Europski parlament
2019-2024

Dokument s plenarne sjednice

A9-0426/2023

8.12.2023

***I
IZVJEŠĆE

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Odbor za industriju, istraživanje i energetiku

Izvjestiteljica: Lina Gálvez Muñoz

Oznake postupaka

*	Postupak savjetovanja
***	Postupak suglasnosti
***I	Redovni zakonodavni postupak (prvo čitanje)
***II	Redovni zakonodavni postupak (drugo čitanje)
***III	Redovni zakonodavni postupak (treće čitanje)

(Navedeni se postupak temelji na pravnoj osnovi predloženoj u nacrtu akta.)

Izmjene nacrta akta

Amandmani Parlamenta u obliku dvaju stupaca

Brisanja su označena ***podebljanim kurzivom*** u lijevom stupcu. Izmjene su označene ***podebljanim kurzivom*** u obama stupcima. Novi tekst označen je ***podebljanim kurzivom*** u desnom stupcu.

U prvom i drugom retku zaglavlja svakog amandmana naznačen je predmetni odlomak iz nacrta akta koji se razmatra. Ako se amandman odnosi na postojeći akt koji se želi izmijeniti nacrtom akta, zaglavlje sadrži i treći redak u kojem se navodi postojeći akt te četvrti redak u kojem se navodi odredba akta na koju se izmjena odnosi.

Amandmani Parlamenta u obliku pročišćenog teksta

Novi dijelovi teksta označuju se ***podebljanim kurzivom***. Brisani dijelovi teksta označuju se oznakom ▌ ili su precrtani. Izmjene se naznačuju tako da se novi tekst označi ***podebljanim kurzivom***, a da se zamijenjeni tekst izbriše ili precrta.
Iznimno, izmjene strogo tehničke prirode koje unesu nadležne službe prilikom izrade konačnog teksta ne označuju se.

SADRŽAJ

Stranica

HR

NACRT ZAKONODAVNE REZOLUCIJE EUROPSKOG PARLAMENTA

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Redovni zakonodavni postupak: prvo čitanje)

Europski parlament,

– uzimajući u obzir Prijedlog Komisije upućen Europskom parlamentu i Vijeću (COM(2023)0209),

– uzimajući u obzir članak 294. stavak 2. i članke 173. stavak 3. te 322. stavak 1. točku (a) Ugovora o funkcioniranju Europske unije, u skladu s kojima je Komisija podnijela Prijedlog Parlamentu (C9-0136/2023),

– uzimajući u obzir članak 294. stavak 3. Ugovora o funkcioniranju Europske unije,

– uzimajući u obzir mišljenje Europskog gospodarskog i socijalnog odbora od 13. srpnja 2023.[1],

– uzimajući u obzir članak 59. Poslovnika,

– uzimajući u obzir mišljenja Odbora za vanjske poslove i Odbora za promet i turizam,

– uzimajući u obzir izvješće Odbora za industriju, istraživanje i energetiku (A9-0426/2023),

1. usvaja sljedeće stajalište u prvom čitanju;

2. odobrava svoju izjavu priloženu ovoj Rezoluciji;

3. poziva Komisiju da predmet ponovno uputi Parlamentu ako zamijeni, bitno izmijeni ili namjerava bitno izmijeniti svoj Prijedlog;

4. nalaže svojoj predsjednici da stajalište Parlamenta proslijedi Vijeću, Komisiji i nacionalnim parlamentima.

[1] SL C 349, 29.9.2023, str. 167.

Amandman 1

AMANDMANI EUROPSKOG PARLAMENTA*

na prijedlog Komisije

2023/0109 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih *i izmjeni Uredbe (EU) 2021/694*

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[2],

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[3],

uzimajući u obzir mišljenje Odbora regija[4],

u skladu s redovnim zakonodavnim postupkom,

budući da:

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

(2) ***Na razini Unije i na globalnoj razini*** povećavaju se razmjeri i učestalost te pogoršavaju posljedice kibernetičkih incidenata ***u pogledu njihovih metoda i učinka***, uključujući napade na lance opskrbe s ciljem kibernetičke špijunaže, napada ucjenjivačkim softverom ili izazivanja poremećaja. Oni predstavljaju veliku prijetnju funkcioniranju

* Amandmani: novi ili izmijenjeni tekst označava se podebljanim kurzivom, a brisani tekst oznakom ▌.

2 SL C […], […], str. […].

3 SL C , , str. .

4 SL C , , str. .

mrežnih i informacijskih sustava. S obzirom na to da se prijetnje brzo mijenjaju, mogući incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu ***gospodarstvima i demokracijama*** na kritičnoj infrastrukturi ***u cijeloj Uniji*** zahtijevaju povećanu pripravnost na svim razinama okvira Unije za kibernetičku sigurnost. Ta prijetnja nadilazi rusku vojnu agresiju na Ukrajinu i vjerojatno će se nastaviti s obzirom na mnoštvo državi bliskih ***i*** kriminalnih ▌aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga i obavljanje gospodarskih djelatnosti, među ostalim u kritičnim ili visokokritičnim sektorima, uzrokovati znatne financijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu Unije te čak imati zdravstvene ili po život opasne posljedice. K tomu, kibernetički sigurnosni incidenti su nepredvidivi jer se često pojavljuju i razvijaju u vrlo kratkim vremenskim razdobljima, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u mnogim zemljama ili se brzo šire na mnoge zemlje. ***Stoga je potrebna bliska i koordinirana suradnja između javnog sektora, privatnog sektora, akademske zajednice i medija. Osim toga, odgovor Unije treba koordinirati s međunarodnim institucijama, kao i s pouzdanim međunarodnim partnerima sličnih stavova. Pouzdani međunarodni partneri sličnih stavova zemlje su koje dijele vrijednosti Unije kao što su demokracija, predanost ljudskim pravima, učinkovit multilateralizam i poredak utemeljen na pravilima, u skladu s okvirima i sporazumima o međunarodnoj suradnji. Kako bi se osigurala suradnja s pouzdanim međunarodnim partnerima sličnih stavova te zaštita od sustavnih suparnika, subjektima s poslovnim nastanom u trećim zemljama koji nisu stranke Sporazuma o javnoj nabavi ne bi trebalo dopustiti sudjelovanje u nabavi na temelju ove Uredbe.***

(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibernetičke sigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe[5], potrebno je povećati otpornost građana, poduzeća, ***posebno mikropoduzeća, malih i srednjih poduzeća (MSP-ovi), uključujući start-up poduzeća,*** i subjekata koji upravljaju kritičnim infrastrukturama, ***uključujući lokalna i regionalna tijela***, na sve veće kibernetičke sigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebni ulaganja u infrastrukturu i usluge ***i izgradnja kapaciteta za razvoj kibernetičkih sigurnosnih vještina*** kojima će se omogućiti brže otkrivanje kibernetičkih sigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoć u boljoj pripremi za značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibernetičkim sigurnosnim prijetnjama i incidentima.

(3.a) Kibernetički napadi često su usmjereni na lokalne, regionalne ili nacionalne javne službe i infrastrukture. Lokalna tijela jedna su od meta koje su najizloženije kibernetičkim napadima jer im nedostaje financijskih i ljudskih resursa. Stoga je posebno važno da donositelji odluka na lokalnoj razini budu svjesni potrebe za povećanjem digitalne otpornosti, povećanjem njihovih kapaciteta za smanjenje učinka kibernetičkih napada i iskorištavanjem mogućnosti predviđenih ovom Uredbom.

[5] https://futureu.europa.eu/hr/

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibernetičkih sigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća[6], Preporuku Komisije (EU) 2017/1584[7], Direktivu 2013/40/EU Europskog parlamenta i Vijeća[8] i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[9]. Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

(5) Zbog sve većih kibernetičkih sigurnosnih rizika i općenito složenih prijetnji te uz očit rizik od brzog prelijevanja kibernetičkih incidenata iz jedne države članice u druge i iz treće zemlje u Uniju, potrebna je snažnija solidarnost na razini Unije kako bi se bolje otkrile kibernetičke sigurnosne prijetnje i incidenti te kako bi se za njih bolje pripremilo**,** ▌ na njih bolje odgovorilo ***i od njih bolje oporavilo***. Države članice pozvale su Komisiju i da predstavi prijedlog o novom Fondu za odgovor na hitne situacije u području kibernetičke sigurnosti u Zaključcima Vijeća o položaju EU-a u pogledu kiberprostora[10].

(6) U Zajedničkoj komunikaciji o politici EU-a o kiberobrani[11] donesenoj 10. studenoga 2022. najavljena je inicijativa EU-a za kibernetičku solidarnost sa sljedećim ciljevima: jačanje zajedničkih kapaciteta EU-a za otkrivanje, informiranost o stanju i odgovor poticanjem uvođenja ***mreže*** EU-a za centre za sigurnosne operacije (SOC-ove), podupiranje postupne izgradnje kibernetičke sigurnosne pričuve na razini EU-a s uslugama pouzdanih privatnih pružatelja usluga i testiranje kritičnih subjekata na moguće ranjivosti na temelju procjena rizika EU-a.

(7) Potrebno je poboljšati otkrivanje kibernetičkih prijetnji i kibernetičkih incidenata u cijeloj Uniji i informiranost o njihovu stanju te ojačati solidarnost unapređenjem pripravnosti država članica i Unije te njihove sposobnosti za ***sprečavanje i*** odgovor na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera. Stoga je potrebno uvesti paneuropsku ***mrežu*** SOC-ova (europski kibernetički štit) kako bi se izgradile i poboljšale zajedničke sposobnosti za otkrivanje i

---

6 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.).

7 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.).

8 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.).*

9 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.).

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

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

informiranost o stanju ***i 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 pomoglo u pripremi za značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih; trebalo bi uspostaviti i mehanizam za istraživanje kibernetičkih sigurnosnih incidenata kako bi se istražili i procijenili određeni značajni incidenti ili incidenti velikih razmjera. Tim se mjerama ne dovode u pitanje članci 107. i 108. Ugovora o funkcioniranju Europske unije (UFEU).

(8) Radi postizanja tih ciljeva neophodno je izmijeniti određene dijelove Uredbe (EU) 2021/694 Europskog parlamenta i Vijeća[12]. Konkretno, ovom bi se Uredbom trebala izmijeniti Uredba (EU) 2021/694 u dijelu koji se odnosi na dodavanje novih operativnih ciljeva povezanih s europskim kibernetičkim štitom 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 prijetnji i odgovor na njih te ojačati prekograničnu suradnju u području kibernetičke sigurnosti. Osim toga, trebalo bi utvrditi posebne uvjete pod kojima se može dodijeliti financijska potpora za te mjere te bi trebalo definirati mehanizme upravljanja i koordinacije potrebne za postizanje predviđenih ciljeva. Druge izmjene Uredbe (EU) 2021/694 trebale bi uključivati opise predloženih mjera u okviru novih operativnih ciljeva, kao i mjerljive pokazatelje za praćenje provedbe tih ciljeva.

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

(9.a) S obzirom na razvoj geopolitičke situacije i sve veće kibernetičke prijetnje (EPP 52) te kako bi se osigurali kontinuitet i daljnji razvoj mjera utvrđenih u ovoj Uredbi nakon 2027., posebno europskog kibernetičkog štita i mehanizma za hitne kibernetičke sigurnosne situacije, potrebno je osigurati posebnu proračunsku liniju u višegodišnjem financijskom okviru za razdoblje 2028. – 2034. Države članice trebale bi nastojati obvezati se i na podupiranje svih potrebnih mjera za smanjenje kibernetičkih prijetnji i kibernetičkih incidenata diljem Unije te na jačanje solidarnosti.

(10) Na ovu se Uredbu primjenjuju horizontalna financijska pravila koja su Europski parlament i Vijeće donijeli na temelju članka 322. UFEU-a. Ta su pravila utvrđena u Uredbi ***(EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća[13]*** 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

---

12 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.).

