CSIRT-ova i, prema potrebi, EU-CyCLONe o zahtjevima za potporu odgovoru na incident i hitnom oporavku od njega koje su podnijele na temelju ovog članka.

5. Zahtjevi za potporu odgovoru na incident i hitnom oporavku od njega moraju sadržavati:

(a) odgovarajuće informacije o pogođenom subjektu i mogućim učincima incidenta i planiranoj upotrebi zatražene potpore, uključujući podatke o procijenjenim potrebama;

(b) informacije o mjerama iz stavka 2. poduzetima za ublažavanje incidenta za koje se traži potpora;

(c) informacije o drugim oblicima potpore koji su dostupni pogođenom subjektu, uključujući ugovorne aranžmane za usluge odgovora na incident i hitnog oporavka od njega, te o ugovorima o osiguranju koji potencijalno pokrivaju takvu vrstu incidenta.

6. Kako bi se olakšalo podnošenje zahtjeva za potporu iz kibersigurnosne pričuve EU-a, ENISA je dužna, u suradnji s Komisijom i Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava, izraditi predložak.

7. Komisija može provedbenim aktima pobliže utvrditi detaljne aranžmane za dodjelu usluga potpore iz kibersigurnosne pričuve EU-a. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2.

Članak 14.

Ostvarivanje potpore iz kibersigurnosne pričuve EU-a

1. Zahtjeve za potporu iz kibersigurnosne pričuve EU-a ocjenjuje Komisija uz potporu ENISA-e ili kako je definirano u sporazumima o doprinosu na temelju članka 12. stavka 6., a odgovor na zahtjev se bez odgode šalje korisnicima iz članka 12. stavka 3.

2. U slučaju više istodobnih zahtjeva prednost zahtjeva određuje se, prema potrebi, na temelju sljedećih kriterija:

(a) ozbiljnost kibersigurnosnog incidenta;

(b) vrsta pogođenog subjekta, pri čemu se veća prednost daje incidentima koji utječu na ključne subjekte kako su definirani u članku 3. stavku 1. Direktive (EU) 2022/2555;

(c) mogući učinak na pogođene države članice ili korisnike;

(d) moguća prekogranična priroda incidenta i opasnost od širenja na druge države članice ili korisnike;

(e) mjere koje je korisnik poduzeo da pomogne u odgovoru i poduzeti koraci za hitni oporavak iz članka 13. stavka 2. i članka 13. stavka 5. točke (b).

3. Usluge kibersigurnosne pričuve EU-a pružaju se u skladu s posebnim sporazumima između pružatelja usluga i korisnika kojem se pruža potpora iz kibersigurnosne pričuve EU-a. Ti sporazumi moraju sadržavati uvjete o odgovornosti.

4. Sporazumi iz stavka 3. mogu se temeljiti na predlošcima koje izradi ENISA nakon savjetovanja s državama članicama.

5. Komisija i ENISA ne snose ugovornu odgovornost za štetu koju trećim stranama prouzroče usluge pružene u okviru primjene kibersigurnosne pričuve EU-a.

6. U roku od mjesec dana od završetka mjere potpore korisnici Komisiji i ENISA-i dostavljaju sažeto izvješće o pruženoj usluzi, ostvarenim rezultatima i stečenim iskustvima. Ako je korisnik iz treće zemlje kako je utvrđeno u članku 17., to se izvješće dijeli s Visokim predstavnikom.

7. Komisija o korištenju i rezultatima potpore izvješćuje Skupinu za suradnju u području sigurnosti mrežnih i informacijskih sustava.

Članak 15.

Koordinacija s mehanizmima za upravljanje krizama

1. Kad su značajni kibersigurnosni incidenti ili kibersigurnosni incidenti velikih razmjera posljedica ili uzrok katastrofa kako su definirane u Odluci 1313/2013/EU[19], potporom odgovoru na takve incidente na temelju ove Uredbe dopunjuju se djelovanja na temelju Odluke 1313/2013/EU ne dovodeći je u pitanje.

2. U slučaju prekograničnih kibersigurnosnih incidenata velikih razmjera zbog kojih se aktiviraju aranžmani za integrirani politički odgovor na krizu (IPCR), s potporom odgovoru na takve incidente na temelju ove Uredbe postupa se u skladu s relevantnim protokolima i postupcima u okviru IPCR-a.

3. Uz savjetovanje s Visokim predstavnikom, potpora u okviru mehanizma za izvanredne kibersigurnosne situacije može biti dopuna pomoći koja se pruža u kontekstu zajedničke vanjske i sigurnosne politike te zajedničke sigurnosne i obrambene politike, među ostalim putem timova za brz odgovor na kiberincidente. Također može biti dopuna ili doprinos pomoći koju jedna država članica pruža drugoj državi članici u kontekstu članka 42. stavka 7. Ugovora o Europskoj uniji.

4. Potpora iz mehanizma za izvanredne kibersigurnosne situacije može biti dio zajedničkog odgovora Unije i država članica u situacijama iz članka 222. Ugovora o funkcioniranju Europske unije.

Članak 16.

Pouzdani pružatelji

1. U postupcima nabave za potrebe uspostave kibersigurnosne pričuve EU-a javni naručitelj pridržava se načela utvrđenih u Uredbi (EU, Euratom) 2018/1046 i sljedećih načela:

(a) vodi računa da kibersigurnosna pričuva EU-a obuhvaća usluge koje se mogu pružati u svim državama članicama, uzimajući osobito u obzir nacionalne zahtjeve za pružanje takvih usluga, među ostalim u pogledu certifikacije ili akreditacije;

(b) vodi računa da su ključni sigurnosni interesi Unije i njezinih država članica zaštićeni;

(c) vodi računa da kibersigurnosna pričuva EU-a donosi dodanu vrijednost EU-a tako što doprinosi ciljevima iz članka 3. Uredbe (EU) 2021/694, među ostalim poticanju razvoja vještina u području kibersigurnosti u EU-u.

2. Pri nabavi usluga za kibersigurnosnu pričuvu EU-a javni naručitelj u dokumentaciju o nabavi uključuje sljedeće kriterije za odabir:

(a) pružatelj mora dokazati da njegovo osoblje ima najviši stupanj profesionalnog integriteta, neovisnosti, odgovornosti i potrebne tehničke stručnosti za obavljanje aktivnosti u svojem području te osigurava trajnost/kontinuitet stručnosti i potrebne tehničke resurse;

[19] Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu (SL L 347, 20.12.2013., str. 924.).

