EUROPSKA UNIJA

EUROPSKI PARLAMENT **VIJEĆE**

Bruxelles, 19. prosinca 2024.
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

UREDBA EUROPSKOG PARLAMENTA I VIJEĆA O UTVRĐIVANJU MJERA ZA POVEĆANJE SOLIDARNOSTI I KAPACITETA U UNIJI ZA OTKRIVANJE KIBERNETIČKIH PRIJETNJI I INCIDENATA, PRIPREMU ZA NJIH I ODGOVOR NA NJIH TE O IZMJENI UREDBE (EU) 2021/649 (AKT O KIBERNETIČKOJ SOLIDARNOSTI)

UREDBA (EU) 2024/…
EUROPSKOG PARLAMENTA I VIJEĆA

od 19. prosinca 2024.

o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibernetičkih prijetnji i incidenata, pripremu za njih i odgovor na njih te o izmjeni Uredbe (EU) 2021/649
(Akt o kibernetičkoj solidarnosti)

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[4],

---

1 Mišljenje od 18. travnja 2023. (još nije objavljeno u Službenom listu).
2 SL C 349, 29.9.2023., str. 167.
3 SL C, C/2024/1049, 9.2.2024., ELI: http://data.europa.eu/eli/C/2024/1049/oj.
4 Stajalište Europskog parlamenta od 24. travnja 2024. (još nije objavljeno u Službenom listu) i odluka Vijeća od 2. prosinca 2024.

budući da:

(1) Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora gospodarske aktivnosti i društva u svjetlu sve veće međusobne povezanosti i međuovisnosti javnih uprava država članica, poduzeća i građana u svim sektorima te preko granica, što u isto vrijeme stvara moguće ranjivosti.

(2) Na razini Unije i na globalnoj razini povećavaju se razmjeri, učestalost i učinci kibernetičkih sigurnosnih incidenata, uključujući napade na lance opskrbe u svrhe kibernetičke špijunaže, napada ucjenjivačkim softverom ili izazivanja poremećaja. Oni predstavljaju veliku prijetnju funkcioniranju mrežnih i informacijskih sustava. S obzirom na to da se prijetnje brzo mijenjaju, mogući kibernetički sigurnosni incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu na kritičnoj infrastrukturi iziskuju povećanu pripravnost okvira Unije za kibernetičku sigurnost. Ta prijetnja nadilazi agresivni rat Rusije protiv Ukrajine i vjerojatno će se nastaviti s obzirom na mnoštvo aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga jer su kibernetički napadi često usmjereni na lokalne, regionalne ili nacionalne javne usluge i infrastrukture, pri čemu su lokalne vlasti posebno ranjive, među ostalim zbog svojih ograničenih resursa. Oni isto tako mogu ometati obavljanje gospodarskih djelatnosti, među ostalim u sektorima visoke kritičnosti ili drugim kritičnim sektorima, uzrokovati znatne financijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu i demokratskim sustavima Unije te čak imati zdravstvene ili po život opasne posljedice. K tomu, kibernetički sigurnosni incidenti su nepredvidivi jer se često pojavljuju i brzo razvijaju, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u mnogim zemljama ili se brzo šire na mnoge zemlje. Važno je da postoji bliska suradnja između javnog sektora, privatnog sektora, akademske zajednice, civilnog društva i medija.

(3) Potrebno je ojačati konkurentni položaj industrije i usluga u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibernetičke sigurnosti na digitalnom jedinstvenom tržištu, kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe. Potrebno je povećati otpornost građana, poduzeća, uključujući mikropoduzeća, mala i srednja poduzeća i novoosnovana poduzeća, i subjekata koji upravljaju kritičnom infrastrukturom, na sve veće kibernetičke prijetnje koje mogu imati razoran društveni i gospodarski učinak. Stoga su potrebna ulaganja u infrastrukturu i usluge te izgradnja sposobnosti za razvoj vještina u području kibernetičke sigurnosti kojima će se omogućiti brže otkrivanje kibernetičkih prijetnji i incidenata i brži odgovor na njih. Dodatno, državama članicama potrebna je pomoć u boljoj pripremi za značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera i odgovoru na takve incidente kao i pomoć u inicijalnom oporavku od njih. Temeljeći se na postojećim strukturama te u bliskoj suradnji s njima, Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibernetičkim prijetnjama i incidentima.

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu rizika, koje posebice uključuju Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[5], direktive 2013/40/EU[6] i (EU) 2022/2555[7] Europskog parlamenta i Vijeća te Preporuku Komisije (EU) 2017/1584[8].. Nadalje, u Preporuci Vijeća od 8. prosinca 2022. o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture države članice pozivaju se da poduzmu mjere te da surađuju 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 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.).

6 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.).

7 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., str. 80.).

8 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.).

(5) Zbog sve većih kibernetičkih sigurnosnih rizika i općenito složenih prijetnji te uz očit rizik od brzog širenja incidenata iz jedne države članice u druge i iz treće zemlje u Uniju, potrebno je jačanje solidarnosti na razini Unije kako bi se kibernetičke prijetnje i incidenti bolje otkrivali te kako bi se za njih bolje pripremalo, na njih bolje odgovaralo i od njih bolje oporavljalo, posebice jačanjem sposobnosti postojećih struktura. Štoviše, u Zaključcima Vijeća od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora Komisiju se poziva da predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibernetičke sigurnosti.

(6) U Zajedničkoj komunikaciji Komisije i Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku od 10. studenog 2022. Europskom parlamentu i Vijeću o politici kiberobrane EU-a, najavljena je inicijativa EU-a za kibernetičku solidarnost s ciljevima jačanje zajedničkih sposobnosti EU-a za otkrivanje, informiranost o stanju i odgovor poticanjem uvođenja infrastrukture centara za sigurnosne operacije (SOC) u EU-u, podupiranje postupne izgradnje kibernetičke 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) U cijeloj Uniji potrebno je poboljšati otkrivanje i informiranost o stanju kibernetičkih prijetnji i incidenata te ojačati solidarnost unapređenjem pripravnosti država članica i Unije te njihovih sposobnosti za sprečavanje i odgovor na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera. Stoga je potrebno uspostaviti paneuropsku mrežu kibernetičkih centara („europski sustav uzbunjivanja u području kibernetičke sigurnosti”) kako bi se izgradile koordinirane sposobnosti za otkrivanje i informiranost o stanju i tako ojačale sposobnosti Unije za otkrivanje prijetnji i dijeljenje informacija o njima; trebalo bi uspostaviti mehanizam za izvanredne kibernetičke sigurnosne situacije kako bi se državama članicama, na njihov zahtjev, pomoglo u pripremi za značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera, odgovoru na njih i inicijalnom oporavku od njih te kako bi se drugim korisnicima pružila potpora u odgovoru na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera; trebalo bi uspostaviti i europski mehanizam za istraživanje kibernetičkih sigurnosnih incidenata kako bi se istražili i procijenili određeni značajni kibernetički sigurnosni incidenti ili kibernetički sigurnosni incidenti velikih razmjera. Djelovanja na temelju ove Uredbe trebale bi se provoditi uz dužno poštovanje nadležnosti država članica te bi trebale dopunjavati, a ne duplicirati aktivnosti koje provode mreža CSIRT-ova, Europska mreža organizacija za vezu za kibernetičke krize („mreža EU-CyCLONe“) i skupina za suradnju („skupina za suradnju NIS“), koje su sve uspostavljene na temelju Direktive (EU) 2022/2555. Tim se djelovanjima ne dovode u pitanje članci 107. i 108. Ugovora o funkcioniranju Europske unije (UFEU).

(8) Radi postizanja tih ciljeva potrebno je izmijeniti određene dijelove Uredbe (EU) 2021/694 Europskog parlamenta i Vijeća[9]. Ovom bi se Uredbom osobito trebala izmijeniti Uredba (EU) 2021/694 u pogledu dodavanja novih operativnih ciljeva povezanih s europskim sustavom uzbunjivanja u području kibernetičke sigurnosti i mehanizmom za izvanredne kibernetičke sigurnosne situacije u okviru specifičnog cilja 3 programa Digitalna Europa, kojim se nastoji zajamčiti otpornost, integritet i pouzdanost jedinstvenog digitalnog tržišta, ojačati kapacitete za praćenje kibernetičkih napada i kibernetičkih prijetnji i odgovor na njih te ojačati prekograničnu suradnju i koordinaciju u području kibernetičke sigurnosti. Europski sustav uzbunjivanja u području kibernetičke sigurnosti mogao bi imati važnu ulogu u pružanju potpore državama članicama u predviđanju kibernetičkih prijetnji i zaštiti od njih, a pričuva EU-a za kibernetičku sigurnost mogla bi imati važnu ulogu u pružanju potpore državama članicama, institucijama, tijelima, uredima i agencijama Unije te trećim zemljama pridruženima programu Digitalna Europa u odgovoru na učinak značajnih kibernetičkih sigurnosnih incidenata, kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih sigurnosnih incidenata ekvivalentnima onima velikih razmjera te ublažavanju tog učinka. Taj bi učinak mogao uključivati znatnu materijalnu ili nematerijalnu štetu i ozbiljne rizike za javnu sigurnost i zaštitu. S obzirom na posebne uloge koje bi europski sustav uzbunjivanja u području kibernetičke sigurnosti i pričuva EU-a za kibernetičku sigurnost mogli imati, ovom bi se Uredbom trebala izmijeniti Uredba (EU) 2021/694 u pogledu sudjelovanja pravnih subjekata s poslovnim nastanom u Uniji, ali pod kontrolom iz trećih zemalja, ako postoji stvaran rizik da potrebni i dostatni alati, infrastrukture i usluge, ili tehnologija, stručno znanje i kapaciteti, nisu dostupni u Uniji te da koristi od uključivanja takvih subjekata nadmašuju sigurnosni rizik. Trebalo bi utvrditi posebne uvjete pod kojima se može dodijeliti financijska potpora za djelovanja kojima se provodi europski sustav uzbunjivanja u području kibernetičke sigurnosti i pričuva EU-a za kibernetičku sigurnost te bi trebalo definirati mehanizme upravljanja i koordinacije potrebne za postizanje predviđenih ciljeva. Druge izmjene Uredbe (EU) 2021/694 trebale bi uključivati opise predloženih djelovanja u okviru novih operativnih ciljeva, kao i mjerljive pokazatelje za praćenje provedbe tih novih operativnih ciljeva.

---

9 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.).

(9) Za jačanje odgovora Unije na kibernetičke prijetnje i incidente ključna je suradnja s međunarodnim organizacijama te s pouzdanim međunarodnim partnerima sličnih stavova. U tom bi kontekstu pouzdane međunarodne partnere sličnih stavova trebalo tumačiti kao zemlje koje dijele načela koja su nadahnula stvaranje Unije odnosno demokracije, vladavine prava, univerzalnosti i nedjeljivosti ljudskih prava i temeljnih sloboda, poštovanja ljudskog dostojanstva, načela jednakosti i solidarnosti te poštovanja načela Povelje Ujedinjenih naroda i međunarodnog prava, te koje ne ugrožavaju ključne sigurnosne interese Unije ili njezinih država članica. Takva suradnja mogla bi biti korisna i u pogledu djelovanja koja se poduzimaju na temelju ove Uredbe, a posebno europskog sustava uzbunjivanja u području kibernetičke sigurnosti i pričuve EU-a za kibernetičku sigurnost. Uredbom (EU) 2021/694 trebalo bi predvidjeti, podložno određenim uvjetima dostupnosti i sigurnosti, da natječaji za europski sustav uzbunjivanja u području kibernetičke sigurnosti i pričuvu EU-a za kibernetičku sigurnost budu otvoreni pravnim subjektima pod kontrolom iz trećih zemalja, podložno sigurnosnim zahtjevima. Pri procjeni sigurnosnog rizika takvog otvaranja nabave važno je uzeti u obzir načela i vrijednosti koje Unija dijeli s međunarodnim partnerima sličnih stavova, kada su ta načela i vrijednosti povezani s ključnim sigurnosnim interesima Unije. Povrh toga, ako se takvi sigurnosni zahtjevi razmatraju na temelju Uredbe (EU) 2021/694, u obzir bi se moglo uzeti nekoliko elemenata, kao što su korporativna struktura subjekta i njegov postupak donošenja odluka, sigurnost podataka i klasificiranih ili osjetljivih informacija te osiguravanje da rezultati djelovanja ne podliježu kontroli ili ograničenjima trećih zemalja koje ne ispunjavaju uvjete.

(10) Financiranje djelovanja na temelju ove Uredbe trebalo bi biti predviđeno Uredbom (EU) 2021/694, koja bi trebala ostati relevantni temeljni akt za ta djelovanja obuhvaćena specifičnim ciljem 3 programa Digitalna Europa. Posebni uvjeti za sudjelovanje za svako djelovanje definiraju se u relevantnim programima rada, u skladu s Uredbom (EU) 2021/694.

(11) 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 Uredbi (EU, Euratom) 2024/2509 Europskog parlamenta i Vijeća[10] 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].

[10] Uredba (EU, Euratom) 2024/2509 Europskog parlamenta i Vijeća od 23. rujna 2024. o financijskim pravilima koja se primjenjuju na opći proračun Unije (SL L, 2024/2509, 26.9.2024., http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Uredba (EU, Euratom) 2020/2092 Europskog parlamenta i Vijeća od 16. prosinca 2020. o općem režimu uvjetovanosti za zaštitu proračuna Unije, (SL L 433 I, 22.12.2020., str. 1., ELI: http://data.europa.eu/eli/reg/2020/2092/oj).

(12) Iako su mjere prevencije i pripravnosti ključne za povećanje otpornosti Unije pri suočavanju sa značajnim kibernetičkim sigurnosnim incidentima, kibernetičkim sigurnosnim incidentima velikih razmjera i kibernetičkim sigurnosnim incidentima ekvivalentnima kibernetičkom sigurnosnom incidentu velikih razmjera, sama pojava, vrijeme i razmjer takvih incidenata po svojoj su prirodi nepredvidivi. Financijska sredstva koja su potrebna za osiguravanje adekvatnog odgovora mogu znatno varirati od godine do godine te bi ih se trebalo moći odmah staviti na raspolaganje. Pomirivanje proračunskog načela predvidljivosti s potrebom da se brzo odgovori na nove potrebe stoga iziskuje prilagodbu financijskog izvršenja programa rada. Stoga je primjereno, uz prijenos odobrenih sredstava odobren u skladu s člankom 12. stavkom 4. Uredbe (EU, Euratom) 2024/2509, odobriti prijenos neiskorištenih odobrenih sredstava, ali isključivo u sljedeću godinu i isključivo u pričuvu EU-a za kibernetičku sigurnost i djelovanja kojima se podupire uzajamna pomoć.

(13) Kako bi se učinkovitije spriječile i procijenile kibernetičke prijetnje i kibernetički incidenti te na njih odgovorilo i od njih bolje oporavilo, 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 kibernetičkih napada koji pogađaju te infrastrukture. Proaktivan pristup utvrđivanju, ublažavanju i sprečavanju kibernetičkih prijetnji uključuje povećane sposobnosti za napredno otkrivanje. Europski sustav uzbunjivanja u području kibernetičke sigurnosti trebao bi se sastojat od nekoliko interoperabilnih prekograničnih kibernetičkih centara, od kojih svaki okuplja tri ili više nacionalnih kibernetičkih centara. Ta bi infrastruktura trebala služiti kibernetičkim sigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijim tehnologijama za napredno prikupljanje relevantnih podataka i informacija koji se, prema potrebi, anonimiziraju, te alatima za analitiku podataka, jačajući koordinirane sposobnosti kibernetičkog otkrivanja i upravljanja i osiguravajući informiranost o stanju u stvarnom vremenu. Ta bi infrastruktura trebala služiti za poboljšanje razine kibernetičke sigurnosti i to povećanjem otkrivanja, objedinjavanja i analize podataka i informacija kako bi se spriječile kibernetičke prijetnje i incidenti te tako dopunili i poduprli subjekti i mreže Unije odgovorni za upravljanje kibernetičkim krizama u Uniji, posebno mreža EU-CyCLONe.

(14) Sudjelovanje u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti dobrovoljno je za države članice. Svaka bi država članica trebala na nacionalnoj razini imenovati jednog subjekta zaduženog za koordinaciju aktivnosti otkrivanja kibernetičkih prijetnji u toj državi članici. Ti nacionalni kibernetički centri trebali bi djelovati kao referentna i pristupna točka na nacionalnoj razini za sudjelovanje u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti te bi trebali osigurati da se informacije o kibernetičkim prijetnjama dobivene od javnih i privatnih subjekata dijele i prikupljaju na nacionalnoj razini na djelotvoran i optimiziran način. Nacionalni kibernetički centri mogli bi ojačati suradnju i dijeljenje informacija između javnih i privatnih subjekata te bi mogli podupirati razmjenu relevantnih podataka i informacija s relevantnim sektorskim i međusektorskim zajednicama, uključujući relevantne industrijske centre za dijeljenje i analizu informacija („ISAC-i”). Bliska i koordinirana suradnja javnih i privatnih subjekata ključna je za jačanje kibernetičke otpornosti Unije. Takva suradnja posebno je vrijedna u kontekstu dijeljenja saznanja o kibernetičkim prijetnjama kako bi se poboljšala aktivna kibernetička zaštita. U okviru takve suradnje i dijeljenja informacija nacionalni kibernetički centri mogli bi tražiti i primati specifične informacije. Ti se nacionalni kibernetički centri ovom Uredbom niti obvezuju niti ovlašćuju za izvršavanje takvih zahtjeva. Prema potrebi i u skladu s pravom Unije i nacionalnim pravom, zatražene ili primljene informacije mogle bi uključivati telemetrijske i senzorske podatke i podatke o evidentiranju od subjekata, kao što su pružatelji upravljanih sigurnosnih usluga, koji posluju u sektorima visoke kritičnosti ili drugim kritičnim sektorima unutar te države članice, kako bi se unaprijedilo brzo otkrivanje potencijalnih kibernetičkih prijetnji i incidenata u ranijoj fazi, čime bi se poboljšala informiranost o stanju. Ako nacionalni kibernetički centar nije nadležno tijelo koje je imenovala ili uspostavila relevantna država članica u skladu s člankom 8. stavkom 1. Direktive (EU) 2022/2555, ključno je da se on koordinira s tim nadležnim tijelom u pogledu zahtjeva za takve podatke i primanja takvih podataka.