13 ***Uredba (EU, Euratom) 2018/1046 Europskog parlamenta i Vijeća od 18. srpnja 2018. o financijskim pravilima koja se primjenjuju na opći proračun Unije, o izmjeni uredaba (EU) br. 1296/2013, (EU) br. 1301/2013, (EU) br. 1303/2013, (EU) br. 1304/2013, (EU) br. 1309/2013, (EU) br. 1316/2013, (EU) br. 223/2014, (EU) br. 283/2014 i Odluke br. 541/2014/EU te o stavljanju izvan snage Uredbe (EU, Euratom) br. 966/2012 (SL L 193, 30.7.2018, str. 1., ELI: https://eur-lex.europa.eu/eli/reg/2018/1046/oj?locale=hr).***

uključuju i opći režim uvjetovanosti za zaštitu proračuna Unije kako je utvrđen u Uredbi (EU, Euratom) 2020/2092 Europskog parlamenta i Vijeća[14].

(11) U svrhu dobrog financijskog upravljanja trebalo bi utvrditi posebna pravila za prijenos neiskorištenih odobrenih sredstava za preuzete obveze i odobrenih sredstava za plaćanje. Uz poštovanje načela da se proračun Unije utvrđuje na godišnjoj razini, ovom bi se Uredbom, zbog nepredvidive, neuobičajene i specifične prirode kibernetičkog sigurnosnog okruženja, trebao omogućiti prijenos neiskorištenih sredstava koja premašuju ona utvrđena u ***Uredbi (EU, Euratom) 2018/1046***, čime bi se maksimalno povećao kapacitet mehanizma za izvanredne kibernetičke sigurnosne situacije za potporu državama članicama u djelotvornoj borbi protiv kibernetičkih prijetnji.

(11.a) Mehanizam za izvanredne kibernetičke sigurnosne situacije i kibernetička sigurnosna pričuva EU-a uspostavljeni ovom Uredbom nove su inicijative i nisu bile predviđene pri uspostavi višegodišnjeg financijskog okvira za razdoblje 2021. – 2027., a financiranje tih inicijativa namijenjeno je ograničavanju smanjenja sredstava za druge prioritete programa Digitalna Europa u najvećoj mogućoj mjeri. Iznos financijskih sredstava namijenjenih za kibernetičku sigurnosnu pričuvu EU-a trebalo bi stoga smanjiti te bi ga prvenstveno trebalo povući iz nedodijeljenih razlika do gornje granice višegodišnjeg financijskog okvira ili mobilizirati putem posebnih instrumenata netematskog višegodišnjeg financijskog okvira. Svako namjenjivanje ili preraspodjelu sredstava iz postojećih programa trebalo bi svesti na apsolutno najmanju moguću mjeru kako bi se postojeći programi, posebno Erasmus+, zaštitili od negativnog učinka i kako bi se osiguralo da ti programi mogu ostvariti postavljene ciljeve.

(12) Kako bi se učinkovitije spriječile i procijenile kibernetičke prijetnje i kibernetički incidenti te na njih odgovorilo ***i od njih 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 kibernetičkog napada koji pogađaju te infrastrukture. ***Proaktivan pristup utvrđivanju, ublažavanju i sprečavanju potencijalnih kibernetičkih prijetnji uključuje povećane kapacitete za napredno otkrivanje koji su potrebni za zaustavljanje naprednih trajnih prijetnji. Obavještajni podaci o prijetnjama su informacije koje se prikupljaju, analiziraju i tumače kako bi se razumjele potencijalne prijetnje i rizici. Analizom i korelacijom golemih količina podataka otkrivaju se obrasci, trendovi i pokazatelji ugroženosti koji mogu otkriti zlonamjerne aktivnosti ili ranjivosti.*** Trebalo bi uvesti ***mrežu*** SOC-ova („europski kibernetički štit”), koja se sastoji od nekoliko interoperabilnih prekograničnih platformi, od kojih svaka okuplja nekoliko nacionalnih SOC-ova. Ta bi infrastruktura trebala služiti kibernetičkim sigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijom tehnologijom za napredne alate za prikupljanje i analizu podataka, jačajući kapacitete otkrivanja i upravljanja kibernetičkim tehnologijama i osiguravajući informiranost o stanju u stvarnom vremenu. ***Nacionalni SOC odnosi se na centralizirani kapacitet za kontinuirano prikupljanje obavještajnih informacija o prijetnjama i poboljšanje položaja subjekata pod nacionalnom jurisdikcijom u pogledu kibernetičke sigurnosti sprečavanjem, otkrivanjem i analizom kibernetičkih sigurnosnih prijetnji.*** Ta bi

[14] ***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: https://eur-lex.europa.eu/eli/reg/2020/2092/oj?locale=hr).***

infrastruktura trebala služiti za bolje otkrivanje kibernetičkih sigurnosnih prijetnji i incidenata te na taj način dopunjavati i podržavati subjekte i mreže Unije odgovorne za upravljanje krizama u Uniji, posebno Europsku mrežu organizacija za vezu za kibernetičke krize („EU-CyCLONe”), kako je definirana u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća[15].

(13) ***Kako bi sudjelovala u kibernetičkom štitu, svaka*** bi država članica trebala na nacionalnoj razini imenovati javnopravno tijelo zaduženo za koordinaciju aktivnosti otkrivanja kibernetičkih prijetnji i razmjene informacija u toj državi članici. ***Države članice se potiče da uključe nacionalne kapacitete SOC-a u svoju postojeću kibernetičku strukturu i upravljanje kibernetičkim prostorom kako bi se izbjeglo stvaranje dodatnih razina upravljanja i kako bi se ova Uredba uskladila s postojećim zakonodavnim aktima, uključujući Direktivu 2022/2555.*** Ti nacionalni SOC-ovi trebali bi djelovati kao referentna i pristupna točka na nacionalnoj razini za sudjelovanje ***privatnih i javnih subjekata, a posebno njihovih nacionalnih SOC-ova,*** u europskom kibernetičkom štitu te bi trebali osigurati da se informacije o kibernetičkim prijetnjama dobivene od javnih i privatnih subjekata dijele i prikupljaju na nacionalnoj razini na učinkovit i pojednostavnjen način. ***Nacionalni SOC-ovi trebali bi ojačati suradnju i razmjenu informacija između javnih i privatnih subjekata kako bi se razbili postojeći izoliranu sustavi komunikacije. Pritom mogu podupirati stvaranje modela razmjene podataka te bi trebali olakšati i poticati razmjenu informacija u pouzdanom i sigurnom okruženju. Bliska i koordinirana suradnja javnih i privatnih subjekata ključna je za jačanje otpornosti Unije u području kibernetičke sigurnosti.***

(14) U okviru europskog kibernetičkog štita trebalo bi uspostaviti niz prekograničnih centara za sigurnosne operacije („prekograničnih SOC-ova”). U njima bi se trebali okupiti nacionalni SOC-ovi iz najmanje triju država članica kako bi se u potpunosti ostvarile koristi od otkrivanja prekograničnih prijetnji te dijeljenja informacija i upravljanja njima. Opći cilj prekograničnih SOC-ova trebao bi biti jačanje kapaciteta za analizu, sprečavanje i otkrivanje kibernetičkih sigurnosnih prijetnji te podupiranje proizvodnje visokokvalitetnih obavještajnih podataka, ***uključujući prikupljanje i dijeljenje podataka i informacija o zlonamjernom hakiranju, novorazvijenim zlonamjernim prijetnjama i napadima iskorištavanjem ranjivosti koji još nisu upotrijebljeni u kibernetičkim incidentima i napore u području analize,*** o kibernetičkim sigurnosnim prijetnjama, osobito dijeljenjem podataka iz različitih izvora, javnih ili privatnih te dijeljenjem i zajedničkom uporabom najsuvremenijih alata i zajedničkim razvojem sposobnosti otkrivanja, analize i sprečavanja u pouzdanom ***i sigurnom*** okruženju ***uz potporu ENISA-e u pitanjima povezanima s operativnom suradnjom među državama članicama***. ***Prekogranični SOC-ovi trebali bi olakšati i poticati razmjenu informacija u pouzdanom i sigurnom okruženju te bi im*** se trebali osigurati dodatni kapaciteti, koji se temelje na postojećim SOC-ovima i timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovima) i drugim relevantnim akterima te ih nadopunjuju.

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

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

kapacitete koji su ***ugrađeni u postojeću infrastrukturu za kibernetičku sigurnost, posebno u*** mrežu CSIRT-ova jer bi objedinjavali i dijelili podatke o kibernetičkim sigurnosnim prijetnjama dobivene od javnih i privatnih subjekata***, posebno njihovih SOC-ova***, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsuvremenijim alatima te doprinosili ***tehnološkoj suverenost Unije, njezinoj otvorenoj strateškoj autonomiji, konkurentnosti i otpornosti te razvoju znatnog ekosustava kibernetičke sigurnosti, među ostalim u suradnji s pouzdanim međunarodnim partnerima sličnih stavova***. .

(16) Prekogranični SOC-ovi trebali bi djelovati kao središnja točka koja omogućuje opsežno objedinjavanje relevantnih podataka i obavještajnih podataka o kibernetičkim prijetnjama, omogućiti širenje informacija o prijetnjama među velikim i različitim akterima (npr. timovima za hitne računalne intervencije (CERT-ovima), CSIRT-ovima, centrima za razmjenu i analizu informacija (ISAC-ima), operaterima ključnih infrastruktura) ***kako bi se olakšalo razbijanje postojećih izoliranih sustava komunikacije***. ***Time bi prekogranični SOC-ovi mogli poduprijeti i stvaranje modela razmjene podataka u cijeloj Uniji.*** Informacije koje razmjenjuju sudionici u prekograničnom SOC-u mogle bi uključivati podatke iz mreža i senzora, obavještajne podatke o prijetnjama, pokazatelje ugroženosti i informacije o incidentima, prijetnjama i ranjivostima stavljene u kontekst***, uključujući prikupljanje i razmjenu podataka i informacija o mogućem zlonamjernom hakiranju, novorazvijenim zlonamjernim prijetnjama i napadima iskorištavanjem ranjivosti koji još nisu upotrijebljeni u kibernetičkim incidentima i napore u području analize***. Osim toga, prekogranični SOC-ovi trebali bi sklapati sporazume o suradnji s drugim prekograničnim SOC-ovima.

(17) Nužan preduvjet za pripravnost i koordinaciju na razini Unije u pogledu značajnih kibernetičkih sigurnosnih incidenata i kibernetičkih sigurnosnih incidenata velikih razmjera je da relevantna tijela budu jednako informirana o stanju. Direktivom (EU) 2022/2555 uspostavlja se EU-CyCLONe kako bi se omogućilo koordinirano upravljanje kibernetičkim sigurnosnim incidentima i krizama velikih razmjera na operativnoj razini te kako bi se zajamčila redovita razmjena relevantnih informacija među državama članicama i institucijama, tijelima i agencijama Unije. U Preporuci (EU) 2017/1584 o koordiniranom odgovoru na kibernetičke sigurnosne incidente i krize velikih razmjera navedene su uloge svih relevantnih aktera. U Direktivi (EU) 2022/2555 se podsjeća i na odgovornosti Komisije u okviru Mehanizma Unije za civilnu zaštitu uspostavljenog Odlukom 1313/2013/EU Europskog parlamenta i Vijeća[16], kao i na odgovornost za dostavu analitičkih izvješća za aranžmane za integrirani politički odgovor na krizu (IPCR) na temelju Provedbene odluke (EU) 2018/1993[17]. Kada dobiju informacije povezane s potencijalnim ili aktualnim kibernetičkim incidentima velikih razmjera, prekogranični SOC-ovi stoga bi trebali relevantne informacije proslijediti mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji***, u skladu s Direktivom (EU) 2022/2555***. Konkretno, ovisno o situaciji, informacije koje se dijele mogle bi uključivati tehničke informacije, informacije o prirodi i motivima napadača ili potencijalnog napadača te netehničke informacije više razine o potencijalnom ili aktualnom kibernetičkom

---

16 ***Odluka br. 1313/2013/EU Europskog parlamenta i Vijeća od 17. prosinca 2013. o Mehanizmu Unije za civilnu zaštitu (Tekst značajan za EGP) (***SL L 347, 20.12.2013., str. 924.), ***ELI:*** https://eur-lex.europa.eu/eli/dec/2013/1313/oj?locale=hr***).***

17 ***Provedbena 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: https://eur-lex.europa.eu/eli/dec_impl/2018/1993/oj?locale=hr).***

incidentu velikih razmjera. U tom bi kontekstu dužnu pozornost trebalo posvetiti načelu nužnosti pristupa podacima i potencijalno osjetljivoj prirodi informacija koje se dijele.