(b) pružatelj, njegova društva kćeri i podugovaratelji moraju imati uspostavljen okvir za zaštitu osjetljivih informacija koje se odnose na uslugu, posebice dokaza, nalaza i izvješća, te biti usklađeni sa sigurnosnim pravilima Unije o zaštiti klasificiranih podataka EU-a;

(c) pružatelj mora dati dostatan dokaz da je njegova upravljačka struktura transparentna i da vjerojatno neće ugroziti njegovu nepristranost i kvalitetu njegovih usluga ili prouzročiti sukob interesa;

(d) pružatelj mora imati odgovarajuće uvjerenje o sigurnosnoj provjeri, barem za osoblje koje će pružati usluge;

(e) sigurnost pružateljevih IT sustava mora biti na odgovarajućoj razini;

(f) pružatelj mora biti opremljen hardverskom i softverskom tehničkom opremom koja omogućuje traženu uslugu;

(g) pružatelj mora moći dokazati da ima iskustvo u pružanju sličnih usluga relevantnim nacionalnim tijelima ili subjektima koji djeluju u kritičnim ili visokokritičnim sektorima;

(h) u državama članicama u kojima može pružati uslugu pružatelj je mora moći pružiti u kratkom roku;

(i) u državama članicama u kojima može pružati uslugu pružatelj je mora moći pružiti na lokalnom jeziku države članice;

(j) nakon što se uspostavi program certifikacije EU-a za upravljane sigurnosne usluge na temelju Uredbe (EU) 2019/881 pružatelj mora biti certificiran u skladu s tim programom.

Članak 17.

Potpora trećim zemljama

1. Treće zemlje mogu zatražiti potporu iz kibersigurnosne pričuve EU-a ako je tako uređeno sporazumima o pridruživanju sklopljenima u pogledu njihova sudjelovanja u programu Digitalna Europa.

2. Potpora iz kibersigurnosne pričuve EU-a mora biti u skladu s ovom Uredbom i svim posebnim uvjetima utvrđenima u sporazumima o pridruživanju iz stavka 1.

3. Korisnici iz pridruženih trećih zemalja koji su prihvatljivi za primanje usluga iz kibersigurnosne pričuve EU-a uključuju nadležna tijela kao što su CSIRT-ovi i tijela za upravljanje kiberkrizama.

4. Svaka treća zemlja koja ispunjava uvjete za potporu iz kibersigurnosne pričuve EU-a imenuje tijelo koje će biti jedinstvena kontaktna točka za potrebe ove Uredbe.

5. Prije nego što prime bilo kakvu potporu iz kibersigurnosne pričuve EU-a, treće zemlje Komisiji i Visokom predstavniku dostavljaju informacije o svojoj kiberotpornosti i kapacitetima za upravljanje rizicima, uključujući barem informacije o poduzetim nacionalnim mjerama pripreme za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera te informacije o odgovornim nacionalnim subjektima, uključujući CSIRT-ove ili ekvivalentne subjekte, njihovim sposobnostima i resursima koji su im dodijeljeni. Odredbe iz

članaka 13. i 14. ove Uredbe koje se odnose na države članice primjenjuju se na treće zemlje iz stavka 1.

6. Komisija surađuje s Visokim predstavnikom u vezi sa zaprimljenim zahtjevima i primjenom potpore koja je trećim zemljama dodijeljena iz kibersigurnosne pričuve EU-a.

Poglavlje IV.

MEHANIZAM ZA ISTRAŽIVANJE KIBERSIGURNOSNIH INCIDENATA

Članak 18.

Mehanizam za istraživanje kibersigurnosnih incidenata

1. Na zahtjev Komisije, mreže EU-CyCLONe ili mreže CSIRT-ova ENISA istražuje i procjenjuje prijetnje, ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibersigurnosni incident ili kibersigurnosni incident velikih razmjera. Nakon završetka istraživanja i procjenjivanja incidenta ENISA mreži CSIRT-ova, mreži EU-CyCLONe i Komisiji dostavlja izvješće o istraživanju incidenta kako bi im pomogla u obavljanju njihovih zadaća, osobito u pogledu onih utvrđenih u člancima 15. i 16. Direktive (EU) 2022/2555. Komisija prema potrebi izvješće šalje Visokom predstavniku.

2. ENISA u pripremi izvješća o istraživanju incidenta iz stavka 1. surađuje sa svim relevantnim dionicima, uključujući predstavnike država članica, Komisije, drugih relevantnih institucija, tijela i agencija EU-a, pružatelja upravljanih sigurnosnih usluga i korisnika usluga kibersigurnosti. ENISA prema potrebi surađuje i sa subjektima pogođenima značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera. Kao pomoć u istraživanju, ENISA se može savjetovati i s drugim vrstama dionika. Konzultirani predstavnici dužni su dati informacije o svakom mogućem sukobu interesa.

3. Izvješće obuhvaća istraživanje i analizu konkretnog značajnog kibersigurnosnog incidenta ili kiberincidenta velikih razmjera, uključujući glavne uzroke, ranjivosti i stečena iskustva. Povjerljive informacije u izvješću štite se u skladu s pravom Unije ili nacionalnim pravom o zaštiti osjetljivih ili klasificiranih podataka.

4. U izvješću se, prema potrebi, daju preporuke za poboljšanje kibersigurnosnog položaja Unije.

5. Kad je to moguće, jedna verzija izvješća mora biti javno dostupna. Ta verzija sadržava samo javne informacije.

Poglavlje V.

ZAVRŠNE ODREDBE

Članak 19.

Izmjene Uredbe (EU) 2021/694

Uredba (EU) 2021/694 mijenja se kako slijedi:

1. članak 6. mijenja se kako slijedi:

(a) stavak 1. mijenja se kako slijedi:

1. umeće se sljedeća točka (aa):

„(aa) pružanje potpore razvoju kiberštita EU-a, što uključuje razvoj, uvođenje i rad nacionalnih i prekograničnih platformi centara za sigurnosne operacije koje doprinose informiranosti o stanju u Uniji i jačanju kapaciteta Unije za prikupljanje podataka o kiberprijetnjama”;

2. dodaje se sljedeća točka (g):

„(g) uspostava i rad mehanizma za izvanredne kibersigurnosne situacije radi pružanja potpore državama članicama u pripremi za značajne kibersigurnosne incidente i odgovaranju na njih kao dopune nacionalnim resursima i kapacitetima te drugim oblicima potpore dostupnima na razini Unije, uključujući uspostavu kibersigurnosne pričuve EU-a”;

(a) stavak 2. zamjenjuje se sljedećim:

„2. Djelovanja u okviru specifičnog cilja 3 provode se ponajprije putem Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti te mreže nacionalnih koordinacijskih centara u skladu s Uredbom (EU) 2021/887 Europskog parlamenta i Vijeća[20], uz iznimku djelovanja radi primjene kibersigurnosne pričuve EU-a, koja provode Komisija i ENISA.”;

2. članak 9. mijenja se kako slijedi:

(a) u stavku 2. točke (b), (c) i (d) zamjenjuju se sljedećim:

„(b) 1 776 956 000 EUR za specifični cilj 2 – umjetna inteligencija;

(c) 1 629 566 000 EUR za specifični cilj 3 – kibersigurnost i povjerenje;

(d) 482 347 000 EUR za specifični cilj 4 – napredne digitalne vještine”;

(b) dodaje se sljedeći stavak 8.:

„8. Odstupajući od članka 12. stavka 4. Uredbe (EU, Euratom) 2018/1046, neiskorištena odobrena sredstva za preuzimanje obveza i za plaćanje za djelovanja kojima se nastoje ostvariti ciljevi utvrđeni u članku 6. stavku 1. točki (g) ove Uredbe automatski se prenose

[20] Uredba (EU) 2021/887 Europskog parlamenta i Vijeća od 20. svibnja 2021. o osnivanju Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti i mreže nacionalnih koordinacijskih centara (SL L 202, 8.6.2021., str. 1.–31.).

te se za njih mogu preuzeti obveze i mogu se isplatiti do 31. prosinca sljedeće financijske godine.”;

3. u članku 14. stavak 2. zamjenjuje se sljedećim:

„2. Programom se može predvidjeti financiranje u bilo kojem od oblika utvrđenih u Financijskoj uredbi, uključujući posebno putem nabave kao primarnog oblika ili bespovratnih sredstava i nagrada.

Ako je za ostvarenje cilja djelovanja potrebna nabava inovativne robe i usluga, bespovratna sredstva mogu se dodijeliti samo korisnicima koji su javni naručitelji ili naručitelji kako su definirani u direktivama 2014/24/EU[27] i 2014/25/EU[28] Europskog parlamenta i Vijeća.

Ako je za ostvarenje ciljeva djelovanja potrebna isporuka inovativne robe ili usluga koje još nisu šire komercijalno dostupne, javni naručitelj ili naručitelj može odobriti dodjelu više ugovora u okviru istog postupka nabave.

Zbog propisno opravdanih razloga javne sigurnosti javni naručitelj ili naručitelj može zahtijevati da se mjesto izvršenja ugovora nalazi na području Unije.

Pri provedbi postupaka nabave za kibersigurnosnu pričuvu EU-a uspostavljenu člankom 12. Uredbe (EU) 2023/XX Komisija i ENISA mogu djelovati kao središnje tijelo za nabavu u ime ili za račun trećih zemalja pridruženih Programu u skladu s člankom 10. Komisija i ENISA mogu djelovati i kao trgovac na veliko kupnjom, skladištenjem i preprodajom ili doniranjem robe i usluga, uključujući najam, tim trećim zemljama. Odstupajući od članka 169. stavka 3. Uredbe (EU) XXX/XXXX [preinaka Financijske uredbe], zahtjev jedne treće zemlje dovoljan je da se Komisiju ili ENISA-u ovlasti za djelovanje.

Pri provedbi postupaka nabave za kibersigurnosnu pričuvu EU-a uspostavljenu člankom 12. Uredbe (EU) 2023/XX Komisija i ENISA mogu djelovati kao središnje tijelo za nabavu u ime ili za račun institucija, tijela i agencija Unije. Komisija i ENISA mogu djelovati i kao trgovac na veliko kupnjom, skladištenjem i preprodajom ili doniranjem robe i usluga, uključujući najam, tim institucijama, tijelima i agencijama Unije. Odstupajući od članka 169. stavka 3. Uredbe (EU) XXX/XXXX [preinaka Financijske uredbe], zahtjev jedne institucije, tijela ili agencije Unije dovoljan je da se Komisiju ili ENISA-u ovlasti za djelovanje.

Programom se može omogućiti financiranje i u obliku financijskih instrumenata u okviru operacija mješovitog financiranja.”;

4. dodaje se sljedeći članak 16.a:

„U slučaju djelovanja radi implementacije europskog kiberštita uspostavljenog člankom 3. Uredbe (EU) 2023/XX primjenjiva pravila su ona utvrđena u člancima 4. i 5. Uredbe (EU) 2023/XX. U slučaju proturječja između odredaba ove Uredbe i članaka 4. i 5. Uredbe (EU) 2023/XX, potonji članci imaju prednost i primjenjuju se na ta djelovanja.”;

5. članak 19. zamjenjuje se sljedećim:

„Bespovratna sredstva u okviru Programa dodjeljuju se te se njima upravlja u skladu s glavom VIII. Financijske uredbe i mogu pokrivati do 100 % prihvatljivih troškova, ne dovodeći u pitanje načelo sufinanciranja kako je utvrđeno u članku 190. Financijske uredbe. Takva bespovratna sredstva dodjeljuju se te se njima upravlja kako je navedeno za svaki specifični cilj.

U skladu s člankom 195. stavkom 1. točkom (d) Financijske uredbe Europski stručni centar u području kibersigurnosti može nacionalnim centrima za sigurnosne operacije iz članka 4. Uredbe XXXX i konzorciju domaćinu iz članka 5. Uredbe XXXX izravno, bez poziva na podnošenje prijedloga, dodijeliti potporu u obliku bespovratnih sredstava.

U skladu s člankom 195. stavkom 1. točkom (d) Financijske uredbe Europski stručni centar u području kibersigurnosti može državama članicama izravno, bez poziva na podnošenje prijedloga, dodijeliti potporu u obliku bespovratnih sredstava za mehanizam za izvanredne kibersigurnosne situacije, kako je utvrđeno u članku 10. Uredbe XXXX.

Za mjere iz članka 10. stavka 1. točke (c) Uredbe 202X/XXXX Europski stručni centar u području kibersigurnosti obavješćuje Komisiju i ENISA-u o zahtjevima država članica za izravna bespovratna sredstva bez poziva na podnošenje prijedloga.

Kad je riječ o potpori uzajamnoj pomoći pri odgovoru na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, kako je definirana u članku 10. točki (c) Uredbe XXXX i u skladu s člankom 193. stavkom 2. drugim podstavkom točkom (a) Financijske uredbe, u propisno opravdanim slučajevima troškovi se mogu smatrati prihvatljivima čak i ako su nastali prije podnošenja zahtjeva za bespovratna sredstva.”;

6. Prilozi I. i II. mijenjaju se u skladu s Prilogom ovoj Uredbi.

Članak 20.