(15) U okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti trebalo bi uspostaviti niz prekograničnih kibernetičkih centara. U tim bi prekograničnim kibernetičkim centrima trebalo okupiti nacionalne kibernetičke centre iz najmanje triju država članica kako bi se osiguralo da se u potpunosti ostvare koristi od otkrivanja prekograničnih prijetnji te dijeljenja informacija i upravljanja njima. Opći cilj prekograničnih kibernetičkih centara trebao bi biti jačanje kapaciteta za analizu, sprečavanje i otkrivanje kibernetičkih sigurnosnih prijetnji te podupiranje proizvodnje visokokvalitetnih saznanja o kibernetičkim prijetnjama, osobito dijeljenjem relevantnih informacija koje se, prema potrebi, anonimiziraju, u pouzdanom i sigurnom okruženju iz različitih izvora, javnih ili privatnih, te dijeljenjem i zajedničkom uporabom najsuvremenijih alata i zajedničkim razvojem sposobnosti otkrivanja, analize i sprečavanja u pouzdanom i sigurnom okruženju. Prekograničnim kibernetičkim centrima trebalo bi se osigurati nove dodatne kapacitete koji se temelje na postojećim SOC-ovima, CSIRT-ovima i drugim relevantnim akterima, uključujući mrežu CSIRT-ova, te koji ih nadopunjuju.

(16) Država članica koju je Europski stručni centar za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti („ECCC”) osnovan Uredbom (EU) 2021/887 Europskog parlamenta i Vijeća[12] odabrao nakon poziva na iskaz interesa za osnivanje ili unapređenje sposobnosti nacionalnog kibernetičkog centra trebala bi zajedno s ECCC-om kupiti relevantne alate, infrastrukturu ili usluge. Takva država članica trebala bi biti prihvatljiva za primanje bespovratnih sredstava za upravljanje alatima, infrastrukturom ili uslugama. Konzorcij domaćin koji se sastoji od najmanje tri države članice, a kojeg je odabrao ECCC nakon poziva na iskaz interesa za uspostavljanje ili unapređenje sposobnosti prekograničnog kibernetičkog centra, trebao bi zajedno s ECCC-om kupiti relevantne alate, infrastrukturu ili usluge. Konzorcij domaćin trebao bi biti prihvatljiv za primanje bespovratnih sredstava za upravljanje alatima, infrastrukturom ili uslugama. Postupak nabave za kupnju relevantnih alata, infrastrukture i usluga trebali bi zajednički provoditi ECCC i relevantni javni naručitelji iz država članica odabrani na temelju tih poziva na iskaz interesa. Takva bi nabava trebala biti u skladu s člankom 168. stavkom 2. Uredbe (EU) 2024/25091046 i financijskim pravilima ECCC-a. Privatni subjekti stoga ne bi trebali biti prihvatljivi za sudjelovanje u pozivima na iskaze interesa za kupnju alata, infrastrukture ili usluga zajedno s ECCC-om ili za primanje bespovratnih sredstava za upravljanje tim alatima, infrastrukturom ili uslugama. Međutim, države članice trebale bi moći uključiti privatne subjekte u uspostavu, unapređenje i rad svojih nacionalnih kibernetičkih centara i prekograničnih kibernetičkih centara na druge načine koje smatraju primjerenima, u skladu s pravom Unije i nacionalnim pravom. Privatni subjekti isto bi tako mogli biti prihvatljivi za primanje financijskih sredstava Unije u skladu s Uredbom (EU) 2021/887 radi pružanja potpore nacionalnim kibernetičkim centrima.

---

[12] Uredba (EU) 2021/887 Europskog parlamenta i Vijeća 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., ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) Kako bi se poboljšalo otkrivanje kibernetičkih prijetnji i informiranost o stanju u Uniji, država članica koja je nakon poziva na iskaz interesa odabrana za osnivanje ili unapređivanje sposobnosti nacionalnog kibernetičkog centra trebala bi se obvezati da će se prijaviti za sudjelovanje u prekograničnom kibernetičkom centru. Ako država članica ne postane sudionica u prekograničnom kibernetičkom centru u roku od dvije godine od datuma stjecanja alata, infrastrukture ili usluga ili datuma na koji primi bespovratna sredstva, ovisno o tome što nastupi ranije, ona ne bi trebala biti prihvatljiva za sudjelovanje u daljnjim potpornim djelovanjima Unije u okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti za unapređenje sposobnosti njezina nacionalnog kibernetičkog centra. U takvim slučajevima subjekti iz država članica i dalje bi mogli sudjelovati u pozivima na podnošenje prijedloga koji se odnose na druge teme u okviru programa Digitalna Europa ili drugih programa financiranja Unije, uključujući pozive koji se odnose na kapacitete za kibernetičko otkrivanje i dijeljenje informacija, pod uvjetom da ti subjekti ispunjavaju kriterije prihvatljivosti utvrđene u tim programima.

(18) CSIRT-ovi razmjenjuju informacije unutar mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Europski sustav uzbunjivanja u području kibernetičke sigurnosti trebao bi predstavljati novu sposobnost koja je komplementarna mreži CSIRT-ova na način da doprinosi izgradnji informiranosti o stanju u Uniji, čime se omogućuje jačanje sposobnosti mreže CSIRT-ova. Prekogranični kibernetički centri trebali bi se koordinirati i blisko surađivati s mrežom CSIRT-ova. Trebali bi djelovati na način da objedinjuju podatke i dijele relevantne informacije, koji se, prema potrebi, anonimiziraju, o kibernetičkim sigurnosnim prijetnjama od javnih i privatnih subjekata, povećavajući vrijednosti takvih podataka i informacija stručnom analizom i zajednički nabavljenim infrastrukturama i najsuvremenijim alatima te doprinošenjem tehnološkoj suverenosti Unije, njezinoj otvorenoj strateškoj autonomiji, konkurentnosti i otpornosti te razvoju sposobnosti Unije.

(19) Prekogranični kibernetički centri trebali bi djelovati kao središnje točke koje omogućuju opsežno objedinjavanje relevantnih podataka i saznanja o kibernetičkim prijetnjama, te omogućiti širenje informacija o prijetnjama među velikim i raznolikim skupom dionika kao što su timovi za hitne računalne intervencije (CERT), CSIRT-ovi, ISAC-ovi i operateri kritične infrastrukture. Članovi konzorcija domaćina trebali bi u sporazumu o konzorciju navesti relevantne informacije koje će se dijeliti među sudionicima predmetnog prekograničnog kibernetičkog centra. Informacije koje razmjenjuju sudionici u prekograničnom kibernetičkom centru mogle bi uključivati, na primjer, podatke iz mreža i senzora, saznanja o prijetnjama, pokazatelje ugroženosti i informacije s kontekstom o incidentima, kibernetičkim prijetnjama, izbjegnutim incidentima, ranjivostima, tehnikama i postupcima, neprijateljskim taktikama, informacije o počiniteljima prijetnji, kibernetička sigurnosna upozorenja i preporuke o konfiguraciji kibernetičkih sigurnosnih alata za otkrivanje kibernetičkih napada. Osim toga, prekogranični kibernetički centri trebali bi međusobno sklapati sporazume o suradnji. U tim sporazumima o suradnji posebno bi trebalo utvrditi načela dijeljenja informacija i interoperabilnost. Za njihove odredbe o interoperabilnosti, posebno u pogledu formata i protokola za dijeljenje informacija, trebalo bi se voditi smjernicama o interoperabilnosti koje izdaje Agencija Europske unije za kibersigurnost osnovana Uredbom (EU) 2019/881 (ENISA) i koje bi za te odredbe trebale služiti kao polazište. Te bi smjernice trebalo brzo izdati kako bi se osiguralo da ih prekogranični kibernetički centri mogu primijeniti u ranoj fazi. U njima bi se trebali uzeti u obzir međunarodni standardi i najbolje prakse te funkcioniranje eventualno uspostavljenih prekograničnih kibernetičkih centara.

(20) Prekogranični kibernetički centri i mreža CSIRT-ova trebali bi blisko surađivati kako bi se osigurale sinergije i komplementarnost aktivnosti. Oni bi u tu svrhu trebali postići dogovor o postupovnim aranžmanima za suradnju i dijeljenje relevantnih informacija. To bi moglo uključivati dijeljenje relevantnih informacija o kibernetičkim prijetnjama i značajnim kibernetičkim sigurnosnim incidentima te osiguravanje da se iskustva s najsuvremenijim alatima, posebno umjetnom inteligencijom i tehnologijom analitike podataka, koji se upotrebljavaju u prekograničnim kibernetičkim centrima, dijele s mrežom CSIRT-ova.

(21) Zajednička informiranost o stanju relevantnih tijela nužan je preduvjet za pripravnost i koordinaciju na razini Unije u pogledu značajnih kibernetičkih sigurnosnih incidenata i kibernetičkih sigurnosnih incidenata velikih razmjera. Direktivom (EU) 2022/2555 uspostavljena je mreža EU-CyCLONe radi podupiranja koordiniranog upravljanja kibernetičkim sigurnosnim incidentima i krizama velikih razmjera na operativnoj razini te osiguravanja redovite razmjene relevantnih informacija među državama članicama i institucijama, tijelima, uredima i agencijama Unije. Direktivom (EU) 2022/2555 također je uspostavljena mreža CSIRT-ova u cilju promicanja brze i djelotvorne operativne suradnje među svim državama članicama. Kako bi se osigurala informiranost o stanju i ojačala solidarnost, kada prekogranični kibernetički centri dobiju informacije povezane s potencijalnim ili aktualnim kibernetičkim sigurnosnim incidentom velikih razmjera, oni bi trebali relevantne informacije proslijediti mreži CSIRT-ova te, kao rano upozorenje, obavijestiti mrežu EU-CyCLONe. Osobito, 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 kibernetičkom sigurnosnom incidentu velikih razmjera. U tom bi kontekstu dužnu pozornost trebalo posvetiti načelu nužnosti pristupa podacima i potencijalno osjetljivoj prirodi informacija koje se dijele. U Direktivi (EU) 2022/2555 ponovno se ukazuje na odgovornosti Komisije u okviru Mehanizma Unije za civilnu zaštitu uspostavljenog Odlukom 1313/2013/EU Europskog parlamenta i Vijeća[13], kao i na njezinu odgovornost za dostavljanje analitičkih izvješća za aranžmane EU-a za integrirani politički odgovor na krizu („aranžmani za IPCR”) u skladu s Provedbenom odlukom Vijeća (EU) 2018/1993[14].

---

13 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., ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 Provedben odluka Vijeća (EU) 2018/1993 od 11. prosinca 2018. o aranžmanima EU-a za integrirani politički odgovor na krizu (SL L 320, 17.12.2018., str. 28., ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Kada prekogranični kibernetički centri s mrežom EU-CyCLONe i mrežom CSIRT-ova dijele relevantne informacije i rana upozorenja o potencijalnom ili aktualnom kibernetičkom sigurnosnom incidentu velikih razmjera, nužno je da se te informacije putem tih mreža dijele s tijelima država članica kao i s Komisijom. U tom se pogledu Direktivom (EU) 2022/2555 predviđa da je svrha mreže EU-CyCLONe podupiranje koordiniranog upravljanja kibernetičkim sigurnosnim incidentima i krizama velikih razmjera na operativnoj razini te osiguravanje redovite razmjene relevantnih informacija među državama članicama i institucijama, tijelima, uredima i agencijama Unije. Zadaće mreže EU-CyCLONe uključuju razvoj zajedničke informiranosti o stanju u pogledu takvih incidenata i kriza. Od ključne je važnosti da EU-CyCLONe osigura, u skladu s tom svrhom i svojim zadaćama, da se takve informacije odmah pružaju relevantnim predstavnicima država članica i Komisijom. U tu je svrhu ključno da poslovnik mreže EU-CyCLONe sadržava odgovarajuće odredbe.

(22) Subjekti koji sudjeluju u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti trebali bi osigurati visoku razinu međusobne interoperabilnosti, uključujući, prema potrebi, formata podataka, taksonomije, alata za obradu i analitiku podataka. Trebali bi osigurati i sigurne komunikacijske kanale, minimalnu razinu sigurnosti aplikacijskog sloja, pregled informiranosti o stanju i pokazatelje. Pri donošenju zajedničke taksonomije i izradi predložaka za izvješća o stanju u kojima se opisuju uzroci otkrivenih kibernetičkih prijetnji i i rizika trebalo bi uzeti u obzir rezultate rada koji je već obavljen u kontekstu provedbe Direktive (EU) 2022/2555.

(23) Kako bi se omogućilo da se opsežna razmjena relevantnih podataka i informacija o kibernetičkim prijetnjama iz različitih izvora odvija u pouzdanom i sigurnom okruženju, subjekti koji sudjeluju u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti trebali bi raspolagati najsuvremenijim, vrlo sigurnim alatima, opremom i infrastrukturom, kao i kvalificiranim osobljem. 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.

(24) Prikupljanjem, analiziranjem, dijeljenjem i razmjenom relevantnih podataka i informacija europski sustav uzbunjivanja u području kibernetičke sigurnosti trebao bi povećati tehnološku suverenost i otvorenu stratešku autonomiju Unije u području kibernetičke sigurnosti te njezinu konkurentnost i otpornost. Objedinjavanje visokokvalitetnih, prilagođenih podataka moglo bi doprinijeti i razvoju naprednih tehnologija umjetne inteligencije i analitike podataka. Ljudski nadzor, a u tu svrhu kvalificirana radna snaga, i dalje su ključni za djelotvorno objedinjavanje visokokvalitetnih podataka.

(25) Iako je europski sustav uzbunjivanja u području kibernetičke sigurnosti civilni projekt, zajednica u području kibernetičke obrane mogla bi imati koristi od snažnijih sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture.

(26) Dijeljenje informacija među sudionicima europskog sustava uzbunjivanja u području kibernetičke sigurnosti 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 više ne budu potrebni za navedenu svrhu i obavijestiti subjekt koji je stavio podatke na raspolaganje da su podaci uništeni.

(27) Očuvanje povjerljivosti i sigurnosti informacija ključno je za sva tri stupa ove Uredbe, i to za poticanje dijeljena ili razmjene informacija u kontekstu europskog sustava uzbunjivanja u području kibernetičke sigurnosti, zaštitu interesa subjekata koji podnose zahtjev za potporu u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije ili osiguravanje da izvješća u okviru europskog mehanizma za istraživanje kibernetičkih sigurnosnih incidenata mogu proizvesti korisne pouke bez negativnog učinka na subjekte pogođene incidentima. Sudjelovanje država članica i subjekata u tim mehanizmima ovisi o odnosu povjerenja među njihovim komponentama. Ako su određene informacije povjerljive u skladu s pravilima Unije ili nacionalnim pravilima, dijeljene ili razmjena tih informacija na temelju ove Uredbe trebala bi biti ograničena na ono što je relevantno i razmjerno svrsi dijeljenja ili razmjene. Pri dijeljenju ili razmjeni štiti se i povjerljivost tih informacija, što uključuje i zaštitu sigurnosti i komercijalnih interesa svih predmetnih subjekata. Dijeljenje ili razmjena informacija na temelju ove Uredbe mogla bi se odvijati na temelju sporazuma o povjerljivosti ili smjernica o distribuciji informacija kao što je Protokol o semaforu. Protokol o semaforu treba shvatiti kao sredstvo za pružanje informacija o svim ograničenjima u pogledu daljnjeg širenja informacija. Upotrebljava se u gotovo svim CSIRT-ovima i u nekim ISAC-ovima. Povrh tih općih zahtjeva, kada je riječ o europskom sustavu uzbunjivanja u području kibernetičke sigurnosti, sporazumima konzorcija domaćina trebala bi se utvrditi posebna pravila o uvjetima za dijeljenje informacija u okviru predmetnog prekograničnog kibernetičkog centra. Tim bi se sporazumima posebice moglo zahtijevati da se informacije dijele samo u skladu s pravom Unije i nacionalnim pravom.

(28) Kada je riječ o primjeni pričuve EU-a za kibernetičku sigurnost, potrebna su posebna pravila o povjerljivosti. Potpora će se tražiti, procjenjivati i pružati u kontekstu krize te za subjekte koji djeluju u osjetljivim sektorima. Kako bi pričuva djelotvorno funkcionirala, ključno je da korisnici i subjekti mogu dijeliti sve informacije koje su svakom subjektu potrebne kako bi ispunio svoju ulogu u procjeni zahtjeva i primjeni potpore te da mogu bez odgode omogućiti pristup tim informacijama. U skladu s tim, ovom bi Uredbom trebalo predvidjeti da se sve takve informacije upotrebljavaju ili dijele samo ako je to potrebno za rad pričuve EU-a za kibernetičku sigurnost te da bi se informacije koje su povjerljive ili klasificirane u skladu spravom Unije i nacionalnim pravom upotrebljavaju i dijele samo u skladu s tim pravom. Osim toga, korisnici bi trebali moći, prema potrebi, upotrebljavati protokole za dijeljenje informacija kao što je Protokol o semaforu kako bi dodatno utvrdili ograničenja. Iako korisnici imaju diskrecijsko pravo u tom pogledu, važno je da pri primjeni takvih ograničenja vode računa o mogućim posljedicama, posebno u pogledu kašnjenja procjene ili isporuke traženih usluga. Kako bi se osigurala učinkovita pričuva EU-a za kibernetičku sigurnost, važno je da javni naručitelj pojasni te posljedice korisniku prije nego što podnese zahtjev. Te su zaštitne mjere ograničene na traženje i pružanje usluga pričuve EU-a za kibernetičku sigurnost i ne utječu na razmjenu informacija u drugim kontekstima, kao što je nabava pričuve EU-a za kibernetičku sigurnost.