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

(19) Kako bi se omogućilo da se opsežna razmjena podataka o kibernetičkim sigurnosnim prijetnjama iz različitih izvora odvija u pouzdanom ***i sigurnom*** okruženju, subjekti koji sudjeluju u europskom kibernetičkom štitu trebali bi biti opremljeni najsuvremenijim i vrlo sigurnim alatima, opremom i infrastrukturom ***te 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.

(20) Prikupljanjem, dijeljenjem i razmjenom podataka europski kibernetički štit trebao bi povećati tehnološku suverenost Unije***, njezinu otvorenu stratešku autonomiju, konkurentnost i otpornost te uspostaviti ekosustav kibernetičke sigurnosti značajan za EU***. Objedinjavanje visokokvalitetnih prilagođenih podataka trebalo bi doprinijeti i razvoju naprednih tehnologija umjetne inteligencije i analitike podataka. ***Umjetna inteligencija je najučinkovitija u kombinaciji s ljudskom analizom. Stoga je kvalificirana radna snaga i dalje ključna za objedinjavanje visokokvalitetnih podataka.*** To bi trebalo omogućiti povezivanjem europskog kibernetičkog štita s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom Uredbom Vijeća (EU) 2021/1173[18].

(21) Iako je europski kibernetički štit civilni projekt, zajednica za kibernetičku obranu mogla bi imati koristi od bolje sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture. Prekogranični SOC-ovi, uz potporu Komisije i Europskog stručnog centra u području kibernetičke sigurnosti (ECCC) te u suradnji s Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”), trebali bi postupno razvijati ***namjenske uvjete pristupa te zaštitne*** protokole i standarde kako bi se omogućila suradnja sa zajednicom za kibernetičku obranu, uključujući uvjete provjere i sigurnosti ***te bi pritom trebali poštovati civilni karakter institucija i odredište financiranja, čime bi se iskoristila sredstva koja su na raspolaganju obrambenoj zajednici***. Razvoj europskog kibernetičkog štita trebao bi biti popraćen razmatranjem načina na koji bi se omogućila buduća suradnja s mrežama i platformama odgovornima za dijeljenje informacija u zajednici za kibernetičku obranu, u bliskoj suradnji s Visokim predstavnikom ***te uz potpuno poštovanje prava i sloboda***.

(22) Dijeljenje informacija među sudionicima europskog kibernetičkog štita trebalo bi biti u skladu s postojećim pravnim zahtjevima, a posebno s pravom Unije i nacionalnim

[18] Uredba Vijeća (EU) 2021/1173 od 13. srpnja 2021. o osnivanju Zajedničkog poduzeća za europsko računalstvo visokih performansi te stavljanju izvan snage Uredbe (EU) 2018/1488 (SL L 256, 19.7.2021., str. 3., ***ELI: https://eur-lex.europa.eu/eli/reg/2021/1173/oj?locale=hr***).

pravom o zaštiti podataka, kao i s pravilima Unije o tržišnom natjecanju kojima se uređuje razmjena informacija. Primatelj informacija trebao bi, ako je obrada osobnih podataka potrebna, provesti tehničke i organizacijske mjere kojima se štite prava i slobode ispitanika te uništiti podatke čim ne budu potrebni za navedenu svrhu te obavijestiti tijelo koje je stavilo podatke na raspolaganje da su podaci uništeni.

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

(24) S obzirom na sve veće rizike i sve veći broj kibernetičkih incidenata koji pogađaju države članice, potrebno je uspostaviti instrument za potporu u kriznim situacijama kako bi se poboljšala otpornost Unije na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera te dopunile mjere država članica hitnom financijskom potporom za pripravnost, odgovor i hitan oporavak osnovnih usluga. Tim bi se instrumentom trebalo omogućiti brzo ***i učinkovito*** pružanje pomoći u definiranim okolnostima i pod jasnim uvjetima te omogućiti pažljivo praćenje i evaluacija uporabe sredstava. Iako glavnu odgovornost za sprečavanje kibernetičkih sigurnosnih incidenata i kriza te pripravnost i odgovor na njih snose 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).

(25) Mehanizmom za izvanredne kibernetičke sigurnosne situacije trebala bi se pružiti potpora državama članicama te bi se trebale dopuniti njihove vlastite mjere i resursi te druge postojeće mogućnosti potpore u slučaju odgovora na značajne kibernetičke sigurnosne incidente i kibernetičke sigurnosne incidente velikih razmjera i hitnog oporavka od njih, kao što su usluge koje pruža Agencija Europske unije za kibersigurnost (ENISA) u skladu sa svojim mandatom, koordinirani odgovor i pomoć mreže CSIRT-ova, potpora za ublažavanje posljedica koju pruža EU-CyCLONe, te uzajamna pomoć među državama članicama, među ostalim u kontekstu članka 42. stavka 7. UEU-a, timovi za brz odgovor na kibernetičke incidente u okviru PESCO-a[19] i timovi za brz odgovor na hibridne prijetnje. Njime bi se trebalo odgovoriti na potrebu da se osigura dostupnost specijaliziranih sredstava za potporu pripravnosti i odgovoru na kibernetičke sigurnosne incidente u cijeloj Uniji i u trećim zemljama.

(26) Ovim se instrumentom ne dovode u pitanje postupci i okviri za koordinaciju odgovora na krizu na razini Unije, posebno Mehanizam Unije za civilnu zaštitu[20], IPCR[21], i Direktiva (EU) 2022/2555. Može doprinijeti ili dopuniti mjere koje su donesene u kontekstu članka 42. stavka 7. UEU-a ili u situacijama definiranima u članku 222. UFEU-a. Uporabu ovog instrumenta trebalo bi, prema potrebi, koordinirati i s provedbom mjera u okviru alata za kibernetičku diplomaciju.

---

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

20 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.).

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

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

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

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

2022/2554 Europskog parlamenta i Vijeća[22]. Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

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

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

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

(33) Na razini Unije trebalo bi postupno uspostaviti kibernetičku sigurnosnu pričuvu koja bi se sastojala od usluga privatnih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i hitne mjere oporavka u slučajevima značajnih kibernetičkih sigurnosnih incidenata ili kibernetičkih sigurnosnih incidenata velikih razmjera. Kibernetička sigurnosna pričuva EU-a trebala bi osigurati dostupnost i spremnost usluga, ***usporedo s jačanjem otpornost Unije, uključujući sudjelovanje europskih pružatelja upravljanih sigurnosnih usluga koji su MSP-ovi te osiguravanje stvaranja kibernetičkog sigurnosnog ekosustava, posebice za mikropoduzeća i MSP-ove, uključujući start-up poduzeća, ulaganjem u istraživanje i inovacije radi razvoja najsuvremenijih tehnologija, kao što su tehnologije povezane s računalstvom u oblaku i umjetnom inteligencijom***. ***Pouzdani pružatelji usluga, uključujući MSP-ove, trebali bi moći međusobno surađivati kako bi ispunili prethodno navedene kriterije.*** Usluge iz kibernetičke sigurnosne pričuve EU-a trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima koji djeluju u kritičnim ili visokokritičnim sektorima te nadopunjavati njihovo djelovanje na nacionalnoj razini. ***Stoga bi se kibernetičkom sigurnosnom pričuvom trebala poticati ulaganja u istraživanje i inovacije kako bi se potaknuo razvoj tih tehnologija. Prema potrebi, mogle bi se provoditi zajedničke vježbe s pouzdanim pružateljima i potencijalnim korisnicima kibernetičke sigurnosne pričuve kako bi se, tamo gdje je to potrebno, osiguralo učinkovito funkcioniranje te pričuve.*** Pri podnošenju zahtjeva za potporu iz

[22] 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.

kibernetičke sigurnosne pričuve EU-a države članice trebale bi navesti vrstu potpore pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni zahtjeva države članice. Usluge iz kibernetičke sigurnosne pričuve EU-a mogu služiti i za potporu institucijama, tijelima***, uredima*** i agencijama Unije pod sličnim uvjetima. ***Komisija bi trebala osigurati sudjelovanje država članica i opsežne razmjene s njima kako bi se izbjeglo preklapanje sličnih inicijativa, među ostalim u okviru Organizacije sjevernoatlantskog ugovora (NATO).***

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

(35) Kako bi pridonijela uspostavi kibernetičke sigurnosne pričuve EU-a, Komisija bi mogla razmotriti mogućnost da od ENISA-e zatraži izradu prijedloga programa certifikacije u skladu s Uredbom (EU) 2019/881 za upravljane sigurnosne usluge u područjima obuhvaćenima mehanizmom za izvanredne kibernetičke sigurnosne situacije. ***Kako bi ispunila dodatne zadaće koje proizlaze iz te odredbe, ENISA bi trebala dobiti odgovarajuća dodatna sredstva.***

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

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

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

(37.a) U skladu s ovom Uredbom treće zemlje mogle bi pristupiti resursima i potpori koristeći se potporom za odgovor na incidente iz kibernetičke sigurnosne pričuve EU-a. Nadalje, za pružanje posebnih usluga u okviru kibernetičke sigurnosne pričuve EU-a mogli bi biti potrebni pružatelji usluga odgovora na incidente iz trećih zemalja, uključujući treće zemlje pridružene programu Digitalna Europa ili druge međunarodne partnerske zemlje ili članice NATO-a. Odstupajući od Uredbe (EU, Euratom) 2018/1046, kako bi se ojačao tehnološki suverenitet Unije, njezina otvorena strateška autonomija, konkurentnost i otpornost te kako bi se zaštitila strateška imovina, interesi ili sigurnost Unije, ne bi se smjelo dopustiti sudjelovanje subjektima s poslovnim nastanom u trećim zemljama koji nisu sudionici Sporazuma o javnoj nabavi i koji ne podliježu provjerama u smislu Uredbe (EU) 2019/452 Europskog parlamenta i Vijeća[23] te, prema potrebi, mjerama ublažavanja, uzimajući u obzir ciljeve utvrđene u ovoj Uredbi. Vanjska dimenzija ove Uredbe trebala bi biti u skladu s odredbama utvrđenima u Sporazumu o pridruživanju u okviru programa Digitalna Europa. Sudjelovanje trećih zemalja trebalo bi podlijegati javnom nadzoru, uz sudjelovanje zakonodavnih vlasti, kako bi se građanima osiguralo sudjelovanje u postupku.

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

***** ***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).***

(38.a) Za učinkovitu provedbu europskog kibernetičkog štita i mehanizma za izvanredne kibernetičke sigurnosne situacije od ključne je važnosti kvalificirano osoblje, koje

---

[23] Uredba (EU) 2019/452 Europskog parlamenta i Vijeća od 19. ožujka 2019. o uspostavi okvira za provjeru izravnih stranih ulaganja u Uniji (SL L 79I, 21.3.2019., str. 1.), ELI: http://data.europa.eu/eli/reg/2019/452/oj.

može pouzdano pružati relevantne kibernetičke sigurnosne usluge po najvišim standardima. Stoga zabrinjava činjenica da se Unija suočava s nedostatkom talenata, koji karakterizira manjak kvalificiranih stručnjaka, dok se istovremeno suočava i s prijetnjama koje se brzo mijenjaju, kako je potvrđeno u Komunikaciji Komisije od 18. travnja 2023. o akademiji za vještine u području kibernetičke sigurnosti. Važno je premostiti taj nedostatak talenata jačanjem suradnje i koordinacije među različitim dionicima, uključujući privatni sektor, akademsku zajednicu, države članice, Komisiju i ENISA-u, kako bi se u svim regijama povećala i stvorila sinergija za ulaganja u obrazovanje i osposobljavanje, razvoj javno-privatnih partnerstava, potporu inicijativama za istraživanje i inovacije, razvoj i uzajamno priznavanje zajedničkih standarda te certificiranje vještina u području kibernetičke sigurnosti, među ostalim putem Europskog okvira vještina za kibernetičku sigurnost. Time bi se također trebala olakšati mobilnost stručnjaka u području kibernetičke sigurnosti unutar Unije. Cilj ove Uredbe trebao bi biti promicanje raznolikije radne snage u području kibernetičke sigurnosti. Za sve mjere usmjerene na povećanje vještina u području kibernetičke sigurnosti potrebne su zaštitne mjere kako bi se izbjegao „odljev mozgova" i rizik za mobilnost radne snage.