Evaluacija

Komisija do [četiri godine od datuma početka primjene ove Uredbe] Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe.

Članak 21.

Postupak odbora

1. Komisiji pomaže Odbor za koordinaciju programa Digitalna Europa osnovan Uredbom (EU) 2021/694. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.

2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

Članak 22.

Stupanje na snagu

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Strasbourgu,

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

1.2. Predmetna područja politike

1.3. Prijedlog/inicijativa odnosi se na:

1.4. Ciljevi

1.4.1. Opći ciljevi

1.4.2. Specifični ciljevi

1.4.3. Očekivani rezultati i učinak

1.4.4. Pokazatelji uspješnosti

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije" je vrijednost koja proizlazi iz intervencije Unije i koja predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

1.5.3. Pouke iz prijašnjih sličnih iskustava

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

1.6. Trajanje i financijski učinak prijedloga/inicijative

1.7. Planirani načini izvršenja proračuna

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

2.3. Mjere za sprečavanje prijevara i nepravilnosti

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

3.2.3.1. Procijenjene potrebe u pogledu ljudskih resursa

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

3.2.5. Doprinos trećih strana

3.3. Procijenjeni učinak na prihode

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Uredba Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih

1.2. Predmetna područja politike

Europa spremna za digitalno doba

Europska strateška ulaganja

Aktivnost: izgradnja digitalne budućnosti Europe.

1.3. Prijedlog/inicijativa odnosi se na:

☒ **novo djelovanje**

☐ **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**[33]

☐ **produženje postojećeg djelovanja**

☐ **spajanje ili preusmjeravanje jednog ili više djelovanja u drugo/novo djelovanje**

1.4. Ciljevi

1.4.1. Opći ciljevi

Aktom o kibersolidarnosti ojačat će se solidarnost na razini Unije radi poboljšanja otkrivanja kibersigurnosnih prijetnji i incidenata, pripreme za njih i odgovora na njih. Ciljevi su mu:

(a) jačanje zajedničkog otkrivanja kiberprijetnji i kiberincidenata u EU-u te informiranosti o stanju u pogledu kiberprijetnji i kiberincidenata;

(b) jačanje pripravnosti kritičnih subjekata u cijelom EU-u i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore za odgovor na incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa;

(c) povećanje otpornosti Unije i djelotvornosti odgovora istraživanjem i procjenjivanjem značajnih incidenata ili incidenata velikih razmjera, među ostalim učenjem iz iskustva i, prema potrebi, davanjem preporuka.

1.4.2. Specifični ciljevi

Aktom o kibersolidarnosti utvrđeni ciljevi ostvarit će se:

[33] Kako je navedeno u članku 58. stavku 2. točkama (a) ili (b) Financijske uredbe.

(a) uvođenjem paneuropske infrastrukture centara za sigurnosne operacije (europski kiberštit) radi razvoja i poboljšanja zajedničkih sposobnosti za otkrivanje i informiranost o stanju;

(b) uspostavom mehanizma za izvanredne kibersigurnosne situacije kako bi se državama članicama pružila potpora u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih. Potpora za odgovor na incidente stavlja se na raspolaganje i institucijama, tijelima, uredima i agencijama Unije.

Te mjere poduprijet će se financiranjem iz programa Digitalna Europa, koji će se ovim zakonodavnim instrumentom izmijeniti kako bi se uspostavile prethodno navedene mjere, osigurala financijska potpora za njihov razvoj i pojasnili uvjeti za dobivanje financijske potpore;

(c) uspostavom europskog mehanizma za istraživanje kibersigurnosnih incidenata radi istraživanja i procjenjivanja značajnih incidenata ili incidenata velikih razmjera.

1.4.3. Očekivani rezultati i učinak

Navesti očekivane učinke prijedloga/inicijative na ciljane korisnike/skupine.

Prijedlog bi imao znatne koristi za razne dionike. Europskim kiberštitom poboljšat će se sposobnosti država članica za otkrivanje kiberprijetnji. Mehanizmom za izvanredne kibersigurnosne situacije dopunit će se mjere država članica osiguravanjem hitne potpore za pripravnost, odgovor i hitni oporavak / ponovnu uspostavu funkcioniranja ključnih usluga.

Tim će se mjerama ojačati konkurentni položaj industrije i poduzeća u Europi u digitaliziranom gospodarstvu i poduprijeti njihova digitalna transformacija povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Konkretno, cilj Prijedloga je povećati otpornost građana, poduzeća i subjekata koji djeluju u kritičnim i visokokritičnim sektorima na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. To će se postići ulaganjem u alate koji će olakšati brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih te koji će pomoći državama članicama da se bolje pripreme za kibersigurnosne incidente velikih razmjera i bolje odgovore na njih. Time bi se trebalo poduprijeti i jačanje kapaciteta Europe u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibersigurnosnim prijetnjama i incidentima.

1.4.4. Pokazatelji uspješnosti

Navesti pokazatelje za praćenje napretka i postignuća

Kako bi se promicala solidarnost na razini Unije, moglo bi se uzeti u obzir nekoliko pokazatelja:

1. količina infrastrukture i/ili alata za kibersigurnost, nabavljenih zajedničkom javnom nabavom;
2. broj mjera za potporu pripravnosti i odgovoru na kibersigurnosne incidente u okviru mehanizma za izvanredne kibersigurnosne situacije.

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative

Uredba bi se trebala početi u potpunosti primjenjivati ubrzo nakon donošenja, tj. dvadesetog dana od dana objave u *Službenom listu Europske unije*.

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije" je vrijednost koja proizlazi iz intervencije Unije i koja predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

Zbog izražene prekogranične naravi kibersigurnosnih prijetnji općenito i sve više rizika i incidenata, koji imaju učinke prelijevanja preko granica, sektora i proizvoda, države članice ne mogu same učinkovito ostvariti ciljeve ove intervencije te je potrebno zajedničko djelovanje i solidarnost na razini Unije. Iskustvo u borbi protiv kiberprijetnji stečeno na temelju rata Rusije protiv Ukrajine te iskustva stečena vježbom u području kibersigurnosti provedenom tijekom francuskog predsjedanja (EU CyCLES), pokazali su da bi trebalo razviti konkretne mehanizme uzajamne potpore, posebno suradnju s privatnim sektorom, kako bi se postigla solidarnost na razini EU-a. U tom se kontekstu u Zaključcima Vijeća od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora Komisija poziva da predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibersigurnosti. Potpora i mjere na razini Unije radi boljeg otkrivanja kibersigurnosnih prijetnji te povećanja kapaciteta za pripravnost i odgovor pružaju dodanu vrijednost jer se njima izbjegava udvostručavanje napora na razini Unije i u državama članicama. To bi omogućilo bolje iskorištavanje postojećih sredstava te bolju koordinaciju i razmjenu informacija o stečenim iskustvima.