(29) S obzirom na sve veće rizike i sve veći broj incidenata koji pogađaju države članice, potrebno je uspostaviti instrument za potporu u kriznim situacijama, odnosno mehanizam za izvanredne kibernetičke sigurnosne situacije, kako bi se poboljšala otpornost Unije na značajne kibernetičke sigurnosne incidente, kibernetičke sigurnosne incidente velikih razmjera i kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera te dopunile mjere država članica hitnom financijskom potporom za pripravnost, odgovor na incidente i inicijalni oporavak osnovnih usluga. Budući da je potpuni oporavak od incidenta sveobuhvatan postupak u kojem se funkcioniranje subjekta pogođenog incidentom vraća u stanje iz razdoblja prije incidenta te to može biti dugotrajan proces sa znatnim troškovima, potpora iz pričuve EU-a za kibernetičku sigurnost trebala bi biti ograničena na inicijalnu fazu procesa oporavka, što bi rezultiralo ponovnom uspostavom osnovnih funkcionalnosti sustava. Mehanizmom za izvanredne kibernetičke sigurnosne situacije trebalo bi omogućiti brzo i djelotvorno pružanje pomoći u definiranim okolnostima i pod jasnim uvjetima te omogućiti pažljivo praćenje i evaluacija uporabe sredstava. Iako glavnu odgovornost za sprečavanje incidenata i kriza te pripravnost i odgovor na njih imaju države članice, mehanizmom za izvanredne kibernetičke sigurnosne situacije promiče se solidarnost među državama članicama u skladu s člankom 3. stavkom 3. Ugovora o Europskoj uniji (UEU).

(30) Mehanizmom za izvanredne kibernetičke sigurnosne situacije trebala bi se pružiti potpora državama članicama kojom se dopunjavaju njihove vlastite mjere i resursi te druge postojeće mogućnosti potpore u slučaju odgovora na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera i inicijalnog oporavka od njih, kao što su usluge koje pruža ENISA u skladu sa svojim mandatom, koordinirani odgovor i pomoć mreže CSIRT-ova, potpora za ublažavanje posljedica koju pruža mreža EU-CyCLONe, te uzajamna pomoć među državama članicama među ostalim u kontekstu članka 42. stavka 7. UEU-a i timove za brz odgovor na kibernetičke incidente u okviru PESCO-a uspostavljenih na temelju Odluke Vijeća (ZVSP) 2017/20315[15]. Njime bi se trebalo odgovoriti na potrebu da se osigura dostupnost specijaliziranih sredstava za potporu pripravnosti i odgovoru na kibernetičke sigurnosne incidente i oporavku od njih u cijeloj Uniji i u trećim zemljama pridruženima programu Digitalna Europa.

[15] Odluka Vijeća (ZVSP) 2017/2315 od 11. prosinca 2017. o uspostavi stalne strukturirane suradnje (PESCO) i utvrđivanju popisa država članica sudionica (SL L 331, 14.12.2017., str. 57., ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Ovom se Uredbom ne dovode u pitanje postupci i okviri za koordinaciju odgovora na krizu na razini Unije, posebno Direktiva (EU) 2022/2555, Mehanizam Unije za civilnu zaštitu uspostavljen Odlukom br. 1313/2013/EU Europskog parlamenta i Vijeća[16], aranžmani za IPCR i Preporuka Komisije (EU) 2017/1584[17]. Potpora koja se pruža u okviru mehanizma za izvanredne kibernetičke sigurnosne 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 kibernetičke incidente, uzimajući u obzir civilnu prirodu mehanizma za izvanredne kibernetičke sigurnosne situacije. Potpora koja se pruža u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije može dopuniti djelovanja koja se provode u kontekstu članka 42. stavka 7. UEU-a, uključujući pomoć koju jedna država članica pruža drugoj državi članici, ili biti dio zajedničkog odgovora Unije i država članica ili u situacijama iz članka 222. UFEU-a. Provedbu ove Uredbe trebalo bi, prema potrebi, koordinirati i s provedbom mjera u okviru alata za kibernetičku diplomaciju.

---

16 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.).

17 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.).

(32) Pomoć koja se pruža na temelju ove Uredbe trebala bi doprinositi djelovanjima koje države članice poduzimaju na nacionalnoj razini i nadopunjavati ih. U tu bi svrhu trebalo osigurati blisku suradnju i savjetovanje između Komisije, ENISA-e, država članica i, ako je relevantno, ECCC-a. Pri podnošenju zahtjeva za potporu u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije države članice trebale bi dostaviti relevantne informacije kojima se obrazlaže potreba za potporom.

(33) Prema Direktivi (EU) 2022/2555 države članice dužne su imenovati ili uspostaviti jedno ili više tijela za upravljanje kibernetičkim krizama i osigurati da ta tijela imaju odgovarajuće resurse za djelotvorno i učinkovito obavljanje svojih zadaća. Isto su tako države članice dužne utvrditi sposobnosti, sredstva i postupke koji se mogu primijeniti u slučaju krize te donijeti nacionalni plan za odgovor na kibernetičke sigurnosne incidente velikih razmjera i krize u kojem su utvrđeni ciljevi i načini upravljanja kibernetičkim sigurnosnim incidentima i krizama velikih razmjera. Države članice dužne su uspostaviti 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 da im osiguraju odgovarajuće resurse za djelotvorno 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 izvanredne kibernetičke sigurnosne situacije trebala bi se pružiti pomoć za djelovanja usmjerena na jačanje pripravnosti i djelovanja za odgovor na incidente kako bi se ublažile posljedice značajnih kibernetičkih sigurnosnih incidenata i kibernetičkih sigurnosnih incidenata velikih razmjera, podržao inicijalni oporavak ili ponovno uspostavile osnovne funkcionalnosti usluga koje pružaju subjekti koji djeluju u sektorima visoke kritičnosti ili subjekti koji posluju u drugim kritičnim sektorima.

(34) U okviru djelovanja u području pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu testiranju i procjeni kibernetičke sigurnosti subjekata koji djeluju u sektorima visoke kritičnosti utvrđenima u skladu s Direktivom (EU) 2022/2555, na koordiniran način, uključujući preko vježbi i osposobljavanja. U tu bi svrhu Komisija, nakon savjetovanja s ENISA-om, skupinom za suradnju NIS i mrežom EU-CyCLONe, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje pripravnosti na razini Unije. Sektore ili podsektore trebalo bi odabrati iz sektora visoke kritičnosti navedenih u Prilogu I. Direktivi (EU) 2022/2555. Koordinirano testiranje pripravnosti trebalo bi se temeljiti na zajedničkim scenarijima rizika i metodologijama.

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 udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju razine kibernetičke sigurnosti Europske unije u pogledu kiberprostora koje provode Komisija, Visoki predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”) i skupina za suradnju NIS, u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, kao i procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela skupina za suradnju NIS, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za elektroničke komunikacije osnovanog Uredbom (EU) 2018/1971 Europskog parlamenta i Vijeća[18], koordinirane procjene rizika ključnih lanaca opskrbe na razini Unije koja se provodi na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća[19]. Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

---

[18] Uredba (EU) 2018/1971 Europskog parlamenta i Vijeća od 11. prosinca 2018.o osnivanju Tijela europskih regulatora za elektroničke komunikacije (BEREC) i Agencije za potporu BEREC-u (Ured BEREC-a), izmjeni Uredbe (EU) 2015/2120 i stavljanju izvan snage Uredbe (EZ) br. 1211/2009 (SL L 321, 17.12.2018., str. 1.).

[19] 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 (SL L 333, 27.12.2022., str. 1.).

(35) Osim toga, mehanizmom za izvanredne kibernetičke sigurnosne situacije trebala bi se pružati potpora drugim djelovanjima u području pripravnosti i podupirati pripravnost u drugim sektorima koji nisu obuhvaćeni koordiniranim testiranjem pripravnosti subjekata koji djeluju u sektorima visoke kritičnosti ili subjekata koji djeluju u drugim kritičnim sektorima. Ta bi djelovanja mogla uključivati različite vrste aktivnosti u području nacionalne pripravnosti.

(36) Kada države članice prime bespovratna sredstva za potporu djelovanjima u području pripravnosti, subjekti u sektorima visoke kritičnosti mogu dobrovoljno sudjelovati u tim djelovanjima. Dobra je praksa da nakon takvih djelovanja subjekti koji sudjeluju sastave korektivni plan za provedbu svih preporuka za poduzimanje posebnih mjera koje iz toga proizlaze kako bi imali što više koristi od tog djelovanja u području pripravnosti. Iako je važno da države članice u okviru djelovanja zatraže da subjekti koji sudjeluju sastave i provedu takve korektivne planove, države članice ova Uredba ne obvezuje niti ovlašćuje za izvršavanje takvih zahtjeva. Takvim zahtjevima ne dovode se u pitanje zahtjevi za subjekte i nadzorne ovlasti nadležnih tijela u skladu s Direktivom (EU) 2022/2555.

(37) Mehanizmom za izvanredne kibernetičke sigurnosne situacije trebala bi se pružati i potpora mjerama za odgovor na incidente kako bi se ublažio učinak značajnih kibernetičkih sigurnosnih incidenata, kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih sigurnosnih incidenata ekvivalentnih kibernetičkom incidentu velikih razmjera, podržao inicijalni 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 učinak incidenata na građane.

(38) Mehanizmom za izvanredne kibernetičke sigurnosne situacije trebala bi se podupirati tehnička pomoć koju jedna država članica pruža drugoj državi članici pogođenoj značajnim kibernetičkim sigurnosnim incidentom ili kibernetičkim sigurnosnim incidentom velikih razmjera, uključujući CSIRT-ove iz članka 11. stavka 3. točke (f) Direktive (EU) 2022/2555. Državama članicama koje pružaju takvu 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 kibernetičku sigurnost.

(39) S obzirom na ključnu ulogu koju privatna poduzeća imaju u otkrivanju kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih sigurnosnih incidenata ekvivalentnih kibernetičkom sigurnosnom incidentu velikih razmjera te pripravnosti i odgovoru na njih, važno je prepoznati vrijednost dobrovoljne pro bono suradnje s takvim poduzećima, pri čemu ona nude usluge bez naknade u slučaju kibernetičkih sigurnosnih incidenata i velikih razmjera i krizama te kibernetičkih sigurnosnih incidenata i kriza ekvivalentnih kibernetičkim sigurnosnim incidentima i krizama velikih razmjera. ENISA bi u suradnji s mrežom EU-CyCLONe mogla pratiti razvoj takvih pro bono inicijativa i promicati njihovu usklađenost s kriterijima koji se primjenjuju na pouzdane pružatelje upravljanih sigurnosnih usluga u skladu s ovom Uredbom, među ostalim u pogledu pouzdanosti privatnih poduzeća, njihova iskustva i sposobnosti sigurnog postupanja s osjetljivim informacijama.

(40) U okviru mehanizma za izvanredne kibernetičke sigurnosne situacije na razini Unije trebalo bi postupno uspostaviti pričuvu EU-a za kibernetičku sigurnost koja bi se sastojala od usluga pouzdanih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i pokrenula djelovanja za oporavak u slučaju značajnih kibernetičkih sigurnosnih incidenata, kibernetičkih sigurnosnih incidenata velikih razmjera ili kibernetičkih sigurnosnih incidenta ekvivalentnih kibernetičkom sigurnosnom incidentu velikih razmjera koji pogađaju države članice, institucije, tijela, urede ili agencije Unije ili treće zemlje pridružene programu Digitalna Europa. Pričuva EU-a za kibernetičku sigurnost trebala bi osigurati dostupnost i spremnost usluga. Stoga bi trebala uključivati usluge koje su preuzete unaprijed, uključujući, na primjer, kapacitete koji su u stanju pripravnosti i mogu se rasporediti u kratkom roku. Usluge iz pričuve EU-a za kibernetičku sigurnost trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima koji djeluju u sektorima visoke kritičnosti **ili** pogođenim subjektima koji djeluju u drugim sektorima kritičnim sektorima kao nadopuna njihovim vlastitim djelovanjima na nacionalnoj razini. Usluge iz pričuve EU-a za kibernetičku sigurnost trebale bi moći služiti i za potporu institucijama, tijelima, uredima i agencijama Unije pod sličnim uvjetima. Pričuva EU-a za kibernetičku sigurnost mogla bi pridonijeti i jačanju konkurentnog položaja industrije i usluga u Uniji u cijelom digitalnom gospodarstvu, uključujući mikropoduzeća te mala i srednja poduzeća te novoosnovana poduzeća, među ostalim pružanjem poticaja za ulaganja u istraživanje i inovacije. Pri nabavi usluga za pričuvu EU-a za kibernetičku sigurnost važno je uzeti u obzir ENISA-in Europski okvir vještina u području kibernetičke sigurnosti. Pri podnošenju zahtjeva za potporu iz pričuve EU-a za kibernetičku sigurnost korisnici bi u svoj zahtjev trebali uključiti odgovarajuće informacije o pogođenom subjektu i mogućem učinku, informacije o zatraženoj usluzi iz pričuve EU-a za kibernetičku sigurnost, i vrstu potpore pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni podnositeljeva zahtjeva. Kako bi se osigurala komplementarnost s drugim oblicima potpore koji su dostupni pogođenom subjektu, zahtjev bi također trebao uključivati, ako su dostupne, informacije o uspostavljenim ugovornim aranžmanima za usluge za odgovor na incidente i inicijalni oporavak, kao i ugovore o osiguranju koji bi mogli obuhvaćati takvu vrstu incidenta.

(41) Kako bi se osigurala djelotvorna upotreba financijskih sredstava Unije, prethodno namijenjene usluge u okviru pričuve EU-a za kibernetičku sigurnost trebalo bi, u skladu s relevantnim ugovorom, pretvoriti u usluge pripravnosti povezane sa sprečavanjem incidenata i odgovorom na njih, u slučaju da se te usluge za koje su prethodno namijenjene usluge ne upotrebljavaju za odgovor na incidente tijekom razdoblja za koje su prethodno namijenjene. Te bi usluge trebale biti komplementarne te ne bi trebale duplicirati djelovanja u području pripravnosti kojima upravlja ECCC.

(42) Zahtjeve za potporu iz pričuve EU-a za kibernetičku sigurnost od tijela država članica za upravljanje kibernetičkim krizama i CSIRT-ova, ili CERT-EU-a, u ime institucija, tijela, ureda i agencija Unije trebao bi ocjenjivati javni naručitelj. Ako je ENISA-i povjereno upravljanje pričuvom EU-a za kibernetičku sigurnost i njezino djelovanje, ENISA je taj javni naručitelj. Komisija bi trebala ocijeniti zahtjeve trećih zemalja pridruženih programu Digitalna Europa za potporu. Kako bi se olakšalo podnošenje i procjena zahtjeva za potporu, ENISA bi mogla uspostaviti sigurnu platformu.

(43) Ako se zaprimi više istodobnih zahtjeva, tim bi zahtjevima trebalo dati prednost u skladu s kriterijima utvrđenima u ovoj Uredbi. S obzirom na opće ciljeve ove Uredbe, ti bi kriteriji trebali uključivati razmjer i ozbiljnost incidenta, vrstu pogođenog subjekta, mogući učinak incidenta na pogođene države članice i korisnike, moguću prekograničnu prirodu incidenta i rizik od širenja, kao i mjere koje je korisnik već poduzeo kako bi pomogao u odgovoru i inicijalnom oporavku. S obzirom na te iste ciljeve i s obzirom na to da su zahtjevi korisnika iz država članica namijenjeni isključivo pružanju potpore u cijeloj Uniji subjektima koji djeluju u sektorima visoke kritičnosti ili subjektima koji djeluju u drugim kritičnim sektorima, primjereno je dati veći prioritet zahtjevima država članica ako ti kriteriji dovode do toga da se dva ili više zahtjeva ocijene jednakima. Time se ne dovode u pitanje obveze koje države članice mogu imati na temelju relevantnih ugovora o smještaju da poduzmu mjere za zaštitu i pomoć institucijama, tijelima, uredima i agencijama Unije.

(44) Komisija bi općenito trebala biti odgovorna za provedbu pričuve EU-a za kibernetičku sigurnost. S obzirom na bogato iskustvo koje je ENISA stekla u pogledu djelovanja za potporu kibernetičkoj sigurnosti, ENISA je najprikladnija agencija za provedbu pričuve EU-a za kibernetičku sigurnost. Stoga bi Komisija ENISA-i trebala povjeriti rad pričuve EU-a za kibernetičku sigurnost i upravljanje njome djelomično ili, ako to Komisija smatra primjerenim, u cijelosti. Povjeravanje bi se trebalo provoditi u skladu s primjenjivim pravilima iz Uredbe (EU, Euratom) 2024/2509, a posebno bi trebalo podlijegati ispunjenju relevantnih uvjeta za potpisivanje sporazuma o doprinosu. Svi aspekti rada pričuve EU-a za kibernetičku sigurnost i upravljanja njome koji nisu povjereni ENISA-i trebali bi podlijegati izravnom upravljanju Komisije, među ostalim i prije potpisivanja sporazuma o doprinosu.

(45) Države članice trebale bi imati ključnu ulogu u uspostavi, uvođenju i nakon uvođenja pričuve EU-a za kibernetičku sigurnost. Budući da je Uredba (EU) 2021/694 relevantan temeljni akt za djelovanja za provedbu pričuve EU-a za kibernetičku sigurnost, djelovanja u okviru pričuve EU-a za kibernetičku sigurnost trebalo bi predvidjeti u programima rada iz članka 24. Uredbe (EU) 2021/694. Na temelju stavka 6. tog članka Komisija te programe donosi provedbenim aktima u skladu s postupkom ispitivanja. Nadalje, Komisija bi u suradnji sa skupinom za suradnju NIS trebala utvrditi prioritete i razvoj pričuve EU-a za kibernetičku sigurnost.