(38.b) Potrebno je jačanje specijaliziranih, interdisciplinarnih i općih vještina i kompetencija diljem Unije, s posebnim naglaskom na žene, s obzirom na to da u području kibernetičke sigurnosti i dalje postoji rodni jaz, a žene čine 20 % prosječne prisutnosti u svijetu. Žene moraju biti prisutne i dio osmišljavanja digitalne budućnosti i njezina upravljanja.

(38.c) Jačanjem istraživanja i inovacija u području kibernetičke sigurnosti trebala bi se povećati otpornost i otvorena strateška autonomija Unije. Slično tome, važno je stvoriti sinergije s programima istraživanja i inovacija i s postojećim instrumentima i institucijama te ojačati suradnju i koordinaciju među različitim dionicima, uključujući privatni sektor, civilno društvo, akademsku zajednicu, države članice, Komisiju i ENISA-u.

(38.d) Ovom bi se Uredbom trebala ispuniti obveza iz Europske deklaracije o digitalnim pravima i načelima za digitalno desetljeće koja je povezana sa zaštitom interesa naših demokracija, ljudi, poduzeća i javnih institucija od kibernetičkih sigurnosnih rizika i kibernetičkog kriminaliteta, uključujući povrede podataka i krađu identiteta ili manipulaciju njime. Primjena ove Uredbe trebala bi doprinijeti i boljoj provedbi drugog zakonodavstva, primjerice zakonodavstva o umjetnoj inteligenciji, privatnosti podataka i propisima o podacima u pogledu kibernetičke sigurnosti i kibernetičke otpornosti.

(38.e) Za uspješnu provedbu ove Uredbe bit će ključno povećanje kulture kibernetičke sigurnosti koja obuhvaća sigurnost, uključujući sigurnost digitalnog okruženja kao javnog dobra. Stoga bi razvoj mjera za uključivanje građana i podizanje njihove svijesti trebao biti još jedan način jamčenja zaštite naših demokracija i temeljnih vrijednosti.

(38.f) 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 utvrdili uvjeti za interoperabilnost između prekograničnih SOC-ova, uspostavili postupovni aranžmani za razmjenu informacija između prekograničnih SOC-ova s jedne strane i mreže EU-CyCLONe, mreže CSIRT-ova i Komisije s druge strane, utvrdile vrste i broj usluga odgovora potrebnih za kibernetičku sigurnosnu pričuvu

EU-a te dodatno utvrdili detaljni aranžmani za dodjelu usluga potpore za kibernetičku sigurnosnu pričuvu EU-a. 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.* 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.

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

(39) ***S obzirom na to da ciljeve*** ove Uredbe, ***to jest jačanje kapaciteta Unije za sprečavanje i otkrivanje kibernetičkih prijetnji, odgovor na njih i oporavak od njih te uspostavljanje općeg okvira za uklanjanje komunikacijske izoliranosti, ne mogu dostatno ostvariti države članice, nego se oni na bolji način mogu*** ostvariti na razini Unije. Stoga Unija može donijeti mjere u skladu s načelima supsidijarnosti i proporcionalnosti utvrđenima u članku 5. Ugovora o Europskoj uniji. ***U skladu s načelom proporcionalnosti utvrđenim u tom članku,*** ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

DONIJELI SU OVU UREDBU:

Poglavlje I.

OPĆI CILJEVI, PREDMET I DEFINICIJE

Članak 1.

Predmet i ciljevi

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

(a) uvođenjem paneuropske ***mreže*** centara za sigurnosne operacije („europski kibernetički štit”) radi razvoja i poboljšanja zajedničkih sposobnosti za otkrivanje i informiranost o stanju;

(b) uspostavom 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 i hitnom oporavku od njih;

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

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

(a) poboljšanja zajedničkog otkrivanja kibernetičkih prijetnji i kibernetičkih incidenata te zajedničke informiranosti o njihovu stanju u Uniji da bi se ***omogućila potpora industrijskim kapacitetima Unije i država članica u sektoru kibernetičke sigurnosti te*** učvršćivanje konkurentnog položaja industrijskog ***sektora, posebno mikropoduzeća i MSP-ova, uključujući start-up poduzeća,*** i uslužnog sektora u Uniji u cijelom digitalnom gospodarstvu te doprinijelo tehnološkom suverenitetu Unije***, njezinoj otvorenoj strateškoj autonomiji, konkurentnosti i otpornosti u tom sektoru, uz jačanje kibernetičkog sigurnosnog ekosustava s ciljem osiguravanja snažnih sposobnosti Unije, među ostalim u suradnji s međunarodnim partnerima***;

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

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

(ca) koordiniranog razvijanja vještina, sposobnosti stručnog znanja i kompetencija radne snage kako bi se osigurala kibernetička sigurnost i stvorile sinergije s Akademijom za vještine u području kibernetičke sigurnosti.

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

Članak 2.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

-1.a „nacionalni centar za sigurnosne operacije” ili „nacionalni SOC” znači centralizirani nacionalni kapacitet za kontinuirano prikupljanje i analizu obavještajnih informacija o kibernetičkim prijetnjama i poboljšanje položaja u pogledu kibernetičke sigurnosti u skladu s člankom 4.;

1. „**prekogranični centar za sigurnosne operacije**” ili „**prekogranični SOC**” znači višedržavna platforma na kojoj su, u koordiniranoj mrežnoj strukturi, okupljeni nacionalni SOC-ovi ***u skladu s člankom 5.***;

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

3. „**konzorcij domaćin**” znači konzorcij sastavljen od država sudionica, koje predstavljaju nacionalni SOC-ovi, ***u skladu s člankom 5.***;

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

4.a „kritični subjekt” znači kritični subjekt kako je definiran u članku 2. točki 1. Direktive (EU) 2022/2557 Europskog parlamenta i Vijeća[25];

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

5.a „postupanje s incidentom” znači postupanje s incidentom kako je definirano u članku 6. točki 8. Direktive (EU) 2022/2555;

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

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

6.a „ozbiljna kibernetička prijetnja” znači ozbiljna kibernetička prijetnja kako je definirana u članku 6. točki 11. Direktive (EU) 2022/2555;

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

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

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

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

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

11. „**pouzdani pružatelji *upravljanih sigurnosnih usluga***” znači pružatelji upravljanih sigurnosnih usluga odabrani ***za uključivanje u kibernetičku sigurnosnu pričuvu EU-a*** u skladu s člankom 16. ove Uredbe.

---

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

[25] ***Direktiva (EU) 2022/2557 Europskog parlamenta i Vijeća od 14. prosinca 2022. o otpornosti kritičnih subjekata i o stavljanju izvan snage Direktive Vijeća 2008/114/EZ (SL L 333, 27.12.2022., str. 164., ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***

Poglavlje II.

EUROPSKI KIBERNETIČKI ŠTIT

Članak 3.

Uspostava europskog kibernetičkog štita

1. Uspostavlja se ***mreža*** centara za sigurnosne operacije („europski kibernetički štit”) radi razvoja naprednih sposobnosti Unije za otkrivanje, analizu i obradu podataka o kibernetičkim prijetnjama i ***sprečavanje incidenata*** u Uniji. Sastoji se od svih nacionalnih centara za sigurnosne operacije („nacionalni SOC-ovi”) i prekograničnih centara za sigurnosne operacije („prekogranični SOC-ovi”).

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

2. 2. Europski kibernetički štit:

(a) objedinjuje i dijeli podatke o kibernetičkim prijetnjama i kibernetičkim incidentima iz raznih izvora putem prekograničnih SOC-ova ***i po potrebi razmjenjuje informacije s mrežom CSIRT-ova***;

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

(c) doprinosi boljoj zaštiti i odgovoru na kibernetičke prijetnje***, među ostalim davanjem konkretnih preporuka subjektima***;

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

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

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

Članak 4.

Nacionalni centri za sigurnosne operacije

1. Kako bi mogla sudjelovati u europskom kibernetičkom štitu, svaka država članica imenuje barem jedan nacionalni SOC. Nacionalni SOC mora biti ***centralizirani kapacitet u javnopravnom tijelu***. ***Kad je to moguće, nacionalni SOC-ovi uključuju se u CSIRT-ove ili drugu postojeću kibernetičku sigurnosnu infrastrukturu i upravljanje.***

Mora moći služiti drugim javnim i privatnim organizacijama na nacionalnoj razini***, a posebno njihovim nacionalnim SOC-ovima,*** kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibernetičkim sigurnosnim prijetnjama i incidentima ***i po potrebi razmjenu tih informacija s članovima mreže CSIRT-ova iz te države članice*** te za doprinos prekograničnom SOC-u. Mora biti opremljen najsuvremenijim tehnologijama za ***sprečavanje,*** otkrivanje, agregiranje i analiziranje podataka relevantnih za kibernetičke sigurnosne prijetnje i incidente.

Nacionalni SOC ili CSIRT može od pružatelja upravljanih sigurnosnih usluga koji pružaju uslugu kritičnom subjektu zatražiti telemetriju, senzore ili bilježenje podataka svojih nacionalnih kritičnih subjekata. Ti se podaci razmjenjuju u skladu s pravom Unije o zaštiti podataka i isključivo u svrhu pružanja potpore nacionalnom SOC-u ili CSIRT-u u otkrivanju i sprečavanju kibernetičkih sigurnosnih prijetnji i incidenata.

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

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

Članak 5.

Prekogranični centri za sigurnosne operacije

1. Konzorcij domaćin koji čine najmanje tri države članice, koje predstavljaju nacionalni SOC-ovi, koje su se obvezale međusobno surađivati radi koordinacije svojih aktivnosti otkrivanja i

praćenja kibernetičkih prijetnji ima pravo sudjelovati u aktivnostima za uspostavu prekograničnog SOC-a. ***Prekogranični SOC osmišljen je za otkrivanje i analizu kibernetičkih prijetnji, sprečavanje incidenata i podupiranje proizvodnje visokokvalitetnih obavještajnih podataka, posebno preko razmjene podataka iz različitih javnih i privatnih izvora, kao i preko dijeljenja najsuvremenijih alata te zajedničkog razvoja kibernetičkih kapaciteta za otkrivanje, analizu, prevenciju i zaštitu u pouzdanom i sigurnom okruženju.***

2. Nakon poziva na iskaz interesa ECCC ***može odabrati*** konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski doprinos Unije pokriva do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva konzorcij domaćin. Prije pokretanja postupka nabave alata i infrastrukture ECCC i konzorcij domaćin sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.

2.a Odstupajući od članka 176. Uredbe (EU, Euratom) 2018/1046, subjekti s poslovnim nastanom u trećim zemljama koji nisu stranke Sporazuma o javnoj nabavi ne sudjeluju u zajedničkoj nabavi alata i infrastrukture.

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

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

Članak 6.

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

1. Članovi konzorcija domaćina unutar prekograničnog SOC-a međusobno razmjenjuju relevantne informacije kao što su informacije o kibernetičkim prijetnjama, izbjegnutim incidentima, ranjivostima, tehnikama i postupcima, pokazateljima ugroženosti, neprijateljskim taktikama i počiniteljima prijetnji, kibernetičko sigurnosna upozorenja te preporuke za konfiguriranje kibernetičkih sigurnosnih alata za otkrivanje kibernetičkih napada ako takva razmjena informacija:

(a) ***poboljšava razmjenu obavještajnih podataka o kibernetičkim prijetnjama između nacionalnih i prekograničnih SOC-ova i sektorskih ISAC-a u cilju sprečavanja, otkrivanja ili ublažavanja prijetnji;***

(b) povećava razinu kibernetičke sigurnosti, posebno 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 ili fazama odgovora i oporavka ili promicanjem suradnje na istraživanju prijetnji između javnih i privatnih subjekata.