1.5.3. Pouke iz prijašnjih sličnih iskustava

Kad je riječ o informiranosti o stanju i otkrivanju u okviru europskog kiberštita, u okviru programa rada za kibersigurnost programa Digitalna Europa za razdoblje 2021.–2022. objavljen je poziv na iskaz interesa za zajedničku nabavu alata i infrastrukture za uspostavu prekograničnih SOC-ova te poziv za dodjelu bespovratnih sredstava za izgradnju kapaciteta SOC-ova koji služe javnim i privatnim organizacijama.

Kad je riječ o pripravnosti i odgovoru na incidente, Komisija je uspostavila kratkoročni program za potporu državama članicama dodjelom dodatnih sredstava ENISA-i kako bi se hitno ojačali pripravnost i kapaciteti za odgovor na velike kiberincidente. Obuhvaćene usluge uključuju mjere pripravnosti, kao što su penetracijsko testiranje kritičnih subjekata kako bi se identificirale slabe točke. Povećavaju se i mogućnosti za pomoć državama članicama u slučaju velikog incidenta koji utječe na kritične subjekte. ENISA trenutačno provodi ovaj kratkoročni program i već je pružila relevantne vrijedne uvide koji su uzeti u obzir pri pripremi ove Uredbe.

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

Akt o kibersolidarnosti temeljit će se na mjerama koje Unija i države članice trenutačno podupiru kako bi se poboljšala informiranost o stanju i otkrivanje

kiberprijetnji te odgovorilo na kibersigurnosne incidente velikih razmjera i prekogranične kibersigurnosne incidente. Osim toga, instrument je u skladu s drugim okvirima za upravljanje krizama, uključujući IPCR, zajedničku sigurnosnu i obrambenu politiku, uključujući timove za brz odgovor na kiberincidente, te pomoć koju jedna država članica pruža drugoj državi članici u kontekstu članka 42. stavka 7. Ugovora o Europskoj uniji. Novim bi se prijedlogom dopunile i poduprle strukture razvijene u okviru drugih instrumenata za kibersigurnost, kao što su Direktiva (EU) 2022/2555 (Direktiva NIS 2) ili Uredba 2019/881 (Akt o kibersigurnosti).

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

Područja djelovanja kojima bi ENISA trebala upravljati odgovaraju njezinu trenutačnom mandatu i općim zadaćama. Ta područja djelovanja možda će zahtijevati posebne profile ili utvrđivanje novih zadaća, ali takvi zahtjevi mogu se apsorbirati postojećim resursima ENISA-e i riješiti preraspodjelom ili povezivanjem raznih zadaća. ENISA trenutačno provodi kratkoročni program koji je Komisija uspostavila 2022. kako bi hitno ojačala pripravnost i kapacitete za odgovor na velike kiberincidente. Obuhvaćene usluge uključuju mogućnosti za pomoć državama članicama u slučaju velikog incidenta koji utječe na kritične subjekte. ENISA trenutačno provodi ovaj kratkoročni program i već je pružila relevantne vrijedne uvide koji su uzeti u obzir pri pripremi ove Uredbe. Sredstva dodijeljena kratkoročnom programu mogla bi se koristiti i u kontekstu ove Uredbe.

1.6. Trajanje i financijski učinak prijedloga/inicijative

☒ **ograničeno trajanje**

– ☒ na snazi od datuma donošenja Prijedloga uredbe Europskog parlamenta i Vijeća o jačanju solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih („Akt o kibersolidarnosti”)

– ☒ financijski učinak od 2023. do 2027. za odobrena sredstva za preuzete obveze i od 2023. do 2031. za odobrena sredstva za plaćanje[34]

☐ **neograničeno trajanje**

– provedba s početnim razdobljem od GGGG do GGGG

– nakon čega slijedi redovna provedba.

1.7. Planirani načini izvršenja proračuna[35]

☒ **Izravno upravljanje** koje provodi Komisija

– ☒ putem svojih službi, uključujući osoblje u delegacijama Unije

– ☐ putem izvršnih agencija

☐ **Podijeljeno upravljanje** s državama članicama

☒ **Neizravno upravljanje** povjeravanjem zadaća izvršenja proračuna:

– ☐ trećim zemljama ili tijelima koja su one odredile

– ☐ međunarodnim organizacijama i njihovim agencijama (navesti)

– ☐ EIB-u i Europskom investicijskom fondu

– ☒ tijelima iz članaka 70. i 71. Financijske uredbe

– ☐ javnopravnim tijelima

– ☐ tijelima uređenima privatnim pravom koja pružaju javne usluge, u mjeri u kojoj su im dana odgovarajuća financijska jamstva

– ☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i kojima su dana odgovarajuća financijska jamstva

– ☐ osobama kojima je povjerena provedba određenih djelovanja u području ZVSP-a u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.

– *Ako je navedeno više načina upravljanja, navedite pojedinosti u odjeljku „Napomene”.*

Napomene

Aktivnosti povezane s europskim kiberštitom provodit će ECCC. Dok ECCC ne uspostavi kapacitete za izvršenje vlastitog proračuna, Europska komisija provodit će mjere pod izravnim upravljanjem u ime ECCC-a. ECCC može odabrati subjekte na temelju poziva na

[34] Mjere iz Akta trebalo bi poduprijeti sljedećim višegodišnjim financijskim okvirom.

[35] Informacije o načinima izvršenja proračuna i upućivanja na Financijsku uredbu dostupni su na internetskim stranicama BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

iskaz interesa za sudjelovanje u zajedničkoj nabavi alata. ECCC može dodijeliti bespovratna sredstva za rad tih alata.

Nadalje, ECCC može dodijeliti bespovratna sredstva za mjere pripravnosti u okviru mehanizma za izvanredne kibersigurnosne situacije.