(46) Ugovori sklopljeni u okviru pričuve EU-a za kibernetičku sigurnost ne bi trebali utjecati na odnos među poduzećima i već postojeće obveze između zahvaćenog subjekta ili korisnika i pružatelja usluga.

(47) U svrhu odabira privatnih pružatelja usluga koji će pružati usluge u kontekstu pričuve EU-a za kibernetičku sigurnost potrebno je utvrditi skup minimalnih kriterija i zahtjeva koje bi trebalo uključiti u poziv na podnošenje ponuda za odabir tih pružatelja, kako bi se osiguralo da su ispunjene potrebe tijela država članica, subjekata koji djeluju u sektorima visoke kritičnosti ili subjekata koji djeluju u drugim kritičnim sektorima. Kako bi se odgovorilo na posebne potrebe država članica, pri nabavi usluga za pričuvu EU-a za kibernetičku sigurnost, javni naručitelj trebao bi, prema potrebi, razviti kriterije za odabir i zahtjeve dodatne uz one utvrđene u ovoj Uredbi. Važno je poticati sudjelovanje manjih pružatelja usluga aktivnih na regionalnoj i lokalnoj razini.

(48) Pri odabiru pružatelja za uključivanje u pričuvu EU-a za kibernetičku sigurnost javni naručitelj trebao bi nastojati osigurati da pričuva EU-a za kibernetičku sigurnost, kad se promatra kao cjelina, sadržava pružatelje koji mogu ispuniti jezične zahtjeve korisnika. U tu bi svrhu javni naručitelj prije pripreme natječajnih specifikacija trebao ispitati imaju li potencijalni korisnici pričuve EU-a za kibernetičku sigurnost posebne jezične zahtjeve kako bi se usluge potpore u okviru pričuve EU-a za kibernetičku sigurnost mogle pružati na jednom od službenih jezika institucija Unije ili država članica koji će pogođeni korisnik ili subjekt vjerojatno razumjeti. Ako korisnik za pružanje usluga potpore u okviru pričuve EU-a za kibernetičku sigurnost zahtijeva više od jednog jezika, a te su usluge nabavljene za tog korisnika na tim jezicima, korisnik bi u zahtjevu za pričuvnu potporu trebao moći navesti na kojem bi od tih jezika usluge trebalo pružati u vezi s konkretnim incidentom zbog kojeg je podnesen zahtjev.

(49) Kako bi pridonijela uspostavi pričuve EU-a za kibernetičku sigurnost, važno je da Komisija od ENISA-e zatraži izradu prijedloga programa kibernetičke sigurnosne certifikacije kandidata na temelju Uredbe (EU) 2019/881 u područjima obuhvaćenima mehanizmom za izvanredne kibernetičke sigurnosne situacije.

(50) 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 kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera, Komisija ili mreža EU-CyCLONe trebali bi moći zatražiti od ENISA-e, uz potporu mreže CSIRT-ova i uz odobrenje dotične države članice, da istraži i procijeni kibernetičke prijetnje, poznate iskoristive ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibernetički sigurnosni incident ili kibernetički sigurnosni incidentom velikih razmjera. Nakon završetka istraživanja i procjenjivanja incidenta ENISA bi trebala pripremiti izvješće o istraživanju incidenta u suradnji s dotičnom državom članicom, relevantnim dionicima, uključujući predstavnike iz privatnog sektora, Komisijom i drugim relevantnim institucijama, tijelima, uredima i agencije Unije. Na temelju suradnje s dionicima, uključujući privatni sektor, izvješće o istraživanju određenih incidenata trebalo bi biti usmjereno na procjenu uzroka, učinka i ublažavanje 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 mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji te bi ih oni trebali uzeti u obzir u svojem radu i radu ENISA-e. Ako se incident odnosi na treću zemlju pridruženu programu Digitalna Europa, Komisija bi izvješće trebala dostaviti i Visokom predstavniku.

(51) Uzimajući u obzir nepredvidivu prirodu kibernetičkih napada i činjenicu da ti napadi često nisu ograničeni na određeno zemljopisno područje te da postoji visok rizik od širenja, jačanje otpornosti susjednih zemalja i njihove sposobnosti da djelotvorno odgovore na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera doprinosi zaštiti Unije, a posebno njezina unutarnjeg tržišta i industrije, u cjelini. Takve aktivnosti mogle bi dodatno doprinijeti kibernetičkoj diplomaciji Unije. Stoga bi treće zemlje pridružene programu Digitalna Europa trebale moći primiti potporu iz pričuve EU-a za kibernetičku sigurnost na cijelom svojem državnom području ili dijelu njihova državnog područja ako je to predviđeno sporazumom kojim je ta treća zemlja pridružena programu Digitalna Europa. Unija bi trebala podupirati financiranje trećih zemalja pridruženih programu Digitalna Europa u okviru relevantnih partnerstava i instrumenata financiranja za te zemlje. Potpora bi trebala obuhvaćati usluge za odgovor na značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera te započinjanje oporavka od njih.

(52) Uvjeti za pričuvu EU-a za kibernetičku sigurnost i pouzdane pružatelje upravljanih sigurnosnih usluga utvrđeni u ovoj Uredbi trebali bi se primjenjivati pri pružanju potpore trećim zemljama pridruženima programu Digitalna Europa. Treće zemlje pridružene programu Digitalna Europa trebale bi moći zatražiti potporu iz pričuve EU-a za kibernetičku sigurnost ako su ciljani subjekti za koje traže potporu iz pričuve EU-a za kibernetičku sigurnost subjekti koji djeluju u sektorima visoke kritičnosti ili subjekti koji djeluju u drugim kritičnim sektorima i ako otkriveni incidenti dovode do znatnih poremećaja u radu ili bi mogli imati učinke širenja u Uniji. Treće zemlje pridružene programu Digitalna Europa trebale bi biti prihvatljive za primanje potpore samo ako je takva potpora izričito predviđena sporazumom kojim su pridružene programu Digitalna Europa. Osim toga, takve treće zemlje trebale bi ostati prihvatljive samo ako su ispunjena tri kriterija. Prvo, treća zemlja trebala bi u potpunosti poštovati relevantne uvjete tog sporazuma. Drugo, s obzirom na komplementarnu prirodu pričuve EU-a za kibernetičku sigurnost, treća zemlja trebala je poduzeti odgovarajuće korake za pripremu za značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera. Treće, pružanje potpore iz pričuve EU-a za kibernetičku sigurnost trebalo bi biti u skladu s politikom Unije prema toj zemlji i sveukupnim odnosima s tom zemljom te u skladu s drugim politikama Unije u području sigurnosti. U kontekstu svoje procjene usklađenosti s tim trećim kriterijem Komisija bi se trebala savjetovati s Visokim predstavnikom radi usklađivanja dodjele takve potpore sa zajedničkom vanjskom i sigurnosnom politikom.

(53) Pružanje potpore trećim zemljama pridruženima programu Digitalna Europa može utjecati na odnose s trećim zemljama i sigurnosnu politiku Unije, među ostalim u kontekstu zajedničke vanjske i sigurnosne politike te zajedničke obrambene i sigurnosne politike. Stoga je primjereno da se Vijeću dodijele provedbene ovlasti za odobravanje i određivanje razdoblja tijekom kojeg se takva potpora može pružiti. Vijeće bi trebalo djelovati na temelju prijedloga Komisije, uzimajući u obzir Komisijinu procjenu triju kriterija. Isto bi trebalo vrijediti i za produljenja i za prijedloge za izmjenu ili ostavljanje izvan snage takvih akata. Ako u iznimnim okolnostima Vijeće smatra da je došlo do znatne promjene okolnosti u odnosu na treći kriterij, Vijeće bi trebalo moći djelovati na vlastitu inicijativu radi izmjene ili stavljanja izvan snage akta, a da ne čeka prijedlog Komisije. Takve znatne promjene vjerojatno će zahtijevati hitno djelovanje koje će imati posebno važne posljedice za odnose s trećim zemljama i neće zahtijevati prethodnu detaljnu procjenu Komisije. Nadalje, Komisija bi trebala surađivati s Visokim predstavnikom u pogledu zahtjeva za potporu trećih zemalja pridruženih programu Digitalna Europa i provedbi potpore koja se odobrava takvim trećim zemljama. Komisija bi trebala uzeti u obzir i sva stajališta ENISA-e o tim zahtjevima i potpori. Komisija bi trebala obavijestiti Vijeće o ishodu procjene zahtjeva, uključujući relevantna razmatranja u tom pogledu, i o uslugama koje se uvode.

(54) U komunikaciji Komisije od 18. travnja 2023. o Akademiji za vještine u području kibersigurnosti prepoznat je nedostatak kvalificiranih stručnjaka. Takve su vještine potrebne za postizanje ciljeva ove Uredbe. Uniji su hitno potrebni stručnjaci s vještinama i kompetencijama za sprečavanje, otkrivanje, odvraćanje od kibernetičkih napada i obranu Unije, među ostalim njezine najkritičnije infrastrukture, od takvih napada i osiguravanja njezine otpornosti. U tu je svrhu važno poticati suradnju među dionicima, uključujući iz privatnog sektora, akademske zajednice i javnog sektora. Jednako je važno stvoriti sinergije na svim područjima Unije kako bi se ulaganjem u obrazovanje i osposobljavanje promicalo stvaranje zaštitnih mjera kako bi se izbjegao odljev mozgova ili povećavanje nedostatka vještina u nekim regijama ne poveća više nego u drugima. Hitno je potrebno premostiti nedostatak vještina u području kibernetičke sigurnosti, s posebnim naglaskom na smanjenju rodnog jaza u radnoj snazi u području kibernetičke sigurnosti kako bi se promicala prisutnost i sudjelovanje žena u osmišljavanju digitalnog upravljanja.

(55) Kako bi se potaknule inovacije na jedinstvenom digitalnom tržištu, važno je ojačati istraživanja i inovacije u području kibernetičke sigurnosti radi doprinošenja povećanju otpornosti država članica i otvorenoj strateškoj autonomiji Unije, što su ciljevi ove Uredbe. Sinergije su ključne za jačanje suradnje i koordinacije među različitim dionicima, uključujući iz privatnog sektora, civilnog društva i akademske zajednice.

(56) Ovom bi se Uredbom trebala uzeti u obzir obveza iz zajedničke deklaracije od 26. siječnja 2022. Europskog parlamenta, Vijeća i Komisije pod naslovom „Europska deklaracije o digitalnim pravima i načelima za digitalno desetljeće" koja je povezana sa zaštitom interesa demokracija, ljudi, poduzeća i javnih institucija u Uniji od kibernetičkih sigurnosnih rizika i kibernetičkog kriminaliteta, uključujući povrede podataka i krađu identiteta ili manipulaciju njime.

(57) Kako bi se dopunili određeni elementi ove Uredbe koji nisu ključni, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. UFEU-a kako bi se utvrdile vrste i broj usluga odgovora potrebnih za pričuvu EU-a za kibernetičku sigurnost. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.[20]. Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

[20] SL L 123, 12.5.2016., str. 1., ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.

(58) Radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe, Komisiji bi trebalo dodijeliti provedbene ovlasti za dodatno utvrđivanje detaljnih postupovnih aranžmana za dodjelu usluga potpore pričuve EU-a za kibernetičku sigurnost. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća[21].

(59) Ne dovodeći u pitanje pravila koja se odnose na godišnji proračun Unije u skladu s Ugovorima, Komisija bi pri procjeni proračunskih i kadrovskih potreba ENISA-e trebala uzeti u obzir obveze koje proizlaze iz ove Uredbe.

(60) Komisija bi trebala redovito provoditi evaluaciju mjera utvrđenih u ovoj Uredbi. Prva takva evaluacija trebala bi se provesti u prve dvije godine od datuma stupanja na snagu ove Uredbe i najmanje svake četiri godine nakon toga, uzimajući u obzir vrijeme revizije višegodišnjeg financijskog okvira uspostavljenog u skladu s člankom 312. UFEU-a. Komisija bi trebala podnijeti izvješće o postignutom napretku Europskom parlamentu i Vijeću. Kako bi procijenila različite potrebne elemente, uključujući opseg informacija koje se razmjenjuju u okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti, Komisija bi se trebala osloniti isključivo na informacije koje su lako dostupne ili dobrovoljno pružene. Uzimajući u obzir geopolitička kretanja i kako bi se osigurao kontinuitet i daljnji razvoj mjera utvrđenih u ovoj Uredbi nakon 2027., važno je da Komisija procijeni potrebu za dodjelom odgovarajućih sredstava u višegodišnjem financijskom okviru za razdoblje od 2028. do 2034.

---

[21] Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13., ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(61) S obzirom na to da ciljeve ove Uredbe, odnosno jačanje konkurentnog položaja industrije i usluga u Uniji u cijelom digitalnom gospodarstvu te doprinos tehnološkoj suverenosti i otvorenoj strateškoj autonomiji Unije, ne mogu dostatno ostvariti države članice, nego se oni na bolji način mogu ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenom u članku 5. UEU-a. U skladu s načelom proporcionalnosti utvrđenim u tom članku, ova Uredba ne prelazi ono što je potrebno za ostvarivanje tih ciljeva,

DONIJELI SU OVU UREDBU:

Poglavlje I.
Opće odredbe

Članak 1.

Predmet i ciljevi

1. Ovom se Uredbom utvrđuju mjere za jačanje kapaciteta u Uniji za otkrivanje kibernetičkih sigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih, osobito uspostavom:

(a) paneuropske mreže kibernetičkih centara („europski sustav uzbunjivanja u području kibernetičke sigurnosti”) radi razvoja i poboljšanja koordiniranih sposobnosti za otkrivanje i zajedničku informiranost o stanju;

(b) mehanizma za izvanredne kibernetičke sigurnosne situacije kako bi se državama članicama pružila potpora u pripremi za značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera, odgovoru na njih, ublažavanju njihovog učinka i započinjanju oporavka od njih te kako bi se drugim korisnicima pružila potpora u odgovoru na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente ekvivalentne onima velikih razmjera;

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

2. Ovom se Uredbom nastoje ostvariti opći ciljevi jačanja konkurentnog položaja industrije i usluga u Uniji u digitalnom gospodarstvu, uključujući mikropoduzeća te mala i srednja poduzeća te novoosnovana poduzeća, te doprinosa tehnološkoj suverenosti i otvorenoj strateškoj autonomiji Unije u području kibernetičke sigurnosti, među ostalim poticanjem inovacija na jedinstvenom digitalnom tržištu. Ti se ciljevi nastoje ostvariti jačanjem solidarnosti na razini Unije, jačanjem kibernetičkog sigurnosnog ekosustava, jačanjem kibernetičke otpornosti država članica i razvojem vještina, znanja, sposobnosti i kompetencija radne snage u području kibernetičke sigurnosti.

3. Opći ciljevi iz stavka 2. ostvaruju se putem sljedećih specifičnih ciljeva:

(a) jačanje zajedničkih kapaciteta Unije za koordinirano otkrivanje kibernetičkih prijetnji i kibernetičkih incidenata te zajedničke informiranosti o stanju u pogledu kibernetičkih prijetnji i kibernetičkih incidenata;

(b) podizanje pripravnosti subjekata koji djeluju u sektorima visoke kritičnosti ili subjekata koji djeluju u drugim kritičnim sektorima u Uniji i jačanje solidarnosti razvojem koordiniranog testiranja pripravnosti i pojačanih kapaciteta za odgovor i oporavak radi postupanja sa značajnim kibernetičkim sigurnosnim incidentima, kibernetičkim sigurnosnim incidentima velikih razmjera ili kibernetičkim sigurnosnim incidentima ekvivalentnima kibernetičkom sigurnosnom incidentu velikih razmjera, među ostalim mogućim stavljanjem potpore Unije za odgovor na kibernetičke sigurnosne incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa;

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

4. Djelovanja na temelju ove Uredbe provode se uz dužno poštovanje nadležnosti država članica i dopunjuju aktivnosti koje provode mreža CSIRT-ova, mreža EU-CyCLONe i skupina za suradnju NIS.

5. Ovom se Uredbom ne dovode u pitanje temeljne državne funkcije država članica, uključujući osiguravanje teritorijalne cjelovitosti države, očuvanje javnog poretka i zaštitu nacionalne sigurnosti. Nacionalna sigurnost posebice ostaje isključiva odgovornost svake države članice.

6. Dijeljenje ili razmjena informacija na temelju ove Uredbe koje su u skladu s pravilima Unije ili nacionalnim pravilima povjerljive ograničena je na ono što je relevantno i razmjerno svrsi tog dijeljenja ili te razmjene. Pri takvom dijeljenju ili razmjeni informacija čuva se njihova povjerljivost te se štite sigurnost i komercijalni interesi predmetnih subjekata. To ne obuhvaća dostavljanje informacija čije bi otkrivanje bilo protivno ključnim interesima država članica u pogledu nacionalne sigurnosti, javne sigurnosti ili obrane.

Članak 2.