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

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

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

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

3. Kako bi potaknuli razmjenu informacija ***među*** prekograničnim SOC-ovima ***i sa sektorskim ISAC-ovima***, prekogranični SOC-ovi osiguravaju visoku razinu interoperabilnosti među sobom ***i, ako je to moguće, sa sektorskim ISAC-ovima***. Kako bi se olakšala interoperabilnost među prekograničnim SOC-ovima ***i sa sektorskim ISAC-ovima, standardi i protokoli za razmjenu informacija mogu se uskladiti s međunarodnim standardima i najboljim sektorskim praksama***. ***Potiče se i zajednička nabava kibernetičkih infrastruktura, usluga i alata. Nadalje,*** nakon savjetovanja s ECCC-om ***i ENISA-om, Komisiji se daje ovlast da do... [šest mjeseci od datuma stupanja na snagu ove Uredbe] donese delegirane akte u skladu s člankom 20.a radi dopune ove Uredbe utvrđivanjem*** uvjeta za tu interoperabilnost ***u bliskoj suradnji s prekograničnim SOC-ovima i na temelju međunarodnih normi i najboljih sektorskih praksi***.

4. Prekogranični SOC-ovi sklapaju sporazume o suradnji međusobno ***i, prema potrebi, sa sektorskim ISAC-ovima,*** u kojima se utvrđuju načela razmjene informacija ***i interoperabilnosti*** među prekograničnim platformama***, uzimajući u obzir već postojeće relevantne mehanizme za razmjenu informacija utvrđene u Direktivi (EU) 2022/2555***. ***Prekogranični SOC-ovi, kada je to primjereno, sklapaju sporazume o suradnji sa sektorskim ISAC-ovima. U kontekstu potencijalnog ili aktualnog kibernetičkog sigurnosnog incidenta velikih razmjera, mehanizmi za razmjenu informacija moraju biti u skladu s relevantnim odredbama Direktive (EU) 2022/2555.***

Članak 7.

Suradnja i dijeljenje informacija s *mrežom CSIRT-ova*

1. Ako prekogranični SOC-ovi dobiju informacije o potencijalnom ili aktualnom kibernetičkom sigurnosnom incidentu velikih razmjera ***u svrhu zajedničke informiranosti o situaciji, koordinacijski SOC*** bez nepotrebne odgode dostavlja relevantne informacije ***svojem CSIRT-u ili nadležnom tijelu, koji će o tome izvijestiti*** mrežu EU-CyCLONe, mrežu CSIRT-ova te Komisiju ***i ENISA-u, u skladu s*** njihovim ulogama u upravljanju krizama ***i postupcima*** u skladu s Direktivom (EU) 2022/2555. ***Ovim se stavkom javnim ili privatnim subjektima ne nameću dodatne obveze u pogledu obavješćivanja o potencijalnom ili aktualnom kibernetičkom sigurnosnom incidentu velikih razmjera radi ispunjavanja obveza utvrđenih u Direktivi (EU) 2022/2555.***

2. Komisija ***je ovlaštena donijeti delegirane akte u skladu s člankom 20.a nakon savjetovanja s mrežom CSIRT-ova radi dopune ove Uredbe utvrđivanjem*** postupovnih aranžmana za dijeljenje informacija iz stavka 1. ***ovog članka i u skladu s Direktivom (EU) 2022/2555***.

Članak 8.

Sigurnost

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

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

3. Komisija može donijeti provedbene akte kojima se utvrđuju tehnički zahtjevi za ispunjavanje obveze država članica propisane u stavcima 1. i 2. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2. ove Uredbe. ***Oni moraju biti u skladu s direktivama (EU) 2022/2555 i (EU) 2022/2557.*** Kako bi se olakšala suradnja s vojnim akterima, Komisija ***u svojim provedbenim aktima***, uz podršku Visokog predstavnika, uzima u obzir relevantne obrambene sigurnosne standarde.

Poglavlje III.

MEHANIZAM ZA IZVANREDNE KIBERNETIČKE SIGURNOSNE SITUACIJE

Članak 9.

Uspostava mehanizma za izvanredne *kibernetičke sigurnosne* situacije

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

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

Članak 10.

Vrste mjera

1. Mehanizmom se podupiru sljedeće vrste mjera:

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

(b) mjere odgovora, kojima se doprinosi odgovoru na značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera i hitnom oporavku od njih, koje trebaju poduzeti pouzdani pružatelji ***upravljanih sigurnosnih usluga*** koji sudjeluju u kibernetičkoj sigurnosnoj pričuvi EU-a uspostavljenoj člankom 12.;

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

1.a Komisija nakon aktivacije mehanizma, na godišnjoj osnovi, provodi procjenu kako pozitivnih tako i negativnih aspekata funkcioniranja mehanizma, među ostalim i kada je riječ o tome jesu li potrebni dodatni zahtjevi u pogledu suradnje ili osposobljavanja, te o tome objavljuje izvješće.

Članak 11.

Koordinirano testiranje pripravnosti subjekata

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

2. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava izrađuje, u suradnji s Komisijom, ENISA-om i Visokim predstavnikom ***te tijelima koja podliježu koordiniranom testiranju pripravnosti u skladu sa stavkom 1.***, zajedničke scenarije rizika i metodologije za koordinirana testiranja ***pripravnosti, koji rezultiraju koordiniranim planom rada***. ***Subjekti koji podliježu koordiniranom testiranju pripravnosti izrađuju i provode plan s korektivnim mjerama u kojem se provode preporuke koje proizlaze iz testiranja pripravnosti.***

Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava može pomoći u određivanju kojim sektorima ili podsektorima treba dati prednost za koordinirano testiranje pripravnosti.

Članak 12.

Uspostava kibernetičke sigurnosne pričuve EU-a

1. Uspostavlja se kibernetička sigurnosna pričuva EU-a radi pomaganja korisnicima iz stavka 3. pri odgovaranju ili pružanju potpore za odgovaranje na značajne kibernetičke

sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera i hitan oporavak od takvih incidenata.

Ako je očito da se nabavljene usluge ne mogu u potpunosti iskoristiti za pružanje potpore za odgovor na značajne incidente ili incidente velikih razmjera, te se usluge iznimno mogu prenamijeniti za vježbe ili osposobljavanje za odgovaranje na incidente te ih javni naručitelj može staviti na raspolaganje korisnicima na njihov zahtjev.

2. Kibernetičku sigurnosnu pričuvu EU-a čine usluge odgovora na incidente koje pružaju pouzdani pružatelji ***upravljanih sigurnosnih usluga*** odabrani u skladu s kriterijima iz članka 16. ***Kibernetička sigurnosna pričuva EU-a*** obuhvaća unaprijed dogovorene usluge. Pružanje tih usluga mora biti moguće u svim državama članicama ***te se njima jača tehnološki suverenitet Unije, njezina otvorena strateška autonomija, konkurentnost i otpornost u sektoru kibernetičke sigurnosti, među ostalim poticanjem inovacija na digitalnom jedinstvenom tržištu u cijeloj Uniji***.

3. Korisnici usluga iz kibernetičke sigurnosne pričuve EU-a uključuju:

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

(b) institucije, tijela i agencije Unije ***iz članka 3. stavka 1. Uredbe (EU).../2023 Europskog parlamenta i Vijeća[26] i CERT-EU-a.***

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

5. Komisija je općenito odgovorna za primjenu kibernetičke sigurnosne pričuve EU-a. Komisija određuje prioritete i razvoj kibernetičke sigurnosne pričuve EU-a ***u suradnji s koordinacijskom skupinom za NIS 2 i*** u skladu sa zahtjevima korisnika iz stavka 3. i nadzire njezinu primjenu te se brine za komplementarnost, dosljednost, sinergije i veze s drugim mjerama potpore na temelju ove Uredbe, kao i s drugim mjerama i programima Unije.

6. Komisija sporazumima o doprinosu rad i vođenje kibernetičke sigurnosne pričuve EU-a u cijelosti ili djelomično ***povjerava*** ENISA-i.

7. Kako bi pomogla Komisiji u uspostavi kibernetičke sigurnosne pričuve EU-a, ENISA izrađuje pregled potrebnih usluga***, uključujući potrebne vještine i kapacitete radne snage u području kibernetičke sigurnosti,*** nakon savjetovanja s državama članicama i Komisijom, ***te, prema potrebi, pružateljima upravljanih sigurnosnih usluga i drugim predstavnicima industrije kibernetičke sigurnosti***. ENISA, nakon savjetovanja s Komisijom***, pružateljima upravljanih sigurnosnih usluga i, prema potrebi, drugim predstavnicima industrije kibernetičke sigurnosti,*** sličan pregled izrađuje i kako bi utvrdila potrebe trećih zemalja koje ispunjavaju uvjete za potporu iz kibernetičke sigurnosne pričuve EU-a na temelju članka 17. Komisija se, prema potrebi, savjetuje s Visokim predstavnikom ***i obavješćuje Vijeće o potrebama trećih zemalja***.

---

[26] ***Uredba (EU) .../2023 o utvrđivanju mjera za visoku zajedničku razinu kibernetičke sigurnosti u institucijama, tijelima, uredima i agencijama Unije (SL C , , str, , ELI: ...).***

8. Komisija ***je ovlaštena za donošenje delegiranih akata u skladu s člankom 20.a radi dopune ove Uredbe utvrđivanjem*** vrste i broja usluga odgovora potrebnih za kibernetičku sigurnosnu pričuvu EU-a. ▌..

Članak 13.

Zahtjevi za potporu iz kibernetičke sigurnosne pričuve EU-a

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

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

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

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

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

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

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

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

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

7. Komisija ***je ovlaštena donositi delegirane akte u skladu s člankom 20.a radi dopune ove Uredbe utvrđivanjem*** detaljnih aranžmana za dodjelu usluga potpore iz kibernetičke sigurnosne pričuve EU-a. ▌

Članak 14.

Ostvarivanje potpore iz kibernetičke sigurnosne pričuve EU-a

1. Zahtjeve za potporu iz kibernetičke sigurnosne pričuve EU-a ocjenjuje Komisija uz potporu ENISA-e ili kako je definirano u sporazumima o doprinosu na temelju članka 12. stavka 6., a

odgovor na zahtjev se bez ***nepotrebne*** odgode***, a u svakom slučaju u roku od 24 sata,*** šalje korisnicima iz članka 12. stavka 3.

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

(a) ozbiljnost kibernetičkog sigurnosnog incidenta;

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

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

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

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

3. Usluge kibernetičke sigurnosne pričuve EU-a pružaju se u skladu s posebnim sporazumima između pružatelja usluga i korisnika kojem se pruža potpora iz kibernetičke sigurnosne pričuve EU-a. Ti sporazumi moraju sadržavati uvjete o odgovornosti ***i sve druge odredbe koje stranke sporazuma smatraju potrebnima za pružanje predmetne usluge***.

4. Sporazumi iz stavka 3. ***temelje se*** na predlošcima koje izradi ENISA nakon savjetovanja s državama članicama ***i, prema potrebi, drugim korisnicima kibernetičke sigurnosne pričuve EU-a***.

5. Komisija i ENISA ne snose ugovornu odgovornost za štetu koju trećim stranama prouzroče usluge pružene u okviru primjene kibernetičke sigurnosne pričuve EU-a, ***osim u slučajevima krajnje nepažnje u evaluaciji zahtjeva pružatelja usluga ili u slučajevima kada su Komisija ili ENISA korisnici kibernetičke sigurnosne pričuve EU-a u skladu s člankom 14. stavkom 3***.

6. U roku od mjesec dana od završetka mjere potpore korisnici Komisiji i ENISA-i***, mreži CSIRT-ova i, prema potrebi, mreži EU-CyCLONe*** dostavljaju sažeto izvješće o pruženoj usluzi, ostvarenim rezultatima i stečenim iskustvima. Ako je korisnik iz treće zemlje kako je utvrđeno u članku 17., to se izvješće dijeli s Visokim predstavnikom.
U izvješću se poštuje pravo Unije i nacionalno pravo o zaštiti osjetljivih ili klasificiranih podataka.