Komisija je općenito odgovorna za primjenu kibersigurnosne pričuve EU-a. Komisija može u cijelosti ili djelomično, putem sporazuma o doprinosu, ENISA-i povjeriti rad kibersigurnosne pričuve EU-a i upravljanje njome. Zadaće dodijeljene ENISA-i na temelju ove Uredbe u skladu su s njezinim postojećim mandatom. Te zadaće uključuju: i. pružanje potpore Skupini za suradnju u području sigurnosti mrežnih i informacijskih sustava u razvoju mjera pripravnosti u skladu s procjenama rizika; ii. pružanje potpore Komisiji u uspostavi i nadzoru primjene kibersigurnosne pričuve EU-a, uključujući zaprimanje i obradu zahtjeva za potporu; iii. razvijanje predložaka kako bi se olakšalo podnošenje zahtjeva za potporu i sklapanje posebnih sporazuma između pružatelja usluga i korisnika kojem se pruža potpora u okviru kibersigurnosne pričuve EU-a; iv. istraživanje i procjenu prijetnji, ranjivosti i mjera ublažavanja u pogledu određenih značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera te pripremu izvješća o njima.

Na temelju stručnog znanja i pripremnog rada koji ENISA trenutačno obavlja u okviru pilot-projekta hitne potpore pripravnosti i odgovoru na incidente, procjenjuje se da sve te zadaće zahtijevaju oko sedam EPRV-a iz postojećih resursa ENISA-e.

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

Komisija će pratiti provedbu, primjenu i sukladnost s novim odredbama kako bi procijenila njihovu djelotvornost. Komisija podnosi izvješće o evaluaciji i preispitivanju ove Uredbe Europskom parlamentu i Vijeću u roku od četiri godine od datuma njezine primjene.

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

Uredbom se uvodi okvir za financiranje sredstvima EU-a radi povećanja otpornosti u području kibersigurnosti mjerama za poboljšanje sposobnosti otkrivanja značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera, odgovora na njih i oporavka od njih. Provedbom Direktive upravljat će odjeli unutar Glavne uprave CNECT zaduženi za to područje politike.

Kako bi mogle obavljati te nove zadaće, službama Komisije potrebno je osigurati odgovarajuća sredstva. Procjenjuje se da će provedba nove Uredbe zahtijevati 6 EPRV-a (3 AD-a i 3 UNS-a) za obavljanje sljedećih zadaća:

- određivanje mjera pripravnosti u skladu s procjenama rizika,
- osiguravanje interoperabilnosti prekograničnih platforma SOC-ova,
- razrada mogućih provedbenih akata (dva za SOC-ove i dva za mehanizam za izvanredne kibersigurnosne situacije),
- upravljanje ugovorima o smještaju i korištenju za SOC-ove,
- uspostava kibersigurnosne pričuve EU-a i upravljanje njome, izravno ili putem sporazuma o doprinosu ENISA-i. U slučaju sporazuma o doprinosu ENISA-i, razrada i nadzor provedbe sporazuma o doprinosu za zadaće dodijeljene ENISA-i,
- sudjelovanje u savjetodavnim skupinama koje saziva ENISA radi istraživanja i procjenjivanja značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera te priprema izvješća.

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

Za europski kiberštit utvrđen je rizik od toga da države članice ne dijele dovoljnu količinu relevantnih informacija o kiberprijetnjama među prekograničnim platformama SOC-a ili između prekograničnih platformi i drugih relevantnih subjekata na razini EU-a. Kako bi se ublažio taj rizik, dodjela sredstava uslijedit će nakon poziva na iskaz interesa u kojem se države članice obvezuju na dijeljenje određene količine informacija na razini EU-a. Ta će se obveza zatim formalizirati ugovorom o smještaju i korištenju, na temelju kojeg će ECCC dobiti ovlasti za provođenje revizija kako bi se osiguralo da se zajednički nabavljeni alati i infrastruktura upotrebljavaju u skladu s ugovorom. Obveze u pogledu visoke razine

dijeljenja informacija među prekograničnim SOC-ovima formalizirat će se ugovorom o konzorciju.

Kad je riječ o mehanizmu za izvanredne kibersigurnosne situacije, utvrđen je rizik od toga da korisnici koji sudjeluju u mehanizmu ne poduzimaju dostatne mjere za osiguravanje pripravnosti za kibernapade. Stoga su korisnici obvezni poduzeti takve mjere pripravnosti kako bi mogli primiti potporu iz kibersigurnosne pričuve EU-a. Pri podnošenju zahtjeva za potporu kibersigurnosnoj pričuvi EU-a korisnici moraju objasniti koje su mjere već poduzete kako bi se odgovorilo na incident, a koje će se uzeti u obzir pri procjeni zahtjeva podnesenog kibersigurnosneoj pričuvi EU-a.

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

Budući da su pravila za sudjelovanje u programu Digitalna Europa koja su primjenjiva na Akt o kibersolidarnosti slična pravilima koja će Komisija iskoristiti u svojim programima rada te da obuhvaćena skupina korisnika ima sličan profil rizičnosti kao korisnici programa u okviru izravnog upravljanja, može se očekivati da će granična vrijednost dopuštene pogreške biti slična onoj koju je Komisija predvidjela za program Digitalna Europa, odnosno da postoji razumna sigurnost da je godišnji rizik pogreške tijekom višegodišnjeg razdoblja rashoda unutar raspona od 2–5 %, uz krajnji cilj postizanja stope preostale pogreške što bliže vrijednosti od 2 % na kraju višegodišnjih programa, nakon što se uzme u obzir financijski učinak svih revizija i mjera namijenjenih ispravljanju i povratu.

2.3. Mjere za sprečavanje prijevara i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu, npr. iz strategije za borbu protiv prijevara.

U slučaju europskog kiberštita ECCC će imati ovlasti revizije, na temelju pristupa informacijama i provjera na licu mjesta, zajednički nabavljenih alata i infrastruktura, u skladu s ugovorom o smještaju i korištenju koji će potpisati konzorcij domaćin i ECCC.

Postojećim mjerama za sprečavanje prijevara koje se primjenjuju na institucije, tijela i agencije Unije pokrit će se dodatna odobrena sredstva potrebna za ovu Uredbu.

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

- Postojeće proračunske linije

Prema redoslijedu naslova višegodišnjeg financijskog okvira i proračunskih linija.