Definicije

Za potrebe ove Uredbe, primjenjuju se sljedeće definicije:

1. „prekogranični kibernetički centar” znači višedržavna platforma uspostavljena na temelju pisanog sporazuma o konzorciju na kojoj su, u koordiniranoj mrežnoj strukturi, okupljeni nacionalni kibernetički centri iz najmanje triju država članica i koja je namijenjena za unapređenje praćenja, otkrivanja i analize kibernetičkih prijetnji radi sprečavanja incidenata i pružanje potpore u pripremi relevantnih saznanja o kibernetičkim prijetnjama, osobito razmjenom relevantnih podataka i informacija, koji se, prema potrebi, anonimiziraju, te dijeljenjem najsuvremenijih alata i zajedničkim razvojem sposobnosti za kibernetičko otkrivanje, analizu, te prevenciju i zaštitu u pouzdanom okruženju;

2. „konzorcij domaćin” znači konzorcij sastavljen od država članica sudionica koje su se sporazumjele uspostaviti prekogranični kibernetički centar i doprinositi nabavi alata, infrastrukture ili usluga za prekogranični kibernetički centar i njegovu radu;

3. „CSIRT” znači CSIRT koji je imenovan ili uspostavljen u skladu s člankom 10. Direktive (EU) 2022/2555;

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

5. „subjekti koji djeluju u sektorima visoke kritičnosti ” znači subjekti vrsta navedenih u Prilogu I. Direktivi (EU) 2022/2555;

6. „subjekti koji djeluju u drugim kritičnim sektorima” znači subjekti vrsta navedenih u Prilogu II. Direktivi (EU) 2022/2555;

7. „rizik” znači rizik kako je definiran u članku 6. točki 9. Direktive (EU) 2022/2555;

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

9. „incident” znači incident kako je definiran u članku 6. točki 6. Direktive (EU) 2022/2555;

10. „značajan kibernetički sigurnosni incident” znači incident koji ispunjava kriterije utvrđene u članku 23. stavku 3. Direktive (EU) 2022/2555;

11. „veliki incident” znači veliki incident kako je definiran u članku 3. stavku 8. Uredbe (EU, Euratom) 2023/2841 Europskog parlamenta i Vijeća[22];

12. „kibernetički sigurnosni incident velikih razmjera” znači kibernetički sigurnosni incident velikih razmjera kako je definiran u članku 6. točki 7. Direktive (EU) 2022/2555;

[22] Uredba (EU, Euratom) 2023/2841 Europskog parlamenta i Vijeća od 13. prosinca 2023. o utvrđivanju mjera za visoku zajedničku razinu kibernetičke sigurnosti u institucijama, tijelima, uredima i agencijama Unije (SL L, 2023/2841, 18.12.2023., ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13. „kibernetički sigurnosni incident ekvivalentan kibernetičkom sigurnosnom incidentu velikih razmjera” znači, u slučaju institucija, tijela, ureda i agencija Unije, veliki incident, a u slučaju trećih zemalja pridruženih programu Digitalna Europa, incident koji uzrokuje razinu poremećaja koja premašuje sposobnost treće zemlje pridružene programu Digitalna Europa da na njega odgovori;

14. „treća zemlja pridružena programu Digitalna Europa” znači treća zemlja koja je stranka sporazuma s Unijom kojim se omogućuje njezino sudjelovanje u programu Digitalna Europa na temelju članka 10. Uredbe (EU) 2021/694;

15. „javni naručitelj” znači Komisija ili ENISA, u mjeri u kojoj su funkcioniranje pričuve EU-a za kibernetičku sigurnost i upravljanje njome povjereni ENISA-i na temelju članka 14. stavka 5.;

16. „pružatelj upravljanih sigurnosnih usluga” znači pružatelj upravljanih sigurnosnih usluga kako je definiran u članku 6. točki 40. Direktive (EU) 2022/2555;

17. „pouzdani pružatelji upravljanih sigurnosnih usluga” znači pružatelji upravljanih sigurnosnih usluga odabrani za uključivanje u pričuvu EU- a za kibernetičku sigurnost u skladu s člankom 17.

Poglavlje II.

Europski sustav uzbunjivanja u području kibernetičke sigurnosti

Članak 3.

Uspostava europskog sustava uzbunjivanja u području kibernetičke sigurnosti

1. Uspostavlja se paneuropska mreža infrastrukture, koja se sastoji od nacionalnih kibernetičkih centara i prekograničnih kibernetičkih centara koji se dobrovoljno pridružuju, pod nazivom europski sustav uzbunjivanja u području kibernetičke sigurnosti radi podržavanja razvoja naprednih sposobnosti kako bi Unija poboljšala sposobnosti otkrivanja, analize i obrade podataka u vezi s kibernetičkim prijetnjama i sprečavanjem incidenata u Uniji.

2. Europski sustav uzbunjivanja u području kibernetičke sigurnosti:

   (a) doprinosi boljoj zaštiti od kibernetičkih prijetnji i odgovoru na njih podupiranjem relevantnih subjekata, posebno CSIRT-ova, mreže CSIRT-ova, mreže EU-CyCLONe i nadležnih tijela imenovanih ili uspostavljenih u skladu s člankom 8. stavkom 1. Direktive (EU) 2022/2555, jačanjem njihovih sposobnosti te suradnjom s njima;

   (b) objedinjuje relevantne podatke i informacije o kibernetičkim prijetnjama i incidentima iz raznih izvora unutar prekograničnih kibernetičkih centara i razmjenjuje analizirane ili agregirane informacije putem prekograničnih kibernetičkih centara, prema potrebi s mrežom CSIRT-ova;

(c) prikuplja i podupire izradu visokokvalitetnih i upotrebljivih informacije te saznanja o kibernetičkim prijetnjama upotrebom najsuvremenijih alata i naprednih tehnologija te dijeli te informacije i saznanja o kibernetičkim prijetnjama;

(d) doprinosi poboljšanju koordiniranog otkrivanja kibernetičkih prijetnji i zajedničke informiranosti o stanju u cijeloj Uniji te izdaje upozorenja, među ostalim, prema potrebi, davanjem konkretnih preporuka subjektima;

(e) pruža usluge i provodi aktivnosti zajednici za kibernetičku sigurnost u Uniji, što uključuje doprinos razvoju naprednih alata i tehnologija poput umjetne inteligencije i naprednih alata za analitiku podataka.

3. Djelovanja kojima se provodi europski sustav uzbunjivanja u području kibernetičke sigurnosti podupiru se financiranjem iz programa Digitalna Europa i provode u skladu s Uredbom (EU) 2021/694, osobito njezinim specifičnim ciljem 3.

Članak 4.

Nacionalni kibernetički centri

1. Ako država članica odluči sudjelovati u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti, imenuje ili, ako je primjenjivo, uspostavlja nacionalni kibernetički centar za potrebe ove Uredbe.

2. Nacionalni kibernetički centar jedinstveni je subjekt koji djeluje pod nadležnošću države članice. To može biti CSIRT ili, prema potrebi, nacionalno tijelo za upravljanje kibernetičkim krizama ili drugo nadležno tijelo imenovano ili uspostavljeno u skladu s člankom 8. stavkom 1. Direktive (EU) 2022/2555 ili drugi subjekt. Nacionalni kibernetički centar mora:

(a) imati kapacitet da služi drugim javnim i privatnim organizacijama na nacionalnoj razini kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibernetičkim prijetnjama i incidentima te doprinosi prekograničnom kibernetičkom centru kako je navedeno u članku 5. ove Uredbe; i

(b) biti sposoban otkrivati, agregirati i analizirati podatke i informacije relevantne za kibernetičke prijetnje i incidente, kao što su saznanja o kibernetičkim prijetnjama, upotrebom najsuvremenijih tehnologija, s ciljem sprečavanja incidenata.

3. U okviru funkcija iz stavka 2. ovog članka nacionalni kibernetički centri mogu surađivati sa subjektima iz privatnog sektora radi razmjene relevantnih podataka i informacija u svrhu otkrivanja i sprečavanja kibernetičkih prijetnji i incidenata, među ostalim sa sektorskim i međusektorskim zajednicama ključnih i važnih subjekata kako su navedeni u članku 3. Direktive (EU) 2022/2555. Prema potrebi i u skladu s pravom Unije i nacionalnim pravom, informacije koje zatraže ili primaju nacionalni kibernetički centri mogu uključivati telemetrijske i senzorske podatke i podatke o evidentiranju.

4. Država članica odabrana u skladu s člankom 9. stavkom 1. obvezuje se podnijeti zahtjev za sudjelovanje svojeg nacionalnog kibernetičkog centra u prekograničnom kibernetičkom centru.

Članak 5.

Prekogranični kibernetički centri

1. Ako su se najmanje tri države članice obvezale osigurati da njihovi nacionalni kibernetički centri surađuju radi koordinacije svojih aktivnosti otkrivanja i praćenja kibernetičkih prijetnji, te države članice za potrebe ove Uredbe mogu osnovati konzorcij domaćin.

2. Konzorcij domaćin sastavljen je od barem tri države članice sudionice koje su se sporazumjele uspostaviti prekogranični kibernetički centar te doprinositi nabavi alata, infrastrukture ili usluga za prekogranični kibernetički centar i njegovu radu u skladu sa stavkom 4.

3. Ako je konzorcij domaćin odabran u skladu s člankom 9. stavkom 3., njegovi članovi sklapaju pisani sporazum o konzorciju u kojem se:

   (a) utvrđuju interni aranžmani za provedbu sporazuma o korištenju i upotrebi iz članka 9. stavka 3.;

   (b) uspostavlja prekogranični kibernetički centar konzorcija domaćina; i

   (c) uključuje specifične odredbe koje se zahtijevaju u skladu s člankom 6. stavcima 1. i 2.

4. Prekogranični kibernetički centar višedržavna je platforma uspostavljena pisanim sporazumom o konzorciju iz stavka 3. U njemu se, u koordiniranoj mrežnoj strukturi, okupljaju nacionalni kibernetički centri sigurnost država članica konzorcija domaćina. Mora biti osmišljen tako da služi praćenju, otkrivanju i analizi kibernetičkih prijetnji, sprečavanju incidenata i podupiranju proizvodnje saznanja o kibernetičkim prijetnjama, posebno razmjenom relevantnih podataka i informacija, koji se prema potrebi anonimiziraju, kao i razmjenom najsuvremenijih alata i zajedničkim razvojem sposobnosti za kibernetičko otkrivanje, analizu, te prevenciju i zaštitu u pouzdanom okruženju.

5. Prekogranični kibernetički centar za pravne potrebe zastupa član odgovarajućeg konzorcija domaćina koji djeluje kao koordinator ili, ako ima pravnu osobnost, konzorcij domaćin. Odgovornost za usklađenost prekograničnog kibernetičkog centra s ovom Uredbom i sporazumom o smještaju i korištenju dodjeljuju se u pisanom sporazumu o konzorciju iz stavka 3.

6. Država članica može se pridružiti postojećem konzorciju domaćinu uz suglasnost članova konzorcija domaćina. Pisani sporazum o konzorciju iz stavka 3. te sporazum o smještaju i korištenju na odgovarajući se način mijenjaju. To ne utječe na vlasnička prava Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibersigurnosti („ECCC”) nad alatima, infrastrukturama ili uslugama koji su već zajednički nabavljeni s tim konzorcijem domaćinom.

Članak 6.

Suradnja i dijeljenje informacija unutar prekograničnih kibernetičkih centara i među njima

1. Članovi konzorcija domaćina osiguravaju da njihovi nacionalni kibernetički centri, u skladu s pisanim sporazumom o konzorciju iz članka 5. stavka 3., međusobno unutar prekograničnog kibernetičkog centra dijele relevantne informacije koje se, prema potrebi, anonimiziraju, kao što su informacije o kibernetičkim prijetnjama, izbjegnutim incidentima, ranjivostima, tehnikama i postupcima, pokazateljima ugroženosti, neprijateljskim taktikama i počiniteljima prijetnji, kibernetička sigurnosna upozorenja te preporuke o konfiguraciji kibernetičkih sigurnosnih alata za otkrivanje kibernetičkih napada ako takvo dijeljenje informacija:

   (a) potiče i poboljšava otkrivanje kibernetičkih prijetnji i jača sposobnosti mreže CSIRT-ova za sprečavanje incidenata i odgovor na njih ili ublažavanje njihova učinka;

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

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

(a) obveza dijeljenja informacija kako su navedene u stavku 1. među članovima konzorcija domaćina i uvjeti pod kojima se te informacije trebaju dijeliti;

(b) upravljački okvir kojim se pojašnjava i potiče dijeljenje od strane svih sudionika relevantnih informacija kako su navedene u stavku 1., koje se, prema potrebi, anonimiziraju;

(c) ciljevi doprinosa razvoju naprednih alata i tehnologija poput umjetne inteligencije i naprednih alata za analitiku podataka.

Pisanim sporazumom o konzorciju može se pobliže odrediti da se informacije iz stavka 1. trebaju dijeliti u skladu s pravom Unije i nacionalnim pravom.

3. Prekogranični kibernetički centri međusobno sklapaju sporazume o suradnji u kojima se utvrđuju načela međusobne operabilnosti i dijeljenja informacija među prekograničnim kibernetičkim centrima. Prekogranični kibernetički centri obavješćuju Komisiju o sklopljenim sporazumima o suradnji.

4. Dijeljenje informacija kako su navedene u stavku 1. među prekograničnim kibernetičkim centrima osigurava se visokom razinom interoperabilnosti. Kako bi se poduprla takva interoperabilnost ENISA, uz blisko savjetovanje s Komisijom, bez nepotrebne odgode, a u svakom slučaju do … [12 mjeseci od datuma stupanja na snagu ove Uredbe], izdaje smjernice o interoperabilnosti u kojima se posebno navode formati i protokoli za dijeljenje informacija, uzimajući u obzir međunarodne standarde i najbolje prakse, kao i funkcioniranje svih uspostavljenih prekograničnih kibernetičkih centara. Zahtjevi za interoperabilnost predviđeni u sporazumima o suradnji prekograničnih kibernetičkih centara temelje se na smjernicama koje izdaje ENISA.

Članak 7.

Suradnja i dijeljenje informacija s mrežama na razini Unije

1. Prekogranični kibernetički centri i mreža CSIRT-ova blisko surađuju, posebno u svrhu dijeljenja informacija. U tu svrhu dogovaraju se o postupovnim aranžmanima o suradnji i dijeljenju relevantnih informacija te, ne dovodeći u pitanje stavak 2., o vrstama informacija koje će se dijeliti.

2. Ako prekogranični kibernetički centri dobiju informacije o potencijalnom ili aktualnom kibernetičkom sigurnosnom incidentu velikih razmjera, osiguravaju, za potrebe zajedničke informiranosti o stanju, da se tijelima država članica i Komisiji bez nepotrebne odgode dostave relevantne informacije i rana upozorenja putem mreže EU-CyCLONe i mreže CSIRT-ova.

Članak 8.

Sigurnost

1. Države članice koje sudjeluju u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti osiguravaju visoku razinu kibernetičke sigurnosti, među ostalim povjerljivosti i sigurnosti podataka, kao i fizičku sigurnost europske mreže sustava uzbunjivanja u području kibernetičke sigurnosti te primjereno upravljanje i kontrolu nad tom mrežom kako bi je se zaštitilo od prijetnji i kako bi se osigurala njezina sigurnost i sigurnost sustavâ, uključujući podatke i informacije koji se dijele putem te mreže.

2. Države članice koje sudjeluju u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti osiguravaju da dijeljenje informacija iz članka 6. stavka 1. u okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti s bilo kojim subjektom koji nije tijelo javne vlasti ili tijelo države članice ne šteti sigurnosnim interesima Unije ili država članica.

Članak 9.

Financiranje europskog sustava uzbunjivanja u području kibernetičke sigurnosti

1. Nakon poziva na iskaz interesa za države članice koje namjeravaju sudjelovati u europskom sustavu uzbunjivanja u području kibernetičke sigurnosti ECCC odabire države članice za sudjelovanje s ECCC-om u zajedničkoj nabavi alata, infrastrukture ili usluga kako bi se uspostavili nacionalni kibernetički centri koji su imenovani ili uspostavljeni u skladu s člankom 4. stavkom 1., ili povećale njihove sposobnosti. ECCC može odabranim državama članicama dodijeliti bespovratna sredstva za financiranje rada tih alata, infrastrukture ili usluga. Financijski doprinos Unije pokriva do 50 % troškova nabave alata, infrastrukture ili usluga te do 50 % operativnih troškova. Preostale troškove pokrivaju odabrane države članice. Prije pokretanja postupka nabave alata, infrastrukture ili usluga ECCC i odabrana država članica sklapaju sporazum o smještaju i korištenju kojim se uređuje upotreba alata, infrastrukture ili usluga.

2. Ako nacionalni kibernetički centar države članice ne postane sudionik u prekograničnom kibernetičkom centru u roku od dvije godine od datuma na koji su nabavljeni alati, infrastruktura ili usluge ili na koji je država članica primila bespovratna sredstva, ovisno o tome što je nastupilo ranije, država članica nije prihvatljiva za dodatnu potporu Unije na temelju ovog poglavlja sve dok se ne pridruži prekograničnom kibernetičkom centru.

3. Nakon poziva na iskaz interesa ECCC odabire konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata, infrastrukture ili usluga s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata, infrastrukture ili usluga. Financijski doprinos Unije pokriva do 75 % troškova nabave alata, infrastrukture ili usluga te do 50 % operativnih troškova. Preostale troškove pokriva konzorcij domaćin. Prije pokretanja postupka nabave alata, infrastrukture ili usluga ECCC i konzorcij domaćin sklapaju sporazum o smještaju i korištenju kojim se uređuje upotreba alata, infrastrukture ili usluga.

4. ECCC najmanje svake dvije godine priprema pregled alata, infrastrukture ili usluga koji su potrebni i odgovarajuće su kvalitete za uspostavu nacionalnih kibernetičkih centara i prekograničnih kibernetičkih centara te povećanje njihovih sposobnosti i njihove dostupnosti, među ostalim od pravnih subjekata s poslovnim nastanom ili za koje se smatra da imaju poslovni nastan u državama članicama i koje kontroliraju države članice ili državljani država članica. Pri pripremi pregleda ECCC se savjetuje s mrežom CSIRT-ova, svim postojećim prekograničnim kibernetičkim centrima, ENISA-om i Komisijom.

Poglavlje III.

Mehanizam za izvanredne kibernetičke sigurnosne situacije

Članak 10.

Uspostava mehanizma za izvanredne kibernetičke sigurnosne situacije

1. Uspostavlja se mehanizam za izvanredne kibernetičke sigurnosne situacije radi podupiranja unapređenja otpornosti Unije na kibernetičke prijetnje i pripreme za kratkoročne posljedice značajnih kibernetičkih sigurnosnih incidenata, kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih sigurnosnih incidenata ekvivalentnih kibernetičkom sigurnosnom incidentu velikih razmjera velikih razmjera i njihovo ublažavanje u duhu solidarnosti.