7. Komisija o korištenju i rezultatima potpore ***redovito te najmanje dvaput godišnje*** izvješćuje Skupinu za suradnju u području sigurnosti mrežnih i informacijskih sustava. ***Povjerljive informacije štite se u skladu s pravom Unije i nacionalnim pravom o zaštiti osjetljivih ili klasificiranih podataka.***

Članak 15.

Koordinacija s mehanizmima za upravljanje krizama

1. Kad su značajni kibernetički sigurnosni incidenti ili kibernetički sigurnosni incidenti velikih razmjera posljedica ili uzrok katastrofa kako su definirane u Odluci 1313/2013/EU[27], potporom

[27] 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.).

odgovoru na takve incidente na temelju ove Uredbe dopunjuju se djelovanja na temelju Odluke 1313/2013/EU ne dovodeći je u pitanje.

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

3. Uz savjetovanje s Visokim predstavnikom, potpora u okviru mehanizma za izvanredne ***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. Također može biti dopuna ili doprinos pomoći koju jedna država članica pruža drugoj državi članici u kontekstu članka 42. stavka 7. ***UEU-a***.

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

Članak 16.

Pouzdani pružatelji

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

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

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

(c) vodi računa da kibernetička sigurnosna pričuva EU-a donosi dodanu vrijednost EU-a tako što doprinosi ciljevima iz članka 3. Uredbe (EU) 2021/694, među ostalim poticanju razvoja kibernetičkih sigurnosnih vještina u EU-u, ***te postizanju rodne ravnoteže u tom sektoru i jačanju tehnološke suverenosti, otvorene strateške autonomije, konkurentnosti i otpornosti Unije***.

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

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

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

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

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

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

(f) pružatelj mora biti opremljen ***ažuriranom*** hardverskom i softverskom tehničkom opremom koja omogućuje traženu uslugu ***te mora, ako je primjenjivo, biti u skladu s Uredbom (EU).../... Europskog parlamenta i Vijeća[28] (2022/0272(COD))***;

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

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

(i) u državama članicama u kojima može pružati uslugu pružatelj je mora moći pružiti na lokalnom jeziku države članice, ***ili na jednom od radnih jezika institucija Unije***;

(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 usvajanja tog programa***.

(ja) pružatelj mora moći pružati uslugu neovisno, a ne kao dio paketa, čime se štiti mogućnost korisnika da prijeđe na drugog pružatelja usluga;

(jb) za potrebe članka 12. stavka 1. pružatelj u prijedlog za podnošenje ponuda uključuje mogućnost pretvaranja neiskorištenih usluga odgovora na incidente u vježbe ili osposobljavanja;

(jc) pružatelj mora imati poslovni nastan i izvršne upravljačke strukture u Uniji, pridruženoj zemlji ili trećoj zemlji koja je sudionica Sporazuma o javnoj nabavi u kontekstu Svjetske trgovinske organizacije.

(jd) . Pružatelj ne smije podlijegati kontroli nepridružene treće zemlje ili subjekta iz nepridružene treće zemlje koji nije sudionik Sporazuma o javnoj nabavi ili, alternativno, takav subjekt mora podlijegati provjeri u smislu Uredbe (EU) 2019/452 i, prema potrebi, mjerama ublažavanja, uzimajući u obzir ciljeve utvrđene u ovoj Uredbi.

Članak 17.

Potpora trećim zemljama

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

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

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

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

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

5. Prije nego što prime bilo kakvu potporu iz kibernetičke sigurnosne pričuve EU-a, treće zemlje Komisiji i Visokom predstavniku dostavljaju informacije o svojoj kibernetičkoj otpornosti i kapacitetima za upravljanje rizicima, uključujući barem informacije o poduzetim nacionalnim mjerama pripreme za značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera te informacije o odgovornim nacionalnim subjektima, uključujući CSIRT-ove ili ekvivalentne subjekte, njihovim sposobnostima i resursima koji su im dodijeljeni. Odredbe iz članaka 13. i 14. ove Uredbe koje se odnose na države članice primjenjuju se na treće zemlje iz stavka 1.

6. Komisija ***bez nepotrebne odgode obavještava Vijeće te*** surađuje s Visokim predstavnikom u vezi sa zaprimljenim zahtjevima i primjenom potpore koja je trećim zemljama dodijeljena iz kibernetičke sigurnosne pričuve EU-a.

Poglavlje IV.

MEHANIZAM ZA ISTRAŽIVANJE KIBERNETIČKIH SIGURNOSNIH INCIDENATA

Članak 18.

Mehanizam za istraživanje kibernetičkih sigurnosnih incidenata

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

2. ENISA u pripremi izvješća o istraživanju incidenta iz stavka 1. surađuje sa svim relevantnim dionicima, uključujući predstavnike država članica, Komisije, drugih relevantnih institucija, tijela***, ureda*** i agencija EU-a, pružatelja upravljanih sigurnosnih usluga ***u nacionalnim i prekograničnim SOC-ovima*** i korisnika usluga kibernetičke sigurnosti ***te od njih prikuplja povratne informacije***, ***što se nadopunjava jamstvima i praćenjem koji su adekvatni kako bi se osiguralo da stečena iskustva i prepoznate najbolje prakse imaju potporu aktera u industriji usluga kibernetičke sigurnosti***. ENISA prema potrebi surađuje i sa subjektima pogođenima značajnim kibernetičkim sigurnosnim incidentom ili kibernetičkim sigurnosnim incidentom velikih razmjera. Kao pomoć u istraživanju, ENISA se može savjetovati i s drugim vrstama dionika. Konzultirani predstavnici dužni su dati informacije o svakom mogućem sukobu interesa.

3. Izvješće obuhvaća istraživanje i analizu konkretnog značajnog kibernetičkog sigurnosnog incidenta ili kibernetičkog sigurnosnog incidenta velikih razmjera, uključujući glavne uzroke, ranjivosti i stečena iskustva. Povjerljive informacije u izvješću štite se u skladu s pravom Unije ili nacionalnim pravom o zaštiti osjetljivih ili klasificiranih podataka. ***U njemu se ne navode pojedinosti o aktivno iskorištenim ranjivostima koje su i dalje prisutne.***

3.a U izvješću iz stavka 1. ovog članka navode se iskustva stečena istorazinskim ocjenjivanjima provedenima u skladu s člankom 19. Direktive (EU) 2022/2555.

4. U izvješću se, prema potrebi, daju preporuke***, uključujući za sve relevantne dionike,*** za poboljšanje kibernetičkog sigurnosnog položaja Unije.

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

Poglavlje V.

ZAVRŠNE ODREDBE

Članak 19.

Izmjene Uredbe (EU) 2021/694

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

(1) članak 6. mijenja se kako slijedi:

(a) stavak 1. mijenja se kako slijedi:

i. umeće se sljedeća točka (aa):

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

ii. dodaje se sljedeća točka (g):

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

(***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 kibernetičke sigurnosti te mreže

nacionalnih koordinacijskih centara u skladu s Uredbom (EU) 2021/887 Europskog parlamenta i Vijeća*, uz iznimku djelovanja radi primjene kibernetičke sigurnosne pričuve EU-a, koja provode Komisija i 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 nacionalnih koordinacijskih centara (SL L 202, 8.6.2021., str. 1. ***ELI: http://data.europa.eu/eli/reg/2021/887/oj).”;***

(2) Članak 9. mijenja se kako slijedi:

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

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

(c) ***1 620 566 000*** EUR za specifični cilj 3 – kibernetička sigurnost i povjerenje;

(d) ***500 347 000*** EUR za specifični cilj 4 – napredne digitalne vještine”;

(aa) umeće se sljedeći novi stavak 2.a:

„ (2.a). Iznos iz stavka 2. točke (c) prvenstveno se upotrebljava za postizanje operativnih ciljeva iz članka 6. stavka 1. točaka od (a) do (f) Programa.”;

(ab) umeće se sljedeći novi stavak 2.b:

„ (2.b). Iznos za uspostavu i provedbu kibernetičke sigurnosne pričuve EU-a ne prelazi 27 milijuna EUR za predviđeno trajanje Uredbe o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibernetičkih sigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih.”;

(b) dodaje se sljedeći stavak 8.:

‘8. Odstupajući od članka 12. stavka 4. Uredbe (EU, Euratom) 2018/1046, neiskorištena odobrena sredstva za preuzimanje obveza i za plaćanje za djelovanja ***u kontekstu provedbe kibernetičke sigurnosne pričuve EU-a***, 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.”;

Komisija obavješćuje Parlament i Vijeće o odobrenim sredstvima prenesenima u skladu s člankom 12. stavkom 6. Uredbe (EU, Euratom) 2018/1046.

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

„2. Programom se može predvidjeti financiranje u bilo kojem od oblika utvrđenih u Uredbi ***(EU, Euratom) 2018/1046***, uključujući posebno putem nabave kao primarnog oblika ili bespovratnih sredstava i nagrada.

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

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

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

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

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

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

(4) dodaje se sljedeći članak 16.a:

„***Članak 16.a***

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

(5) članak 19. zamjenjuje se sljedećim:

„Bespovratna sredstva u okviru Programa dodjeljuju se te se njima upravlja u skladu s glavom VIII. ***Uredbe (EU, Euratom) 2018/1046*** i mogu pokrivati do 100 % prihvatljivih troškova, ne dovodeći u pitanje načelo sufinanciranja kako je utvrđeno u članku 190.

Uredbe (EU, Euratom) 2018/1046. 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) ***Uredbe (EU, Euratom) 2018/1046*** Europski stručni centar u području kibernetičke sigurnosti može nacionalnim centrima za sigurnosne operacije iz članka 4. 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) ***Uredbe (EU, Euratom) 2018/1046*** Europski stručni centar u području kibernetičke sigurnosti može državama članicama izravno, bez poziva na podnošenje prijedloga, dodijeliti potporu u obliku bespovratnih sredstava za mehanizam za izvanredne ***kibernetičke sigurnosne*** situacije, kako je utvrđeno u članku 10. Uredbe ***(EU) .../...***.

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

Kad je riječ o potpori uzajamnoj pomoći pri odgovoru na značajne kibernetičke sigurnosne incidente ili kibernetičke sigurnosne incidente velikih razmjera, kako je definirano u članku 10. točki (c) Uredbe ***(EU) .../...*** i u skladu s člankom 193. stavkom 2. drugim podstavkom točkom (a) ***Uredbe (EU, Euratom) 2018/1046***, u propisno opravdanim slučajevima troškovi se mogu smatrati prihvatljivima čak i ako su nastali prije podnošenja zahtjeva za bespovratna sredstva.”;

(6) Prilozi I. i II. Uredbi (EU) 2021/694 mijenjaju se u skladu s Prilogom ovoj Uredbi.

Članak 19.a
Dodatna sredstva za ENISA-u

ENISA prima dodatna sredstva za obavljanje svojih dodatnih zadaća koje su joj dodijeljene ovom Uredbom. Tom dodatnom potporom, uključujući financiranje, ne ugrožava se postizanje ciljeva drugih programa Unije, osobito programa Digitalna Europa.

Članak 20.

Evaluacija *i preispitivanje*

1. Komisija do [***dvije*** godine od datuma početka primjene ove Uredbe] ***i svake dvije godine nakon toga provodi evaluaciju funkcioniranja mjera utvrđenih u ovoj Uredbi i podnosi izvješće*** Europskom parlamentu i Vijeću.