Naslov višegodišnjeg financijskog okvira	Proračunska linija	Vrsta rashoda	Doprinos			
	Broj	dif./nedif.[36]	zemalja EFTA-e[37]	zemalja kandidatkinja i potencijalnih kandidata[38]	ostalih trećih zemalja	drugi namjenski prihodi
1	02 04 01 10 – Program Digitalna Europa – Kibersigurnost	dif.	DA	DA	NE	NE
1	02 04 01 11 – Program Digitalna Europa – Europski stručni centar za industriju, tehnologiju i istraživanja u području kibersigurnosti	dif.	DA	DA	NE	NE
1	02 04 03 – Program Digitalna Europa – Umjetna inteligencija	dif.	DA	DA	NE	NE
1	02 04 04 – Program Digitalna Europa – Vještine	dif.	DA	DA	NE	NE
1	02 01 30 – Rashodi za potporu programu Digitalna Europa	nedif.	DA	DA	NE	NE

[36] Dif. = diferencirana odobrena sredstva; nedif. = nediferencirana odobrena sredstva.
[37] EFTA: Europsko udruženje slobodne trgovine.
[38] Zemlje kandidatkinje i, ako je primjenjivo, potencijalni kandidati.

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

– ☐ Za prijedlog/inicijativu nisu potrebna odobrena sredstva za poslovanje.

– ☒ Za prijedlog/inicijativu potrebna su sljedeća odobrena sredstva za poslovanje:

U milijunima EUR (do 3 decimalna mjesta)

Naslov višegodišnjeg financijskog okvira	Broj	1 **Jedinstveno tržište, inovacije i digitalizacija**

Prijedlogom se neće povećati ukupna razina obveza u okviru programa Digitalna Europa. Doprinosi ovoj inicijativi sastoji se od preraspodjele obveza koje proizlaze iz specifičnog cilja br. 2 (SO2) i specifičnog cilja br. 4 (SO4) kako bi se povećao proračun za specifični cilj br. 3 i ECCC. Svako povećanje obveza u okviru programa Digitalna Europa koje proizlazi iz revizije VFO-a moglo bi se upotrijebiti za potrebe ove inicijative.

GU CONNECT			Godina **2025.**	Godina **2026.**	Godina **2027.**	Godina **2028.+**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			**UKUPNO**
○ Odobrena sredstva za poslovanje										
Proračunska linija[39] 02.040110 (preraspodjela 02.0403 i 02.0404)	Obveze	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Plaćanja	(2a)	15,000	15,000	6,000					**36,000**
Proračunska linija 02.040111.02 (preraspodjela 02.0403 i 02.0404)	Obveze	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Plaćanja	(2b)	8,450	18,200	25,250	12,100				**64,000**
Administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe[40]										
Proračunska linija 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450
UKUPNA odobrena sredstva	Obveze	=1a+1b	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**

[39] Prema službenoj proračunskoj nomenklaturi.

[40] Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

za GU CONNECT		+3								
	Plaćanja	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ UKUPNA odobrena sredstva za poslovanje	Obveze	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Plaćanja	(5)	23,450	33,200	31,250	12,100				**100,000**
○ UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe		(6)	0,150	0,150	0,150	p.m.				**0,450**
UKUPNA odobrena sredstva iz NASLOVA 1. višegodišnjeg financijskog okvira	Obveze	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Plaćanja	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

<u>Ako prijedlog/inicijativa utječe na više od jednog naslova za poslovanje, ponovite prethodni odjeljak:</u>

○ UKUPNA odobrena sredstva za poslovanje (svi naslovi za poslovanje)	Obveze	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Plaćanja	(5)	23,450	33,200	31,250	12,100				**100,000**
UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe (svi naslovi za poslovanje)		(6)	0,150	0,150	0,150					**0,450**
UKUPNA odobrena sredstva iz NASLOVA 1.–6. višegodišnjeg financijskog okvira (referentni iznos)	Obveze	=4+6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Plaćanja	=5+6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Naslov višegodišnjeg financijskog okvira	7.	„Administrativni rashodi”

U ovaj se odjeljak unose „administrativni proračunski podaci”, koji prethodno moraju biti uneseni u prilog zakonodavnom financijskom izvještaju (Prilog 5. Odluci Komisije o internim pravilima za izvršenje dijela „Komisija” općeg proračuna Europske unije), koji se unosi u DECIDE za potrebe savjetovanja među službama.

U milijunima EUR (do 3 decimalna mjesta)

		Godina **2025.**	Godina **2026.**	Godina **2027.**	Godina **2028.+**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			**UKUPNO**
GU: CONNECT									
○ Ljudski resursi		0,786	0,786	0,786	p.m.				**2,358**
○ Ostali administrativni rashodi		0,035	0,035	0,035	p.m.				**0,105**
UKUPNO GU CONNECT	Odobrena sredstva	**0,821**	**0,821**	**0,821**					**2,463**

UKUPNA odobrena sredstva iz NASLOVA 7. višegodišnjeg financijskog okvira	(ukupne obveze = ukupna plaćanja)	**0,821**	**0,821**	**0,821**					**2,463**

U milijunima EUR (do 3 decimalna mjesta)

		Godina **2025.**	Godina **2026.**	Godina **2027.**	Godina **2028.+**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			**UKUPNO**
UKUPNA odobrena sredstva iz NASLOVA 1.–7. višegodišnjeg financijskog okvira	Obveze	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**
	Plaćanja	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

Odobrena sredstva za preuzimanje obveza u milijunima EUR (do 3 decimalna mjesta)

Navesti ciljeve i rezultate ⇩			Godina **N**		Godina **N+1**		Godina **N+2**		Godina **N+3**		Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)						**UKUPNO**	
	REZULTATI																	
	Vrsta [41]	Prosječni trošak	Ne	Trošak	Ne	Trošak	Ne	Trošak	Ne	Trošak	Ne	Trošak	Ne	Trošak	Ne	Trošak	Ukupni broj	Ukupni trošak
SPECIFIČNI CILJ br. 1[42]…																		
— Rezultat																		
— Rezultat																		
— Rezultat																		
Međuzbroj za specifični cilj br. 1																		
SPECIFIČNI CILJ br. 2...																		
— Rezultat																		
Međuzbroj za specifični cilj br. 2																		
UKUPNO																		

[41] Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

[42] Kako je opisan u točki 1.4.2. „Specifični ciljevi…”.

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

– ☐ Za prijedlog/inicijativu nisu potrebna administrativna odobrena sredstva.