2. U slučaju država članica, djelovanja u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije pružaju se na zahtjev te dopunjuju napore i djelovanja država članica za pripremu za incidente, odgovor na njih i oporavak od njih.

3. Djelovanja kojima se provodi mehanizam za izvanredne kibernetičke sigurnosne situacije podupiru se financiranjem iz programa Digitalna Europa i provode u skladu s Uredbom (EU) 2021/694, osobito njezinim specifičnim ciljem 3.

4. Djelovanja u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije provode se prvenstveno putem ECCC-a u skladu s Uredbom (EU) 2021/887 Europskog parlamenta i Vijeća. Međutim, djelovanja kojima se provodi pričuva EU-a za kibernetičku sigurnost iz članka 11. točke (b) ove Uredbe provode Komisija i ENISA.

Članak 11.

Vrste djelovanja

Mehanizmom za izvanredne kibernetičke sigurnosne situacije podupiru se sljedeće vrste djelovanja:

(a) djelovanja u području pripravnosti, a to su:

i. koordinirano testiranje pripravnosti subjekata koji djeluju u sektorima visoke kritičnosti u cijeloj Uniji kako je navedeno u članku 12.;

ii. druga djelovanja u području pripravnosti za subjekte koji djeluju u sektorima visoke kritičnosti ili subjekte koji djeluju u drugim kritičnim sektorima, kako je navedeno u članku 13.;

(b) djelovanja, kojima se doprinosi odgovoru na značajne kibernetičke sigurnosne incidente, kibernetičke sigurnosne incidente velikih razmjera i kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera i započinjanju oporavka od njih, koje trebaju poduzeti pouzdani pružatelji upravljanih sigurnosnih usluga koji sudjeluju u pričuvi EU-a za kibernetičku sigurnost uspostavljenoj člankom 14.;

(c) djelovanja kojima se podupire uzajamna pomoć kako je navedeno u članku 18.

Članak 12.

Koordinirano testiranje pripravnosti subjekata

1. Mehanizmom za izvanredne kibernetičke sigurnosne situacije podupire se dobrovoljno koordinirano testiranje pripravnosti subjekata koji djeluju u sektorima visoke kritičnosti.

2. Koordinirano testiranje pripravnosti može se sastojati od aktivnosti u području pripravnosti, kao što su penetracijsko testiranje, i procjena prijetnji.

3. Potpora za djelovanja u području pripravnosti na temelju ovog članka pruža se državama članicama prvenstveno u obliku bespovratnih sredstava podložno uvjetima predviđenima u relevantnim programima rada kako su navedeni u članku 24. Uredbe (EU) 2021/694.

4. Za potrebe podupiranja koordiniranog testiranja pripravnosti subjekata iz članka 11. točke (a) podtočke i. ove Uredbe u cijeloj Uniji Komisija, nakon savjetovanja sa skupinom za suradnju NIS, mrežom EU-CyCLONe i ENISA-om, među sektorima visoke kritičnosti navedenima u Prilogu I. Direktivi (EU) 2022/2555 utvrđuje relevantne sektore ili podsektore za koje se može objaviti poziv na podnošenje prijedloga za dodjelu bespovratnih sredstava. Sudjelovanje država članica u tim pozivima na podnošenje prijedloga je dobrovoljno.

5. Pri utvrđivanju sektora ili podsektora iz stavka 4. Komisija uzima u obzir koordinirane procjene rizika i testiranje otpornosti na razini Unije te njihove rezultate.

6. Skupina za suradnju NIS izrađuje, u suradnji s Komisijom, Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”) i ENISA-om te, u okviru svojeg mandata, mrežom EU-CyCLONe, zajedničke scenarije rizika i metodologije za koordinirana testiranja pripravnosti u skladu s člankom 11. točkom (a) podtočkom i. i, prema potrebi, za druga djelovanja u području pripravnosti iz točke (a) podtočke ii. tog članka.

7. Ako subjekt koji djeluje u sektoru visoke kritičnosti dobrovoljno sudjeluje u koordiniranom testiranju pripravnosti, a to testiranje dovede do preporuka za posebne mjere koje bi subjekt koji sudjeluje mogao uključiti u plan s korektivnim mjerama, tijelo države članice odgovorno za koordinirano testiranje pripravnosti, prema potrebi, preispituje daljnje postupanje subjekata koji sudjeluju u vezi s tim mjerama s ciljem jačanja pripravnosti.

Članak 13.

Druga djelovanja u području pripravnosti

1. Mehanizmom za izvanredne kibernetičke sigurnosne situacije podupiru se djelovanja u području pripravnosti koje nisu obuhvaćena člankom 12. Takva djelovanja uključuju djelovanja u području pripravnosti za subjekte u sektorima koji nisu utvrđeni za koordinirano testiranje pripravnosti u skladu s člankom 12. Takvim mjerama mogu se podupirati praćenje ranjivosti, praćenje rizika, vježbe i osposobljavanje.

2. Potpora za djelovanja u području pripravnosti na temelju ovog članka pruža se državama članicama na zahtjev i prvenstveno u obliku bespovratnih sredstava i podložno uvjetima predviđenim u relevantnim programima rada kako su navedeni u članku 24. Uredbe (EU) 2021/694.

Članak 14.

Uspostava pričuve EU-a za kibernetičku sigurnost

1. Uspostavlja se pričuva EU-a za kibernetičku sigurnost radi pomaganja, na zahtjev, korisnicima kako su navedeni u stavku 3. pri odgovaranju ili pružanju potpore za odgovaranje na značajne kibernetičke sigurnosne incidente, kibernetičke sigurnosne incidente velikih razmjera ili kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera i započinjanje oporavka od njih.

2. Pričuvu EU-a za kibernetičku sigurnost čine usluge odgovora koje pružaju pouzdani pružatelji upravljanih sigurnosnih usluga odabrani u skladu s kriterijima utvrđenim u članku 17. stavku 2. Pričuva EU-a za kibernetičku sigurnost može obuhvaćati prethodno namijenjene usluge. Ako se te prethodno namijenjene usluge ne upotrebljavaju za odgovor na incidente tijekom razdoblja izvršavanja za koje su te usluge prethodno namijenjene, prethodno namijenjene usluge pouzdanog pružatelja upravljanih sigurnosnih usluga pretvaraju se u usluge pripravnosti povezane sa sprečavanjem incidenata i odgovorom na njih. Korištenje pričuve EU-a za kibernetičku sigurnost moguće je, na zahtjev, u svim državama članicama, institucijama, tijelima, uredima i agencijama Unije te u trećim zemljama pridruženima programu Digitalna Europa iz članka 19. stavka 1.

3. Korisnici usluga koje se pružaju iz pričuve EU-a za kibernetičku sigurnost su sljedeći:

(a) tijela za upravljanje kibernetičkim krizama i CSIRT-ovi država članica navedeni u članku 9. stavcima 1. i 2. odnosno članku 10. Direktive (EU) 2022/2555;

(b) CERT-EU, u skladu s člankom 13. Uredbe (EU, Euratom) 2023/2841;

(c) nadležna tijela kao što su timovi za odgovor na računalne sigurnosne incidente i tijela za upravljanje kibernetičkim krizama trećih zemalja pridruženih programu Digitalna Europa u skladu s člankom 19. stavkom 8.

4. Komisija je općenito odgovorna za provedbu pričuve EU-a za kibernetičku sigurnost. Komisija određuje prioritete i razvoj pričuve EU-a za kibernetičku sigurnost u suradnji sa skupinom za suradnju NIS i u skladu sa zahtjevima korisnika iz stavka 3,. nadzire njezinu provedbu te osigurava komplementarnost, dosljednost, sinergije i veze s drugim djelovanjima za potporu na temelju ove Uredbe, kao i s drugim djelovanjima i programima Unije. Navedeni prioriteti preispituju se svake dvije godine. Komisija obavješćuje Europski parlament i Vijeće o tim prioritetima i njihovim izmjenama.

5. Ne dovodeći u pitanje općenitu odgovornost Komisije za provedbu pričuve EU-a za kibernetičku sigurnost iz stavka 4. ovog članka i podložno sporazumu o doprinosu kako je definiran u članku 2. točki 19. Uredbe (EU, Euratom) 2024/2509, Komisija rad i pričuve EU-a za kibernetičku sigurnost i upravljanje njome u cijelosti ili djelomično povjerava ENISA-i. Aspekti koji nisu povjereni ENISA-i ostaju pod izravnim upravljanjem Komisije.

6. ENISA najmanje svake dvije godine priprema pregled usluga koje su potrebne korisnicima iz stavka 3. točaka (a) i (b) ovog članka. Pregled obuhvaća i dostupnost takvih usluga, uključujući usluge pravnih subjekata s poslovnim nastanom u državama članicama ili za koje se smatra da imaju poslovni nastan u državama članicama te na one koji su pod kontrolom država članica ili državljana država članica. Pri izradi pregleda te dostupnosti ENISA ocjenjuje vještine i kapacitete radne snage Unije u području kibernetičke sigurnosti relevantne za ciljeve pričuve EU-a za kibernetičku sigurnost. Pri pripremi pregleda ENISA se savjetuje sa skupinom za suradnju NIS, mrežom EU-CyCLONe, Komisijom i, prema potrebi, Međuinstitucijskim odborom za kibernetičku sigurnost osnovanim na temelju članka 10. Uredbe (EU) 2023/2841 (IICB). Pri izradi pregleda dostupnosti usluga ENISA se savjetuje i s relevantnim dionicima iz industrije kibernetičke sigurnosti, uključujući pružatelje upravljanih sigurnosnih usluga. ENISA priprema sličan pregled, nakon što o tome obavijesti Vijeće i nakon savjetovanja s mrežom EU-CyCLONe i Komisijom te, prema potrebi, Visokim predstavnikom, kako bi utvrdila potrebe korisnika iz stavka 3. točke (c) ovog članka.

7. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 23. radi dopune ove Uredbe utvrđivanjem vrste i broja usluga odgovora potrebnih za pričuvu EU-a za kibernetičku sigurnost. Pri pripremi tih delegiranih akata Komisija uzima u obzir pregled iz stavka 6. ovog članka te može razmjenjivati savjete i surađivati sa skupinom za suradnju NIS i ENISA-om.

Članak 15.

Zahtjevi za potporu iz pričuve EU-a za kibernetičku sigurnost

1. Korisnici iz članka 14. stavka 3. mogu zatražiti usluge iz pričuve EU-a za kibernetičku sigurnost radi potpore odgovoru na značajne kibernetičke sigurnosne incidente, kibernetičke sigurnosne incidente velikih razmjera ili kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera i započinjanja oporavka od njih.

2. Da bi primili potporu iz pričuve EU-a za kibernetičku sigurnost, korisnici iz članka 14. stavka 3. dužni su poduzeti sve odgovarajuće mjere za ublažavanje učinaka incidenta za koji se traži potpora, među ostalim, prema potrebi, pružiti izravnu tehničku pomoć i druge resurse za pomoć u odgovoru na incident, te korake za oporavak.

3. Zahtjevi za potporu šalju se javnom naručitelju na sljedeći način:

   (a) u slučaju korisnika iz članka 14. stavka 3. točke (a) ove Uredbe putem jedinstvene kontaktne točke imenovane ili uspostavljene u skladu s člankom 8. stavkom 3. Direktive (EU) 2022/2555;

(b) u slučaju korisnika iz članka 14. stavka 3. točke (b) od strane tog korisnika;

(c) u slučaju korisnika iz članka 14. stavka 3. točke (c) putem jedinstvene kontaktne točke iz članka 19. stavka 9. ove Uredbe.

4. U slučaju zahtjeva korisnika iz članka 14. stavka 3. točke (a), države članice obavješćuju mrežu CSIRT-ova i, prema potrebi, mrežu EU-CyCLONe o zahtjevima svojih korisnika za potporu odgovoru na incident i inicijalnom oporavku od njega koje su podnijeli na temelju ovog članka.

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

(a) odgovarajuće informacije o pogođenom subjektu i mogućem učinku incidenta na:

i. u slučaju korisnika iz članka 14. stavka 3. točke (a), pogođene države članice i korisnike, uključujući rizik od širenja na drugu državu;

ii. u slučaju korisnika iz članka 14. stavka 3. točke (b) ove Uredbe, pogođene institucije, tijela, urede ili agencije Unije;

iii. u slučaju korisnika iz članka 14. stavka 3. točke (c) ove Uredbe, pogođene zemlje pridružene programu Digitalna Europa;

(b) informacije o zatraženoj usluzi, zajedno s planiranom upotrebom zatražene potpore, uključujući naznaku procijenjenih potreba;

(c) odgovarajuće informacije o mjerama poduzetima za ublažavanje incidenta za koji se traži potpora kako je navedeno u stavku 2.;

(d) prema potrebi, dostupne informacije o drugim oblicima potpore koji su dostupni pogođenom subjektu.

6. Kako bi se olakšalo podnošenje zahtjeva za potporu iz pričuve EU-a za kibernetičku sigurnost, ENISA, u suradnji s Komisijom i mrežom EU-CyCLONe, izrađuje predložak.

7. Komisija može provedbenim aktima dodatno utvrditi detaljne postupovne aranžmane za način na koji se traže usluge potpore iz pričuve EU-a za kibernetičku sigurnost i način na koji se na njih odgovara u skladu s ovim člankom, člankom 16. stavkom 1. i člankom 19. stavkom 10., među ostalim aranžmane za podnošenje takvih zahtjeva i dostavu odgovora i predloške za izvješća iz članka 16. stavka 9. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 24. stavka 2.

Članak 16.

Provedba potpore iz pričuve EU-a za kibernetičku sigurnost

1. U slučaju zahtjeva korisnika iz članka 14. stavka 3. točaka (a) i (b), zahtjeve za potporu iz pričuve EU-a za kibernetičku sigurnost ocjenjuje javni naručitelj. Odgovor se šalje korisnicima iz članka 14. stavka 3. točaka (a) i (b) bez odgode, a u svakom slučaju najkasnije 48 sati od podnošenja zahtjeva kako bi se osigurala djelotvornost potpore. Javni naručitelj obavješćuje Vijeće i Komisiju o rezultatima postupka.

2. Kad je riječ o informacijama koje se razmjenjuju tijekom traženja i pružanja usluga pričuve EU-a za kibernetičku sigurnost, sve strane uključene u primjenu ove Uredbe:

   (a) ograničavaju upotrebu i dijeljenje tih informacija na ono što je potrebno za izvršavanje svojih obveza ili funkcija na temelju ove Uredbe;

   (b) upotrebljavaju i dijele sve informacije koje su povjerljive ili klasificirane na temelju prava Unije i nacionalnog prava isključivo u skladu s tim pravom; i

   (c) osiguravaju djelotvornu, učinkovitu i sigurnu razmjenu informacija, prema potrebi upotrebom i poštovanjem relevantnih protokola za dijeljenje informacija, uključujući Protokol o semaforu.

3. Pri ocjenjivanju pojedinačnih zahtjeva u skladu s člankom 16. stavkom 1. i člankom 19. stavkom 10. javni naručitelj ili Komisija, ovisno o slučaju, prvo ocjenjuje jesu li ispunjeni kriteriji iz članka 15. stavaka 1. i 2. Ako su ti kriteriji ispunjeni, ocjenjuju trajanje i prirodu potpore koja je primjerena, uzimajući u obzir cilj iz članka 1. stavka 3. točke (b) i, prema potrebi, sljedeće kriterije:

(a) razmjer i ozbiljnost incidenta;

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

(c) mogući učinak incidenta na pogođene države članice, institucije, tijela, urede ili agencije Unije, ili treće zemlje pridružene programu Digitalna Europa;

(d) moguću prekograničnu prirodu incidenta i rizik od širenja na druge države članice, institucije, tijela, urede ili agencije Unije ili treće zemlje pridružene programu Digitalna Europa;

(e) mjere koje je korisnik poduzeo da pomogne u odgovoru i poduzete korake za inicijalni oporavak iz članka 15. stavka 2.

4. U slučaju istodobnih zahtjeva korisnika iz članka 14. stavka 3. kriteriji iz stavka 3. ovog članka uzimaju se u obzir prema potrebi kako bi se odredio prioritetni zahtjev, ne dovodeći u pitanje načelo lojalne suradnje između država članica i institucija, tijela, ureda i agencija Unije. Ako su dva ili više zahtjeva ocijenjena jednakovrijednima prema tim kriterijima., prednost se daje zahtjevima korisnika iz država članica. Ako su rad pričuve EU-a za kibernetičku sigurnost i upravljanje njome u cijelosti ili djelomično povjereni ENISA-i na temelju članka 14. stavka 5., ENISA i Komisija blisko surađuju na određivanju prioriteta zahtjeva u skladu s ovim stavkom.

5. Usluge pričuve EU-a za kibernetičku sigurnost pružaju se u skladu s posebnim sporazumima između pouzdanog pružatelja upravljanih sigurnosnih usluga i korisnika kojem se pruža potpora iz pričuve EU-a za kibernetičku sigurnost. Te se usluge mogu pružati u skladu s posebnim sporazumima između pouzdanog pružatelja upravljanih sigurnosnih usluga, korisnika i pogođenog subjekta. Svi sporazumi iz ovog stavka moraju sadržavati, između ostalog, uvjete odgovornosti.

6. Sporazumi iz stavka 5. temelje se na predlošcima koje izradi ENISA nakon savjetovanja s državama članicama i, prema potrebi, drugim korisnicima pričuve EU-a za kibernetičku sigurnost.

7. Komisija, ENISA i korisnici pričuve ne snose ugovornu odgovornost za štetu koju trećim stranama uzrokuju usluge pružene u okviru primjene pričuve EU-a za kibernetičku sigurnost.