2. Evaluacijom se posebno ocjenjuje:

(a) upotreba prekograničnih SOC-ova i njihova dodana vrijednost te mjera u kojoj oni doprinose bržem otkrivanju i savladavanju kibernetičkih prijetnji te informiranosti o stanju; aktivno sudjelovanje nacionalnih SOC-ova u europskom kibernetičkom štitu, uključujući broj uspostavljenih nacionalnih i prekograničnih SOC-ova te mjeru u kojoj je to pridonijelo proizvodnji i razmjeni visokokvalitetnih upotrebljivih informacija i obavještajnih podataka o kibernetičkim prijetnjama; količina i troškovi infrastrukture i/ili alata za kibernetičku sigurnost, nabavljenih zajedničkom javnom nabavom; broj sporazuma o suradnji sklopljenih između prekograničnih SOC-ova i s ISAC-ima iz sektora; broj incidenata prijavljenih mreži CSIRT-ova i njegov utjecaj na rad mreže CSIRT-ova;

(b) pozitivan i negativan rad mehanizma za izvanredne kibernetičke sigurnosne situacije, uključujući pitanje jesu li potrebni dodatni zahtjevi za suradnju ili osposobljavanje;

(c) doprinos ove Uredbe jačanju otpornosti i otvorene strateške autonomije Unije, poboljšanju konkurentnosti relevantnih industrijskih sektora, mikropoduzeća i MSP-ova, uključujući start-up poduzeća, i razvoju vještina u području kibernetičke sigurnosti u Uniji;

(d) upotreba i dodana vrijednost kibernetičke sigurnosne pričuve EU-a, uključujući broj pouzdanih pružatelja sigurnosnih usluga koji su dio kibernetičke sigurnosne pričuve EU-a; broj, vrsta, troškovi i učinak provedenih mjera kojima se podupire odgovor na kibernetičke incidente, kao i odgovarajuće korisnike i pružatelje; prosječno vrijeme u kojem Komisija prepoznaje incident, u kojem se kibernetička sigurnosna pričuva EU-a primjenjuje i daje odgovor na incident te u kojem se korisnik oporavlja od incidenta; pitanje treba li područje primjene pričuve proširiti na usluge pripravnosti na incidente ili zajedničke vježbe s pouzdanim pružateljima upravljanih sigurnosnih usluga i potencijalnim korisnicima kibernetičke sigurnosne pričuve EU-a kako bi se prema potrebi osiguralo učinkovito funkcioniranje te pričuve;

(e) doprinos ove Uredbe razvoju i poboljšanju vještina i kompetencija radne snage u sektoru kibernetičke sigurnosti, potrebnih za jačanje kapaciteta Unije za otkrivanje i sprečavanje kibernetičkih sigurnosnih prijetnji i incidenata te odgovor na njih i oporavak od njih;

(f) doprinos ove Uredbe uvođenju i razvoju najsuvremenijih tehnologija u Uniji.

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

Članak 20.a

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 6. stavka 3., članka 7. stavka 2., članka 12. stavka 8. i članka 13. stavka 7. dodjeljuje se Komisiji na razdoblje od … godina počevši od … [datum stupanja na snagu temeljnog zakonodavnog akta ili bilo koji drugi datum koji odrede suzakonodavci]. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od ... 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.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 6. stavka 3., članka 7. stavka 2., članka 12. stavka 8. i članka 13. 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 6. stavka 3., članka 7. stavka 2., članka 12. stavka 8. ili članka 13. 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 21.

Postupak odbora

1. Komisiji pomaže Odbor za koordinaciju programa Digitalna Europa osnovan Uredbom (EU) 2021/694. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.
2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

Članak 22.

Stupanje na snagu

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

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

Sastavljeno u Strasbourgu,

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

PRILOG

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

(1) u Prilogu I. odjeljak/poglavlje „Specifični cilj 3 – kibernetička sigurnost i povjerenje” zamjenjuje se sljedećim:

„Specifični cilj 3 – kibernetička sigurnost 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 kibernetičke sigurnosti te poboljšanjem sposobnosti privatnog i javnog sektora da štite građane i poduzeća od kibernetičkih prijetnji, 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 kibernetičke sigurnosti koji su temeljni za zaštitu ključnih infrastruktura i jedinstvenog digitalnog tržišta u cjelini. Takvo zajedničko ulaganje moglo bi uključivati ulaganja u kvantnoračunalne kapacitete i podatkovne resurse za kibernetičku sigurnost, informiranost o stanju u kibernetičkom prostoru, ***uključujući nacionalne centre za sigurnosne operacije i prekogranične centre za sigurnosne operacije koji čine europski***

kibernetički štit, 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 kibernetička sigurnost i povjerenje unutar jedinstvenog digitalnog tržišta;

3. osiguravanje širokog uvođenja djelotvornih najsuvremenijih rješenja za kibernetičku sigurnost 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 kibernetičke sigurnosti, ***s posebnim naglaskom na postizanje rodne ravnoteže u sektoru,*** primjerice usklađivanjem programa stjecanja tih vještina, njihovim prilagođavanjem specifičnim sektorskim potrebama***, uključujući interdisciplinarni i opći fokus,*** i olakšavanjem pristupa ciljanom specijaliziranom osposobljavanju ***kako bi se podržalo sve osobe i teritorije, ne dovodeći u pitanje mogućnost izvlačenja koristi koje pruža ova Uredba***;

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 – kibernetička sigurnost i povjerenje” zamjenjuje se sljedećim:

„Specifični cilj 3 – kibernetička sigurnost i povjerenje

3.1. Količina infrastruktura ili alata za kibernetičku sigurnost nabavljenih zajedničkom javnom nabavom ***ili kao dio kibernetičkog sigurnosnog štita***;

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

3.3. Broj, ***vrsta, troškovi i učinak*** mjera ***provedenih*** za potporu pripravnosti i odgovoru na kibernetičke sigurnosne incidente u okviru mehanizma za izvanredne ***kibernetičke sigurnosne*** situacije. ***Mjera u kojoj je korisnik primijenio i proveo preporuke iz testova pripravnosti, kao i prosječno vrijeme u kojem Komisija prepoznaje incident, u kojem se kibernetička sigurnosna pričuva EU-a primjenjuje i daje odgovor na incident te u kojem se korisnik oporavlja od incidenta.”***

OBRAZLOŽENJE

KONTEKST

Kibernetička sigurnost jest i trebala bi biti u središtu naših demokracija. Prijetnje kibernetičke sigurnosti povezane su sa širenjem nesigurnosti među stanovništvom i poduzećima, kao i s porastom dezinformacija, što predstavlja izazov demokratskim načelima kojima se štiti poštovanje ljudskih prava. Kako bi se to spriječilo, sigurno digitalno okruženje koje podliježe javnom nadzoru ključno je za naše demokracije.

Kibernetički napadi u EU-u izvode se s pomoću sve većeg broja metoda i imaju sve veći učinak. Osim toga, ruski napad na Ukrajinu doveo je čak i prije invazije do korjenitih promjena te je s njim, prema izvješću ENISA-e o prijetnjama za 2022.[1], započelo novo doba za **kibernetičko ratovanje**. Prioriteti proizašli iz ovog sukoba u kibernetičkom prostoru su **potreba za izgradnjom kapaciteta u multilateralnim programima** i projektima te potreba za brzim **razvojem vještina**. Kako bismo bili otporniji, hitno je potreban zajednički europski odgovor koji se temelji na snažnijoj suradnji na europskoj razini povrh one nacionalne.

Za uspješnu provedbu ove Uredbe bit će ključno povećanje kulture kibernetičke sigurnosti koja obuhvaća sigurnost, uključujući sigurnost digitalnog okruženja, kao javnog dobra.

Nadalje, kibernetički napadi su često usmjereni na **lokalne, regionalne ili nacionalne javne službe** i infrastrukture (npr. zdravstveni sektor koji je i dalje glavna meta kibernetičkih napada[2]). Dokazi upućuju i na to da su **lokalna tijela** jedna od najranjivijih meta zbog nedostatka financijskih i ljudskih resursa te je posebno važno da čelnici i čelnice na lokalnoj razini budu svjesni toga kako bi se povećala digitalna otpornost[3]. Napadi prvenstveno i izravno utječu na građane i time ugrožavaju naše demokracije, među ostalim kampanjama dezinformiranja. Osjećaj nesigurnosti koji te situacije mogu stvoriti kod stanovništva može dovesti do političkih preferencija koje slijede radikalnu predanost sigurnosti na štetu poštovanja temeljnih prava. Međutim, vrijedi suprotno: sigurnost je ključan dio naših demokracija koji je kompatibilan sa svim drugim pravima i nužan za njih.

Osim toga, **poduzeća i MSP-ovi** u EU-u suočavaju se i s kibernetičkim kriminalitetom, a zbog sve veće upotrebe digitalne sfere za poslovanje vlada i veća zabrinutost u pogledu kibernetičke sigurnosti. MSP-ovi su manje pripremljeni od poduzeća, imaju manje resursa da se zaštite i manje su svjesni toga da mogu biti izloženi takvim napadima.

Očekuje se da će se ti napadi u budućnosti nastaviti i povećati. Posebno u situacijama političke nestabilnosti, a pogotovo u kontekstu rata. S obzirom na to da digitalna tranzicija

[1] ENISA Threat Landscape 2022 (Pregled prijetnji ENISA-e za 2022.), listopad 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[2] ENISA Threat Landscape: Health Sector, (Pregled prijetnji ENISA-e: zdravstveni sektor), srpanj 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

[3] Europski odbor regija, Digitalna otpornost, 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf

svakodnevno napreduje, digitalna otpornost postaje sve važnija za naš svakodnevni život i za **otvorenu stratešku autonomiju EU-a**.

PRIJEDLOG IZVJESTITELJICE

Izvjestiteljica smatra da EU treba biti bolje pripremljen za budućnost i pozdravlja ovaj hitan zakonodavni akt kojim se objedinjuju resursi, informacije i znanje kako bi se osigurala solidarnost među državama članicama, povećali industrijski kapaciteti u EU-u, razvile **na koordiniran način vještine i sposobnosti** kojima se osigurava kibernetička sigurnost, povećala otpornost na buduće napade i naše demokracije zaštitilo od sebične instrumentalizacije sigurnosnih potreba. Osim toga, važno je zaštititi integritet naših izbornih postupaka. Ovaj zakonodavni akt ključna je obveza za postizanje cilja **otvorene strateške autonomije**.

Zbog toga su potrebni snažno i **koordinirano upravljanje** u EU-u i strukturirana suradnja s privatnim sektorom kako bi se potaknuo razvoj europske kibernetičke industrije. Osim toga, potrebna je i suradnja s međunarodnim partnerima istomišljenicima, ali i s drugim zemljama koje nemaju iste kapacitete i možda će im biti potrebna pomoć ako budu žrtve kibernetičkih napada. Aktom EU-a o kibernetičkoj solidarnosti mora se dobro definirati njegovo upravljanje i ne smije se doći do preklapanja s već postojećim inicijativama i zakonodavstvom, kao što je Direktiva NIS 2.

Prijedlog se u velikoj mjeri temelji na dobrovoljnoj razmjeni informacija među državama članicama. Zbog toga izvjestiteljica predlaže jačanje jamstava radi izgradnje povjerenja među državama članicama kako bi se povećalo njihovo sudjelovanje i suradnja, primjerice u pogledu zajedničke nabave infrastrukture i uključivanja zakonodavnih vlasti, kako bi se osigurali povjerenje građana i **demokratska jamstva**.

Drugo, izvjestiteljica predlaže da se za tu inicijativu **osiguraju proračunska sredstva** iz predstojećih VFO-a u kombinaciji sa sredstvima država članica kako bi se zajamčio kontinuitet aktivnosti razvijenih u okviru Akta EU-a o kibernetičkoj solidarnosti nakon 2027.

Treće, izvjestiteljica predlaže poboljšanje **upravljačke strukture**, jasnu definiciju upravljanja i njezino povezivanje s postojećim zakonodavstvom.

Izvjestiteljica također predlaže bolju **koordinaciju** među različitim subjektima država članica zaduženima za kibernetičku sigurnost kako bi se osigurao zajednički kibernetički štit. Nadalje, potrebno je povećati doprinos ENISA-e koordinaciji i interakciji među različitim akterima nacionalnih zajednica.