– ☒ Za prijedlog/inicijativu potrebna su sljedeća administrativna odobrena sredstva:

U milijunima EUR (do 3 decimalna mjesta)

	Godina 2025.	Godina 2026.	Godina 2027.	Godina N+3	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			**UKUPNO**
NASLOV 7. višegodišnjeg financijskog okvira								
Ljudski resursi	0,786	0,786	0,786					**2,358**
Ostali administrativni rashodi	0,035	0,035	0,035					**0,105**
Međuzbroj za NASLOV 7. višegodišnjeg financijskog okvira	**0,821**	**0,821**	**0,821**					**2,463**

Izvan NASLOVA 7.[43] višegodišnjeg financijskog okvira								
Ljudski resursi								
Ostali administrativni rashodi	0,150	0,150	0,150					**0,450**
Međuzbroj izvan NASLOVA 7. višegodišnjeg financijskog okvira	**0,150**	**0,150**	**0,150**					**0,450**

UKUPNO	**0,971**	**0,971**	**0,971**					**2,913**

Potrebna odobrena sredstva za ljudske resurse i ostale administrativne rashode pokrit će se odobrenim sredstvima glavne uprave koja su već dodijeljena za upravljanje djelovanjem i/ili su preraspodijeljena unutar glavne uprave te, prema potrebi, dodatnim sredstvima koja se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

[43] Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

3.2.3.1. Procijenjene potrebe u pogledu ljudskih resursa

– ☐ Za prijedlog/inicijativu nisu potrebni ljudski resursi.

– ☒ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu navesti u ekvivalentima punog radnog vremena

		Godina **2025.**	Godina **2026.**	Godina 2027.	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)		
O Radna mjesta prema planu radnih mjesta (dužnosnici i privremeno osoblje)								
20 01 02 01 (sjedište i predstavništva Komisije)		3	3	3				
20 01 02 03 (delegacije)								
01 01 01 01 (neizravno istraživanje)								
01 01 01 11 (izravno istraživanje)								
Druge proračunske linije (navesti)								
O Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV)[44]								
20 02 01 (UO, UNS, UsO iz „globalne omotnice")		3	3	3				
20 02 03 (UO, LO, UNS, UsO i MSD u delegacijama)								
XX 01 xx **yy zz** [45]	— u sjedištima							
	— u delegacijama							
01 01 01 02 (UO, UNS, UsO – neizravno istraživanje)								
01 01 01 12 (UO, UNS, UsO – izravno istraživanje)								
Druge proračunske linije (navesti)								
UKUPNO		**6**	**6**	**6**				

XX se odnosi na odgovarajuće područje politike ili glavu proračuna.

Potrebe za ljudskim resursima pokrit će se osobljem glavne uprave kojemu je već povjereno upravljanje djelovanjem i/ili koje je preraspoređeno unutar glavne uprave te, prema potrebi, resursima koji se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Opis zadaća:

Dužnosnici i privremeno osoblje	- utvrđivanje mjera pripravnosti u skladu s procjenama rizika (članak 11.), - razrada mogućih provedbenih akata (dva za SOC-ove i dva za mehanizam za izvanredne kibersigurnosne situacije), - upravljanje ugovorima o smještaju i korištenju za SOC-ove, - uspostava kibersigurnosne pričuve EU-a i upravljanje njome, izravno ili putem sporazuma o doprinosu ENISA-i.
Vanjsko osoblje	Pod nadzorom dužnosnika, - utvrđivanje mjera pripravnosti u skladu s procjenama rizika (članak 11.), - razrada mogućih provedbenih akata (dva za SOC-ove i dva za mehanizam za izvanredne kibersigurnosne situacije), - upravljanje ugovorima o smještaju i korištenju za SOC-ove, - uspostava kibersigurnosne pričuve EU-a i upravljanje njome, izravno ili putem sporazuma o doprinosu ENISA-i.

[44] UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

[45] U okviru gornje granice za vanjsko osoblje iz odobrenih sredstava za poslovanje (prijašnje linije „BA").

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

Prijedlog/inicijativa:

– [X] može se u potpunosti financirati preraspodjelom unutar relevantnog naslova višegodišnjeg financijskog okvira (VFO).

Objasniti o kakvom je reprogramiranju riječ te navesti predmetne proračunske linije i odgovarajuće iznose. U slučaju većeg reprogramiranja dostaviti tablicu u Excel formatu.

	23	24	25	26	27	ukupno
SC1	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
SC2 početno	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
Inicijativa za kibersolidarnost			18 000 000	28 000 000	19 000 000	65 000 000
NOVI SC2	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
SC3 NACRT 24	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
SC2–SC4			15 000 000	15 000 000	6 000 000	36 000 000
Novi SC3	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
ECCC početno	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
SC2–SC4			13 000 000	23 000 000	28 000 000	64 000 000
Novi ECCC	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
SC4 početno	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
Inicijativa za kibersolidarnost			10 000 000	10 000 000	15 000 000	35 000 000
NOVI SC4	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] zahtijeva upotrebu nedodijeljene razlike u okviru relevantnog naslova VFO-a i/ili upotrebu posebnih instrumenata kako su definirani u Uredbi o VFO-u.

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije, odgovarajuće iznose te instrumente čija se upotreba predlaže.

– [ ] zahtijeva reviziju VFO-a.

Objasniti što je potrebno te navesti predmetne naslove i proračunske linije te odgovarajuće iznose.

3.2.5. Doprinos trećih strana

U prijedlogu/inicijativi:

– [X] ne predviđa se sudjelovanje trećih strana u sufinanciranju

– [ ] predviđa se sudjelovanje trećih strana u sufinanciranju prema sljedećoj procjeni:

Odobrena sredstva u milijunima EUR (do 3 decimalna mjesta)

	Godina **N**[46]	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)	Ukupno

[46] Godina N je godina početka provedbe prijedloga/inicijative. Umjesto „N" upisati predviđenu prvu godinu provedbe (na primjer: 2021.). Isto vrijedi i za ostale godine.

Navesti tijelo koje sudjeluje u financiranju								
UKUPNO sufinancirana odobrena sredstva								

3.3. Procijenjeni učinak na prihode

– ☒ Prijedlog/inicijativa nema financijski učinak na prihode.

– ☐ Prijedlog/inicijativa ima sljedeći financijski učinak:

  – ☐ na vlastita sredstva

  – ☐ na ostale prihode

  – navesti jesu li prihodi namijenjeni proračunskim linijama rashoda ☐

U milijunima EUR (do 3 decimalna mjesta)

Proračunska linija prihoda:	Odobrena sredstva dostupna za tekuću financijsku godinu	Učinak prijedloga/inicijative[47]						
		Godina **N**	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)		
Članak ….								

Za namjenske prihode navesti odgovarajuće proračunske linije rashoda.

[…]

Ostale napomene (npr. metoda/formula za izračun učinka na prihode ili druge informacije)

[…]

[47] Kad je riječ o tradicionalnim vlastitim sredstvima (carine, pristojbe na šećer) navedeni iznosi moraju biti neto iznosi, to jest bruto iznosi nakon odbitka od 20 % na ime troškova naplate.