8. Korisnici se mogu koristiti uslugama pričuve EU-a za kibernetičku sigurnost koje se pružaju kao odgovor na zahtjev na temelju članka 15. stavka 1. samo kako bi poduprli odgovor na značajne incidente, kibernetičke sigurnosne incidente velikih razmjera ili kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera i započeli oporavak od njih. Tim se uslugama mogu koristiti samo u odnosu na:

   (a) subjekte koji djeluju u sektorima visoke kritičnosti ili subjekte koji djeluju u drugim kritičnim sektorima, u slučaju korisnika iz članka 14. stavka 3. točke (a), te ekvivalentne subjekte u slučaju korisnika iz članka 14. stavka 3. točke (c); i

   (b) institucije, tijela, urede i agencije Unije, u slučaju korisnika iz članka 14. stavka 3. točke (b).

9. U roku od dva mjeseca od završetka potpore svi korisnici koji su primili potporu dostavljaju sažeto izvješće o pruženoj usluzi, ostvarenim rezultatima i stečenim iskustvima:

   (a) Komisiji, ENISA-i, mreži CSIRT-ova i mreži EU-CyCLONe, u slučaju korisnikâ iz članka 14. stavka 3. točke (a);

   (b) Komisiji, ENISA-i i IICB-u, u slučaju korisnika iz članka 14. stavka 3. točke (b);

(c) Komisiji, u slučaju korisnikâ iz članka 14. stavka 3. točke (c).

Komisija šalje Vijeću i Visokom predstavniku sva sažeta izvješća koja na temelju prvog podstavka točke (c) ovog stavka primi od korisnika iz članka 14. stavka 3.

10. Ako su rad pričuve EU-a za kibernetičku sigurnost i upravljanje njome u cijelosti ili djelomično povjereni ENISA-i u skladu s člankom 14. stavkom 5. ove Uredbe, ENISA o tome redovito podnosi izvješće Komisiji i savjetuje se s njom. U tom kontekstu ENISA odmah šalje Komisiji sve zahtjeve koje primi od korisnika iz članka 14. stavka 3. točke (c) ove Uredbe i, ako je to potrebno za potrebe određivanja prioriteta na temelju ovog članka, sve zahtjeve koje je zaprimila od korisnika iz članka 14. stavka 3. točke (a) ili (b) ove Uredbe. Obvezama iz ovog stavka ne dovodi se u pitanje članak 14. Uredbe (EU) 2019/881.

11. U slučaju korisnika iz članka 14. stavka 3. točaka (a) i (b), javni naručitelj redovito, a najmanje dvaput godišnje, izvješćuje skupinu za suradnju NIS o korištenju i rezultatima potpore.

12. U slučaju korisnika iz članka 14. stavka 3. točke (c), Komisija redovito, a najmanje dvaput godišnje, izvješćuje Vijeće i obavješćuje Visokog predstavnika o korištenju i rezultatima potpore.

Članak 17.

Pouzdani pružatelji upravljanih sigurnosnih usluga

1. U postupcima nabave za potrebe uspostave pričuve EU-a za kibernetičku sigurnost javni naručitelj pridržava se načela utvrđenih u Uredbi (EU, Euratom) 2024/2509 i sljedećih načela:

   (a) osigurava da su usluge obuhvaćene pričuvom EU-a za kibernetičku sigurnost u cjelini takve da pričuva EU-a za kibernetičku sigurnost obuhvaća usluge koje se mogu pružati u svim državama članicama, uzimajući osobito u obzir posebne nacionalne zahtjeve za pružanje takvih usluga, među ostalim u pogledu jezika, certifikacije ili akreditacije;

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

   (c) osigurava da pričuva EU-a za kibernetičku sigurnost donosi dodanu vrijednost Uniji tako što doprinosi ciljevima iz članka 3. Uredbe (EU) 2021/694, među ostalim poticanju razvoja vještina u području kibernetičke sigurnosti u Uniji.

2. Pri nabavi usluga za pričuvu EU-a za kibernetičku sigurnost javni naručitelj u dokumentaciju o nabavi uključuje sljedeće kriterije i zahtjeve:

(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 i kontinuitet stručnosti kao i potrebne tehničke resurse;

(b) pružatelj i sva relevantna društva kćeri i podugovaratelji poštuju primjenjiva pravila o zaštiti klasificiranih podataka i imaju uspostavljene odgovarajuće mjere, uključujući, prema potrebi, međusobne sporazume za zaštitu povjerljivih informacija koje se odnose na uslugu, a posebno dokaze, nalaze i izvješća;

(c) pružatelj mora dati dostatan dokaz da je njegova upravljačka struktura transparentna i da nije vjerojatno da će ugroziti njegovu nepristranost i kvalitetu njegovih usluga ili dovesti do sukoba interesa;

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

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

(f) pružatelj mora biti opremljen hardverom i softverom koji omogućuju traženu uslugu i ne sadržavaju poznate iskoristive ranjivosti, obuhvaćaju najnovija sigurnosna ažuriranja i u svakom slučaju su usklađeni s relevantnim odredbama Uredbe (EU) 2024/… Europskog parlamenta i Vijeća[23+];

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

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

(i) pružatelj mora moći pružati uslugu na jednom ili više službenih jezika institucija Unije ili države članice, ako tako zahtijevaju države članice ili korisnici iz članka 14. stavka 3. točaka (b) i (c) u kojima pružatelj može isporučiti uslugu.

(j) nakon što se uspostavi europski program kibernetičke sigurnosne certifikacije za upravljane sigurnosne usluge na temelju Uredbe (EU) 2019/881, pružatelj mora biti certificiran u skladu s tim programom u roku od dvije godine od datuma početka primjene tog programa.

---

[23] Uredba (EU) 2024/... Europskog parlamenta i Vijeća od ... o ... (SL L, …, ELI: …).

[+] SL : molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 100/23 (2022/0272(COD)), a u bilješku umetnuti broj, datum, naslov i upućivanje na SL i referentnu internetsku stranicu ELI-ja za tu uredbu.

(k) pružatelj u ponudu mora uključiti uvjete pretvorbe za sve neiskorištene usluge odgovora na incidente koje bi se mogle pretvoriti u usluge pripravnosti koje su usko povezane s odgovorom na incidente, kao što su vježbe ili osposobljavanja.

3. Za potrebe nabave usluga za pričuvu EU-a za kibernetičku sigurnost javni naručitelj može u bliskoj suradnji s državama članicama prema potrebi utvrditi dodatne kriterije i zahtjeve uz one iz stavka 2.

Članak 18.

Djelovanja kojima se podupire uzajamna pomoć

1. Mehanizmom za izvanredne kibernetičke sigurnosne situacije pruža se potpora za tehničku pomoć koju jedna država članica pruža drugoj državi članici pogođenoj značajnim kibernetičkim sigurnosnim incidentom ili kibernetičkim sigurnosnim incidentom velikih razmjera, među ostalim u slučajevima iz članka 11. stavka 3. točke (f) Direktive (EU) 2022/2555.

2. Potpora za uzajamnu tehničku pomoć iz stavka 1. ovog članka pruža se u obliku bespovratnih sredstava i podložno uvjetima predviđenim u relevantnim programima rada kako su navedeni u članku 24. Uredbe (EU) 2021/649.

Članak 19.

Potpora trećim zemljama pridruženim programu Digitalna Europa

1. Treća zemlja pridružena programu Digitalna Europa može zatražiti potporu iz pričuve EU-a za kibernetičku sigurnost ako je sporazumom, kojim je pridružena programu Digitalna Europa, predviđeno sudjelovanje u pričuvi EU-a za kibernetičku sigurnost. Taj sporazum mora sadržavati odredbe kojima se od predmetne treće zemlje pridružene programu Digitalna Europa zahtijeva da ispuni obveze utvrđene u stavcima 2. i 9. ovog članka. Za potrebe sudjelovanja treće zemlje u pričuvi EU-a za kibernetičku sigurnost djelomično pridruživanje treće zemlje programu Digitalna Europa može obuhvaćati pridruživanje ograničeno na operativni cilj iz članka 6. stavka 1. točke (g) Uredbe (EU) 2021/694.

2. U roku od tri mjeseca od sklapanja sporazuma iz stavka 1., a u svakom slučaju prije nego što prime bilo kakvu potporu iz pričuve EU-a za kibernetičku sigurnost, treća zemlja pridružena programu Digitalna Europa Komisiji dostavlja informacije o svojoj kibernetičkoj otpornosti i sposobnostima za upravljanje rizicima, uključujući barem informacije o poduzetim nacionalnim mjerama pripreme za značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente ekvivalentne kibernetičkom sigurnosnom incidentu velikih razmjera, informacije o odgovornim nacionalnim subjektima, uključujući timove za odgovor na računalne sigurnosne incidente ili ekvivalentne subjekte, njihovim sposobnostima i resursima koji su im dodijeljeni. Treća zemlja pridružena programu Digitalna Europa redovito, a najmanje jednom godišnje, ažurira te informacije. Komisija te informacije dostavlja Visokom predstavniku i ENISA-i za potrebe olakšavanja primjene stavka 11.

3. Komisija redovito, a najmanje jednom godišnje, ocjenjuje svaku treću zemlju pridruženu programu Digitalna Europa iz stavka 1. na temelju sljedećih kriterija:

(a) poštuje li ta zemlja uvjete sporazuma iz stavka 1. u mjeri u kojoj se ti uvjeti odnose na sudjelovanje u pričuvi EU-a za kibernetičku sigurnost;

(b) je li ta zemlja poduzela odgovarajuće korake za pripremu za značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente ekvivalentne onima velikih razmjera, na temelju informacija iz stavka 2.; i

(c) je li pružanje potpore u skladu s politikom Unije prema toj zemlji i sveukupnim odnosima s tom zemljom te je li u skladu s drugim politikama Unije u području sigurnosti.

Komisija se pri provedbi ocjenjivanja iz prvog podstavka savjetuje s Visokim predstavnikom u pogledu kriterija iz točke (c) tog podstavka.

Ako Komisija zaključi da treća zemlja pridružena programu Digitalna Europa ispunjava sve uvjete iz prvog podstavka, podnosi prijedlog Vijeću za donošenje provedbenog akta u skladu sa stavkom 4. kojim se odobrava pružanje potpore toj zemlji iz pričuve EU-a za kibernetičku sigurnost.

4. Vijeće može donijeti provedbene akte iz stavka 3.. Ti provedbeni akti primjenjuju se najdulje jednu godinu. Mogu se produljiti. Mogu sadržavati ograničenje broja dana za koje se može pružiti potpora kao odgovor na jedan zahtjev, koje ne smije biti kraće od 75 dana.

Za potrebe ovog članka Vijeće mora djelovati žurno te provedbene akte iz ovog stavka u pravilu donositi u roku od osam tjedana od usvajanja relevantnog prijedloga Komisije u skladu s stavkom 3. trećim podstavkom.

5. Vijeće može na prijedlog Komisije u bilo kojem trenutku izmijeniti ili staviti izvan snage provedbene akte donesene u skladu sa stavkom 4.

Ako Vijeće smatra da je došlo do znatne promjene u pogledu kriterija iz stavka 3. prvog podstavka točke (c), Vijeće može na propisno obrazloženu inicijativu jedne ili više država članica izmijeniti ili staviti izvan snage provedbeni akt donesen u skladu sa stavkom 4.

6. Pri izvršavanju svojih provedbenih ovlasti na temelju ovog članka Vijeće primjenjuje kriterije iz stavka 3. prvog podstavka i objašnjava svoju ocjenu tih kriterija. Posebno, ako djeluje na vlastitu inicijativu u skladu sa stavkom 5. drugim podstavkom, Vijeće objašnjava znatnu promjenu iz tog podstavka.

7. Potpora iz pričuve EU-a za kibernetičku sigurnost pružena trećoj zemlji pridruženoj programu Digitalna Europa mora biti u skladu sa svim posebnim uvjetima utvrđenima u sporazumu iz stavka 1.

8. Korisnici iz trećih zemalja pridruženih programu Digitalna Europa koji ispunjavaju uvjete za primanje usluga iz pričuve EU-a za kibernetičku sigurnost uključuju nadležna tijela kao što su timovi za odgovor na računalne sigurnosne incidente ili ekvivalentni subjekti i tijela za upravljanje kibernetičkim krizama.

9. Svaka treća zemlja pridružena programu Digitalna Europa koja ispunjava uvjete za potporu iz pričuve EU-a za kibernetičku sigurnost imenuje tijelo koje će biti jedinstvena kontaktna točka za potrebe ove Uredbe.

10. Komisija ocjenjuje zahtjeve za potporu iz pričuve EU-a za kibernetičku sigurnost u skladu s ovim člankom. Javni naručitelj može pružiti potporu trećoj zemlji samo ako je i dok je na snazi provedbeni akt Vijeća kojim se odobrava takva potpora u odnosu na tu zemlju donesen na temelju stavka 4. ovog članka. Odgovor se bez nepotrebne odgode šalje korisnicima iz članka 14. stavka 3. točke (c).

11. Po primitku zahtjeva za potporu na temelju ovog članka, Komisija o tome odmah obavješćuje Vijeće. Komisija obavješćuje Vijeće o ocjeni zahtjeva. Komisija također surađuje s Visokim predstavnikom u vezi sa zaprimljenim zahtjevima i primjenom potpore koja je trećim zemljama pridruženima programu Digitalna Europa dodijeljena iz pričuve EU-a za kibernetičku sigurnost. Osim toga, Komisija uzima u obzir i sva stajališta ENISA-e o tim zahtjevima.

Članak 20.

Koordinacija s mehanizmima Unije za upravljanje krizama

1. Kad su značajni kibernetički sigurnosni incidenti, kibernetički sigurnosni incidenti velikih razmjera ili kibernetički sigurnosni incidenti ekvivalentni kibernetičkom sigurnosnom incidentu velikih razmjera posljedica ili uzrok katastrofe kako je definirana u članku 4. točki 1. Odluke br. 1313/2013/EU, potporom odgovoru na takve incidente na temelju ove Uredbe dopunjuju se djelovanja na temelju te odluke ne dovodeći je u pitanje.

2. U slučaju kibernetičkih sigurnosnih incidenata velikih razmjera ili kibernetičkih incidenata ekvivalentnih kibernetičkom sigurnosnom incidentu velikih razmjera zbog kojih se aktiviraju aranžmani za integrirani politički odgovor na krizu na temelju Provedbene odluke (EU) 2018/1993 („aranžmani za IPCR ”), s potporom odgovoru na takve incidente na temelju ove Uredbe postupa se u skladu s relevantnim postupcima u okviru aranžmana za IPCR-a.

Poglavlje IV.
Europski mehanizam za istraživanje kibernetičkih sigurnosnih incidenata

Članak 21.

Europski mehanizam za istraživanje kibernetičkih sigurnosnih incidenata

1. Na zahtjev Komisije ili mreže EU-CyCLONe ENISA, uz potporu mreže CSIRT-ova i odobrenje predmetne države članice, istražuje i procjenjuje kibernetičke prijetnje, poznate iskoristive ranjivosti i mjere ublažavanja s obzirom na određeni značajni kibernetički sigurnosni incident ili kibernetički sigurnosni incident velikih razmjera. Nakon završetka istraživanja i procjenjivanja incidenta te radi izvlačenja pouka iz stečenih iskustava i izbjegavanja ili ublažavanja budućih incidenata ENISA mreži EU-CyCLONe, mreži CSIRT-ova, predmetnim državama članicama i Komisiji dostavlja izvješće o istraživanju incidenta kako bi im pomogla u obavljanju njihovih zadaća, osobito zadaća utvrđenih u člancima 15. i 16. Direktive (EU) 2022/2555,. Ako incident utječe na treću zemlju pridruženu programu Digitalna Europa, ENISA također dostavlja izvješće Vijeću. U takvim slučajevima Komisija izvješće dostavlja Visokom predstavniku.

2. ENISA u pripremi izvješća o istraživanju incidenta iz stavka 1. ovog članka surađuje sa svim relevantnim dionicima, među ostalim predstavnicima država članica, Komisijom, drugim relevantnim institucijama, tijelima, uredima i agencijama Unije, industrijom, uključujući pružatelje upravljanih sigurnosnih usluga, i korisnicima usluga kibernetičke sigurnosti te od njih prikuplja povratne informacije. ENISA prema potrebi, u suradnji s CSIRT-ovima i, ako je relevantno, nadležnim tijelima imenovanim ili osnovanim u skladu s člankom 8. stavkom 1. Direktive (EU) 2022/2555 surađuje i sa subjektima pogođenima značajnim kibernetičkim incidentima ili kibernetičkim sigurnosnim incidentima velikih razmjera. Konzultirani predstavnici dužni su dati informacije o svakom mogućem sukobu interesa.

3. Izvješće o istraživanju incidenta iz stavka 1. ovog članka obuhvaća istraživanje i analizu konkretnog značajnog kibernetičkog sigurnosnog incidenta ili kibernetičkog sigurnosnog incidenta velikih razmjera, uključujući glavne uzroke, poznate iskoristive ranjivosti i stečena iskustva. ENISA osigurava da je izvješće u skladu s pravom Unije ili nacionalnim pravom o zaštiti osjetljivih ili klasificiranih podataka. Ako relevantne države članice ili drugi korisnici iz članka 14. stavka 3. koji su pogođeni tim incidentom to zatraže, podaci informacije u izvješću se anonimiziraju. U njemu se ne navode pojedinosti o aktivno iskorištenim ranjivostima koje su i dalje prisutne.

4. U izvješću o istraživanju incidenta se, prema potrebi, daju preporuke za poboljšanje razine kibernetičke sigurnosti Unije te ono može sadržavati najbolje prakse relevantnih dionika i njihova stečena iskustva.

5. ENISA može izdati javno dostupnu verziju izvješća o istraživanju incidenta. Ta verzija izvješća sadržava samo pouzdane javne informacije ili druge pouzdane informacije uz pristanak predmetnih država članica i, u pogledu informacija koje se odnose na korisnika kako su navedeni u članku 14. stavku 3. točki (b) ili (c), uz suglasnost tog korisnika.

Poglavlje V.
Završne odredbe

Članak 22.

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:

i. umeće se sljedeća točka:

„(aa) pružanje potpore razvoju europskog sustava uzbunjivanja u području kibernetičke sigurnosti uspostavljenog člankom 3. Uredbe (EU) …/… Europskog parlamenta i Vijeća[*+] (‚europski sustav uzbunjivanja u području kibernetičke sigurnosti’), što uključuje razvoj, uvođenje i rad nacionalnih kibernetičkih centara i prekograničnih kibernetičkih centara koji doprinose informiranosti o stanju u Uniji i jačanju kapaciteta Unije za prikupljanje saznanja o kiberprijetnjama;”;

---

[*] Uredba (EU) …2024/… Europskog parlamenta i Vijeća od … o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibernetičkih prijetnji i incidenata, pripremu za njih i odgovor na njih te o izmjeni Uredbe (EU) 2021/649 (Akt o kibernetičkoj solidarnosti) (SL L, …, ELI:…).”;

[+] SL: molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)), a u bilješku umetnuti broj, datum, naslov i upućivanje na SL i referentnu internetsku stranicu ELI-ja za tu uredbu.

ii. dodaje se sljedeća točka:

„(g) uspostava i rad mehanizma za izvanredne kibernetičke sigurnosne situacije uspostavljenog člankom 10. Uredbe (EU) …/…[+], uključujući pričuve EU-a za kibernetičku sigurnost uspostavljene člankom 14. te uredbe („pričuva EU-a za kibernetičku sigurnost”), radi pružanja potpore državama članicama u pripremi za značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera te odgovaranju na njih kao dopune nacionalnim resursima i sposobnostima te drugim oblicima potpore dostupnima na razini Unije, te za pružanje potpore drugim korisnicima u odgovoru na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente ekvivalentne onima velikih razmjera”;

(b) 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[*]. Međutim, pričuvu EU-a za kibernetičku sigurnost provodi Komisija i, u skladu s člankom 14. stavkom 6. Uredbe (EU) …/…[** +], ENISA.

---

[*] 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 centara nacionalnih koordinacijskih (SL L 202, 8.6.2021., str. 1.).

[+] SL: molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

2. članak 9. mijenja se kako slijedi:

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

„(b) 1 760 806 000 EUR za specifični cilj 2 – umjetna inteligencija;

(c) 1 372 020 000 EUR za specifični cilj 3 – kibersigurnost i povjerenje;

(d) 482 640 000 EUR za specifični cilj 4 – napredne digitalne vještine;”;

(b) dodaje se sljedeći stavak:

„8. Odstupajući od članka 12. stavka 1. Financijske uredbe, neiskorištena odobrena sredstva za preuzimanje obveza i za plaćanje za djelovanja u kontekstu primjene pričuve EU-a za kibernetičku sigurnost i djelovanja kojima se podupire uzajamna pomoć na temelju Uredbe …/…[+], kojima se nastoje ostvariti ciljevi utvrđeni u članku 6. stavku 1. točki (g) ove Uredbe automatski se prenose te se za njih mogu preuzeti obveze i mogu se isplatiti do 31. prosinca sljedeće financijske godine. Europski parlament i Vijeće obavješćuju se o odobrenim sredstvima prenesenima u skladu s člankom 12. stavkom 6. Financijske uredbe.”;

[+] SL: molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

3. članak 12. mijenja se kako slijedi:

(a) umeću se sljedeći stavci:

„5.a Stavak 5. ne primjenjuje se, u mjeri u kojoj se odnosi na pravne subjekte s poslovnim nastanom u Uniji, ali pod kontrolom iz trećih zemalja, na bilo koje djelovanje kojim se provodi europski sustav uzbunjivanja u području kibernetičke sigurnosti ako su u pogledu predmetnog djelovanja ispunjena oba sljedeća uvjeta:

(a) postoji stvarni rizik, uzimajući u obzir rezultate pregleda provedenog u skladu s člankom 9. stavkom 4. Uredbe (EU)…/…[+] da pravni subjekti koji imaju poslovni nastan ili za koje se smatra da imaju poslovni nastan u državama članicama i koje kontroliraju države članice ili državljani država članica neće imati alate, infrastrukturu i usluge koji su potrebni i dostatni da se tim djelovanjem na odgovarajući način doprinese cilju europskog sustava uzbunjivanja u području kibernetičke sigurnosti;

(b) sigurnosni rizik nabave od takvih pravnih subjekata u okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti razmjeran je koristima i ne ugrožava ključne sigurnosne interese Unije i njezinih država članica.

[+] SL : molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

5.b Stavak 5. ne primjenjuje se, u mjeri u kojoj se odnosi na pravne subjekte s poslovnim nastanom u Uniji, ali pod kontrolom iz trećih zemalja, na bilo koje djelovanje kojim se provodi pričuva EU-a za kibernetičku sigurnost ako su u pogledu predmetnog djelovanja ispunjena oba sljedeća uvjeta:

(a) postoji stvarni rizik, uzimajući u obzir rezultate izrade pregleda provedenog na temelju članka 14. stavka 6. Uredbe (EU)…/…[+] da pravni subjekti koji imaju poslovni nastan ili za koje se smatra da imaju poslovni nastan u državama članicama i koje kontroliraju države članice ili državljani država članica neće imati tehnologiju, stručno znanje ili kapacitet koji su potrebni i dostatni kako bi pričuva EU-a za kibernetičku sigurnost mogla primjereno obavljati svoje funkcije;

(b) sigurnosni rizik od uključivanja takvih pravnih subjekata u okvir pričuve EU-a za kibernetičku sigurnost razmjeran je koristima i ne ugrožava ključne sigurnosne interese Unije i njezinih država članica.”;

[+] SL : molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

(b) stavak 6. zamjenjuje se sljedećim:

„6. Ako je to propisno opravdano zbog sigurnosnih razloga, programom rada može se predvidjeti i da pravni subjekti s poslovnim nastanom u pridruženim zemljama i pravni subjekti s poslovnim nastanom u Uniji, ali pod kontrolom iz trećih zemalja, mogu biti prihvatljivi za sudjelovanje u svim ili nekim djelovanjima u okviru specifičnih ciljeva 1 i 2 samo ako ispunjavaju zahtjeve koje ti pravni subjekti trebaju ispuniti kako bi se zajamčila zaštita ključnih sigurnosnih interesa Unije i država članica te osigurala zaštita podataka iz klasificiranih dokumenata. Ti se zahtjevi utvrđuju u programu rada.”;

Prvi podstavak primjenjuje se, u mjeri u kojoj se odnosi na pravne subjekte koji imaju poslovni nastan u Uniji, ali su pod kontrolom iz trećih zemalja, na djelovanja u okviru specifičnog cilja 3:

(a) za provedbu europskog sustava uzbunjivanja u području kibernetičke sigurnosti ako se primjenjuje stavak 5.a; i

(b) za provedbu pričuve EU-a za kibernetičku sigurnost ako se primjenjuje stavak 5.b.”;

4. 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* i 2014/25/EU** 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 pričuvu EU-a za kibernetičku sigurnost Komisija i ENISA mogu djelovati kao središnje tijelo za nabavu u ime ili za račun trećih zemalja pridruženih Programu u skladu s člankom 10. ove Uredbe 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 168. stavka 3. Uredbe (EU, Euratom) 2024/2509 Europskog parlamenta i Vijeća[***], zahtjev jedne treće zemlje dovoljan je da se Komisiju ili ENISA-u ovlasti za djelovanje.

Pri provedbi postupaka nabave za pričuvu EU-a za kibernetičku sigurnost Komisija i ENISA mogu djelovati kao središnje tijelo za nabavu u ime ili za račun institucija, tijela, ureda ili 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, uredima ili agencijama Unije. Odstupajući od članka 168. stavka 3. Uredbe (EU, Euratom) 2024/2509, zahtjev jedne institucije, tijela, ureda 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.

---

* 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 094 28.3.2014., str. 65.).

** Direktiva 2014/25/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o nabavi subjekata koji djeluju u sektoru vodnog gospodarstva, energetskom i prometnom sektoru te sektoru poštanskih usluga i stavljanju izvan snage Direktive 2004/17/EZ (SL L 94 28.3.2014., str. 243.).

*** Uredba (EU, Euratom) 2024/2509 Europskog parlamenta i Vijeća od 23. rujna 2024. o financijskim pravilima koja se primjenjuju na opći proračun Unije (SL L, 2024/2509, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).”;

5. umeće se sljedeći članak:

„*Članak 16.a*

Proturječja između pravila

U slučaju djelovanja kojima se provodi europski sustav uzbunjivanja u području kibernetičke sigurnosti primjenjiva pravila su ona utvrđena u člancima 4., 5. i 9. Uredbe (EU) …/…[+]. U slučaju proturječja između odredaba ove Uredbe i članaka 4., 5. i 9. Uredbe (EU) …/…[+], potonji članci imaju prednost i primjenjuju se na ta posebna djelovanja.

[+] SL : molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

U slučaju pričuve EU-a za kibernetičku sigurnost, posebna pravila za sudjelovanje trećih zemalja pridruženih Programu utvrđena su u članku 19. Uredbe (EU) …/…[+]. U slučaju proturječja između odredaba ove Uredbe i članka 17. Uredbe (EU) …/…[+], potonji članci imaju prednost i primjenjuju se na ta posebna djelovanja.”;

6. članak 19. zamjenjuje se sljedećim:

„*Članak 19.*
Bespovratna sredstva

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 kibernetičke sigurnosti („ECCC”) može državama članicama odabranima u skladu s člankom 9. Uredbe (EU) …/… [+] i konzorciju domaćinu iz članka 5. Uredbe (EU) …/..[+] izravno, bez poziva na podnošenje prijedloga, dodijeliti potporu u obliku bespovratnih sredstava.

U skladu s člankom 195. stavkom 1. točkom (d) Financijske uredbe ECCC može državama članicama izravno, bez poziva na podnošenje prijedlogâ, dodijeliti potporu u obliku bespovratnih sredstava za mehanizam za izvanredne kibernetičke sigurnosne situacije.

[+] SL: molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

U pogledu djelovanja kojima se podupire uzajamna pomoć predviđena u članku 18. Uredbe (EU) …/…[+] ECCC obavješćuje Komisiju i ENISA-u o zahtjevima država članica za izravna bespovratna sredstva bez poziva na podnošenje prijedloga.

U pogledu djelovanja kojima podupire uzajamna pomoć predviđena u članku 18. Uredbe (EU) …/…[+] i u skladu s člankom 193. stavkom 2. drugim podstavkom točkom (a) Financijske uredbe, troškovi se u propisno opravdanim slučajevima mogu smatrati prihvatljivima čak i ako su nastali prije podnošenja zahtjeva za bespovratna sredstva.”;

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

Članak 23.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji podložno uvjetima utvrđenima u ovom članku.

2. Ovlast za donošenje delegiranih akata iz članka 14. stavka 7. dodjeljuje se Komisiji na razdoblje od pet godina počevši od … [datum stupanja na snagu ove Uredbe]. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

[+] SL : molimo u tekst umetnuti broj uredbe iz dokumenta PE-CONS 94/24 (2023/0109(COD)).

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 14. stavka 7. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u *Službenom listu Europske unije* ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

6. Delegirani akt donesen na temelju članka 14. stavka 7. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od dva mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 24.

Postupak odbora

1. Komisiji pomaže Odbor za koordinaciju programa Digitalna Europa iz članka 31. stavka 1. Uredbe (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 25.

Evaluacija i preispitivanje

1. Komisija do … [dvije godine od datuma stupanja na snagu ove Uredbe] i najmanje svake četiri godine nakon toga provodi evaluaciju funkcioniranja mjera predviđenih u ovoj Uredbi i podnosi izvješće Europskom parlamentu i Vijeću.

2. Evaluacijom iz stavka 1. posebno se ocjenjuje:

(a) broj uspostavljenih nacionalnih kibernetičkih centara i prekograničnih kibernetičkih centara, opseg informacija koje se dijele, uključujući, ako je moguće, učinak na rad mreže CSIRT-ova, i mjeru u kojoj su oni doprinijeli jačanju zajedničkog otkrivanja kibernetičkih prijetnji i incidenata na razini Unije i informiranosti o stanju u vezi s njima te razvoju najsuvremenijih tehnologija; korištenje financijskih sredstava programa Digitalna Europa za kibernetičke sigurnosne alate, kibernetičku sigurnosnu infrastrukturu ili kibernetičke sigurnosne usluge koje se zajednički nabavljaju; te, ako su informacije dostupne, razinu suradnje između nacionalnih kibernetičkih centara te sektorskih i međusektorskih zajednica ključnih i važnih subjekata kako su navedeni u članku 3. Direktive (EU) 2022/2555;.

(b) upotreba i djelotvornost djelovanja u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije kojima se podupire pripravnost, uključujući osposobljavanje, odgovor na značajne kibernetičke sigurnosne incidente te inicijalni oporavak od značajnih kibernetičkih sigurnosnih incidenata, kibernetičkih sigurnosnih incidenata velikih razmjera i kibernetičkih sigurnosnih incidenata ekvivalentnih kibernetičkom sigurnosnom incidentu velikih razmjera, uključujući korištenje sredstava iz programa Digitalna Europa te stečena iskustva i preporuke proizašle iz provedbe mehanizma za izvanredne kibernetičke sigurnosne situacije;

(c) korištenje i djelotvornost pričuve EU-a za kibernetičku sigurnost u odnosu na vrstu korisnika, uključujući korištenje sredstava iz programa Digitalna Europa, korištenje usluga, uključujući njihovu vrstu, prosječno vrijeme potrebno za odgovor na zahtjeve i za upotrebu pričuve EU-a za kibernetičku sigurnost, postotak usluga pretvorenih u usluge pripravnosti povezane sa sprečavanjem incidenata i odgovorom na njih te stečena iskustva i preporuke proizašle iz primjene pričuve EU-a za kibernetičku sigurnost;

(d) doprinos ove Uredbe jačanju konkurentnog položaja industrije i usluga u Uniji u cijelom digitalnom gospodarstvu, uključujući mikropoduzeća te mala i srednja poduzeća te novoosnovana poduzeća, te doprinos općem cilju jačanja vještina i kapaciteta radne snage u području kibernetičke sigurnosti.

3. Na temelju izvješća navedenih u stavku 1. Komisija, prema potrebi, podnosi zakonodavni prijedlog Europskom parlamentu i Vijeću radi izmjene ove Uredbe.

Članak 26.

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 Bruxellesu

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik/Predsjednica*

PRILOG

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

1. u Prilogu I. odjeljak „Specifični cilj 3 – kibersigurnost i povjerenje” zamjenjuje se sljedećim:

„Specifični cilj 3 – kibersigurnost i povjerenje

Programom se potiče jačanje, izgradnja i stjecanje temeljnih kapaciteta za osiguravanje digitalnoga gospodarstva, društva i demokracije Unije jačanjem industrijskog potencijala i konkurentnosti Unije u području kibersigurnosti te poboljšanjem sposobnosti privatnog i javnog sektora da štite građane i poduzeća od kiberprijetnji, među ostalim podupiranjem provedbe Direktive (EU) 2016/1148.

Početna i, prema potrebi, kasnija djelovanja u okviru ovog cilja uključuju:

1. zajedničko ulaganje s državama članicama u naprednu opremu, infrastrukturu te znanje i iskustvo u području kibersigurnosti koji su temeljni za zaštitu kritičnih infrastruktura i digitalnog jedinstvenog tržišta u cjelini. Takvo zajedničko ulaganje moglo bi uključivati ulaganja u kvantnoračunalne kapacitete i podatkovne resurse za kibersigurnost, informiranost o stanju u kibernetičkom prostoru, uključujući nacionalne i prekogranične kibernetičke centre koji čine europski sustav uzbunjivanja u području kibernetičke sigurnosti, kao i druge alate koji će biti dostupni javnom i privatnom sektoru u Europi;

2. povećanje postojećih tehnoloških kapaciteta i umrežavanje centara za kompetencije u državama članicama te osiguravanje da ti kapaciteti odgovaraju potrebama javnog sektora i industrije, među ostalim putem proizvoda i usluga kojima se povećavaju kibersigurnost i povjerenje unutar digitalnog jedinstvenog tržišta;

3. osiguravanje širokog uvođenja djelotvornih najsuvremenijih rješenja za kibersigurnost i povjerenje u svim državama članicama. Takvo uvođenje obuhvaća povećanje sigurnosti i zaštite proizvoda, od njihova projektiranja do komercijalizacije.;

4. potporu smanjivanju nedostatka vještina u području kibersigurnosti, uzimajući u obzir rodnu ravnotežu, primjerice usklađivanjem programa stjecanja tih vještina, njihovim prilagođavanjem specifičnim sektorskim potrebama i olakšavanjem pristupa ciljanom specijaliziranom osposobljavanju;

5. jačanje solidarnosti među državama članicama pri pripremi za značajne kibernetičke sigurnosne incidente i odgovaranju na njih uvođenjem pružanja kibernetičkih sigurnosnih usluga preko granica, što uključuje potporu za uzajamnu pomoć među javnim tijelima i uspostavu pričuve pouzdanih pružatelja upravljanih sigurnosnih usluga na razini Unije.”;

2. u Prilogu II. odjeljak/poglavlje „Specifični cilj 3 – kibersigurnost i povjerenje” zamjenjuje se sljedećim:

„Specifični cilj 3 – kibersigurnost i povjerenje

3.1. Količina infrastruktura ili alata za kibersigurnost nabavljenih zajedničkom javnom nabavom, uključujući u okviru europskog sustava uzbunjivanja u području kibernetičke sigurnosti

3.2. Broj korisnika i zajednica korisnika s pristupom europskim kapacitetima za kibernetičku sigurnost

3.3 Broj djelovanja kojima se podupire pripravnost i odgovor na kibernetičke sigurnosne incidente u okviru mehanizma za izvanredne kibernetičke sigurnosne situacije”.

U pogledu ovog akta dana je izjava koja se može pronaći u [Ured SL treba navesti: SL C XXX, XX.XX.2024, str. XX] i na sljedećoj poveznici [Ured SL: molimo unijeti poveznicu za izjavu]