Izvjestiteljica smatra da **nova kibernetička sigurnosna pričuva** ima potencijal razviti industrijske kapacitete u EU-u, među ostalim za MSP-ove, ulaganjem u istraživanje i inovacije radi razvoja najsuvremenijih tehnologija, kao što su tehnologije računalstva u oblaku i umjetna inteligencija. Osim toga, izvjestiteljica predlaže da se zadrži sudjelovanje industrije, poboljšaju kriteriji i povjerenje u njezino sudjelovanje (tj. poveže njezino sudjelovanje s nacionalnim ili lokalnim poduzećem) pojašnjavanjem **kriterija** i definicije **tehnološke suverenosti** te da se zajamči ravnoteža između aktera izvan EU-a i aktera EU-a. Osim toga, izvjestiteljica za **mehanizam za izvanredne kibernetičke sigurnosne situacije** predlaže **program**

certificiranja koji bi se upotrebljavao za privatne pružatelje usluga za izgradnju dugogodišnjeg i pouzdanog partnerstva.

Kad je riječ o **mehanizmu za istraživanje incidenata**, izvjestiteljica predlaže jačanje uloge ENISA-e i privatnog sektora u SOC-ovima, uz odgovarajuća jamstva i praćenje, kako bi se potvrdilo podupiru li akteri u industriji stečena iskustva. Nadalje, izvjestiteljica predlaže da se uključe iskustva stečena u okviru istorazinskih ocjenjivanja, kako je navedeno u Direktivi NIS 2, i da se poveća financiranje ENISA-e s ciljem osiguravanja učinkovite primjene zakonodavstva i odgovarajuće zaštite za suočavanje s kibernetičkim sigurnosnim prijetnjama.

Osim toga, ovaj prijedlog po svojoj prirodi ima vrlo relevantnu **vanjsku dimenziju** jer treće zemlje mogu pristupiti resursima i potpori iz Akta EU-a o kibernetičkoj solidarnosti koristeći se potporom za odgovor na incidente iz kibernetičke sigurnosne pričuve EU-a budući da su akteri iz privatnog sektora koji nisu iz EU-a potrebni za kibernetičku pričuvu. Vanjska dimenzija trebala bi podlijegati i javnom nadzoru, uz sudjelovanje zakonodavnih vlasti, kako bi se građanima zajamčilo sudjelovanje u postupku. Kibernetička sigurnost bi se trebala smatrati javnim dobrom.

Nadalje, središnji je stup ovog prijedloga razvoj vještina i kompetencija, pri čemu se ne bi trebalo samo ulagati u razvoj znanja, već i u mogućnost pristupa svih građana osposobljavanju u cilju stjecanja tih vještina. Izvjestiteljica predlaže jačanje veze s **Akademijom EU-a za vještine u području kibernetičke sigurnosti**, čime se želi povećati broj stručnjaka za kibernetičku sigurnost povezivanjem privatnih i javnih inicijativa te pružanjem osposobljavanja i certifikacije za građane. Ta snažnija veza zahtijevat će zaštitne mjere kako bi se izbjegao odljev mozgova i kako se ne bi ugrozila mobilnost radne snage.

Nadalje, izvjestiteljica predlaže ulaganja i uključivanje aktivnih mjera za razvoj vještina u tom sektoru, s obzirom na to da je 2023. Europska godina vještina, kao i povećanje osviještenosti građana. Mjere će biti osmišljene tako da ulaganja ne stvaraju neravnoteže među državama članicama jer trenutačna visoka potražnja i visoke plaće u tom sektoru mogu dovesti do određene vrste odljeva mozgova u smjeru najbolje plaćenih opcija.

S obzirom na navedeno, izvjestiteljica predlaže jačanje specijaliziranih, interdisciplinarnih i općih vještina i kompetencija diljem EU-a, s posebnim naglaskom na žene, s obzirom na to da u području kibernetičke sigurnosti i dalje postoji rodni jaz, a žene čine 20 % prosječne prisutnosti u svijetu[4]. Žene moraju biti prisutne i dio osmišljavanja digitalne budućnosti i njezina upravljanja.

Osim toga, izvjestiteljica predlaže jačanje trokuta između nacionalnih centara stručnosti, Europskog stručnog centra za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti (ECCC) i ENISA-e kako bi se razvile vještine i kompetencije. Nadalje, potrebno je povećanje uloge **industrije** u **razvoju vještina** i stvaranje partnerstava s **akademskom zajednicom** i akterima civilnog društva, uzimajući u obzir regionalno iskustvo, znanje i specijalizaciju te saveze trećih zemalja s partnerima istomišljenicima kako bi se povećale

[4] Rezolucija Europskog parlamenta od 10. lipnja 2021. o promicanju rodne ravnopravnosti u obrazovanju i karijerama u područjima znanosti, tehnologije, inženjerstva i matematike (STEM) (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_HR.html

razmjene i osigurao globalni pristup potpori za građane, poduzeća i institucije.

Izvjestiteljica također predlaže suradnju u privlačenju talenata i mjerenju štete koju kibernetički napadi nanose ljudima (npr. učinak napada ucjenjivačkim softverom na zdravstveni sektor).

Izvjestiteljica predlaže mjere za uključivanje građana i povećanje njihove svijesti bez uzbunjivanja kao još jednu mjeru za jamčenje zaštite naših demokracija i temeljnih vrijednosti. Ključno je povećanje **kulture kibernetičke sigurnosti** koja obuhvaća sigurnost, uključujući sigurnost digitalnog okruženja kao javnog dobra. Na taj ćemo način moći zajamčiti model digitalne demokracije, za razliku od digitalnog autoritarizma, s transparentnošću, demokracijom i sigurnošću koje može donijeti razvoj ex ante zakonodavstva.

Nadalje, izvjestiteljica vjeruje da će se jačanjem **istraživanja i inovacija** u području kibernetičke sigurnosti povećati otpornost i otvorena strateška autonomija EU-a. Isto tako, postići će se osiguravanje sinergija s programima istraživanja i inovacija te s postojećim instrumentima i institucijama te jačanje trokuta znanja kako bi se premostio nedostatak vještina diljem EU-a.

Nadalje, ovim će se zakonodavstvom povećati otpornost EU-a i njegovih država članica, ne samo izravno putem zakona o kibernetičkoj sigurnosti i kibernetičkoj otpornosti, već i učinkom koji ono može imati na eksponencijalni razvoj umjetne inteligencije i učinkom koji regulacija podataka i privatnosti podataka može imati na kibernetičku sigurnost.

Osim toga, ovo će zakonodavstvo pomoći u ispunjavanju obveza iz **Europske deklaracije o digitalnim pravima i načelima za digitalno desetljeće** koja je povezana sa zaštitom interesa ljudi, poduzeća i javnih institucija od kibernetičkih sigurnosnih rizika i kibernetičkog kriminaliteta, uključujući povrede podataka i krađu identiteta ili manipulaciju njime.

S obzirom na to, izvjestiteljica smatra da bi ovaj prijedlog trebao biti operativan što je brže moguće, uključujući europski kibernetički sigurnosni štit i mehanizam za izvanredne kibernetičke sigurnosne situacije, kako bi se uspostavio opći okvir i izbjegli izolirani sustavi (silosi) s obzirom na to da kibernetički prostor nema granica.

PRILOG: POPIS SUBJEKATA ILI OSOBA OD KOJIH JE IZVJESTITELJICA PRIMILA INFORMACIJE

U skladu s člankom 8. Priloga I. Poslovniku izvjestiteljica izjavljuje da je tijekom pripreme izvješća, prije njegova usvajanja u odboru, primila informacije od sljedećih subjekata ili osoba:

Subjekt i/ili osoba
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

Navedeni popis sastavljen je pod isključivom odgovornošću izvjestiteljice.

27.10.2023

MIŠLJENJE ODBORA ZA VANJSKE POSLOVE

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Izvjestitelj za mišljenje: Dragoş Tudorache

Amandman 1

Prijedlog uredbe
Uvodna izjava 1.

Tekst koji je predložila Komisija	*Izmjena*
(1) Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora ***gospodarstva*** jer su javne uprave, poduzeća i građani međusobno povezani i ovisni jedni o drugima u svim sektorima i prekogranično više nego ikada prije.	(1) Uporaba informacijskih i komunikacijskih tehnologija te ovisnost o njima postali su temeljno obilježje svih sektora ***gospodarske i vojne aktivnosti*** jer su javne uprave, poduzeća i građani***, kao i subjekti iz vojnog i obrambenog sektora,*** međusobno povezani i ovisni jedni o drugima u svim sektorima i prekogranično više nego ikada prije.

Amandman 2

Prijedlog uredbe
Uvodna izjava 2.

Tekst koji je predložila Komisija	*Izmjena*
(2) Povećavaju se razmjeri i učestalost te pogoršavaju posljedice kiberincidenata, uključujući napade na lance opskrbe s ciljem kiberšpijunaže, napad ucjenjivačkim softverom ili izazivanje poremećaja. Oni predstavljaju veliku prijetnju	(2) Povećavaju se razmjeri i učestalost te pogoršavaju posljedice kiberincidenata, uključujući napade na lance opskrbe s ciljem kiberšpijunaže, napad ucjenjivačkim softverom ili izazivanje poremećaja. Oni predstavljaju veliku prijetnju

funkcioniranju mrežnih i informacijskih sustava. S obzirom na to da se prijetnje brzo mijenjaju, mogući incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu na kritičnoj infrastrukturi zahtijevaju povećanu pripravnost na svim razinama okvira Unije za kibersigurnost. ***Ta prijetnja nadilazi*** rusku vojnu agresiju na Ukrajinu i vjerojatno će se nastaviti s obzirom na mnoštvo državi bliskih, kriminalnih i haktivističkih aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga i obavljanje gospodarskih djelatnosti, među ostalim u kritičnim ili visokokritičnim sektorima, uzrokovati znatne financijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu Unije te čak imati zdravstvene ili po život opasne posljedice. K tomu, kibersigurnosni incidenti su nepredvidivi jer se često pojavljuju i razvijaju u vrlo kratkim vremenskim razdobljima, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u mnogim zemljama ili se brzo šire na mnoge zemlje.	funkcioniranju mrežnih i informacijskih sustava. S obzirom na to da se prijetnje brzo mijenjaju, mogući incidenti velikih razmjera koji uzrokuju znatne poremećaje ili štetu na kritičnoj infrastrukturi zahtijevaju povećanu pripravnost na svim razinama okvira Unije za kibersigurnost. ***Ozbiljnost tih prijetnji postala je još relevantnija zbog ponovne pojave rata na našem kontinentu. Te prijetnje nadilaze*** rusku vojnu agresiju na Ukrajinu i vjerojatno će se nastaviti s obzirom na mnoštvo državi bliskih, kriminalnih i haktivističkih aktera umiješanih u trenutačne geopolitičke napetosti. Takvi incidenti mogu ometati pružanje javnih usluga i obavljanje gospodarskih djelatnosti, među ostalim u kritičnim ili visokokritičnim sektorima, uzrokovati znatne financijske gubitke, narušiti povjerenje korisnika, nanijeti veliku štetu gospodarstvu ***i sigurnosti*** Unije te čak imati zdravstvene ili po život opasne posljedice***, uz moguće ugrožavanje lokalnih ili nacionalnih objekata povezanih sa sigurnošću***. K tomu, kibersigurnosni incidenti su nepredvidivi jer se često pojavljuju i razvijaju u vrlo kratkim vremenskim razdobljima, nisu ograničeni na određeno zemljopisno područje i događaju se istodobno u mnogim zemljama ili se brzo šire na mnoge zemlje. ***Kibersigurnost je važna za zaštitu naših europskih vrijednosti i osiguravanje funkcioniranja naših demokracija zaštitom naše izborne infrastrukture i demokratskih postupaka od svakog vanjskog upletanja.***

Amandman 3

Prijedlog uredbe
Uvodna izjava 2.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(2.a) Kibersigurnost je ključna za očuvanje sigurnosti naše Unije i

	sprječavanje zlonamjernih aktera, državnih i nedržavnih, u narušavanju naše demokracije, gospodarstva i sigurnosti. Potrebno je spriječiti fragmentirano okruženje jer takva situacija ne bi predstavljala odgovarajući pristup, posebno kad je riječ o budućim kibernapadima velikih razmjera koji su istodobno usmjereni na nekoliko država članica ili transnacionalnu ključnu infrastrukturu. Stoga je potrebno tijelo Unije koje bi djelovalo kao koordinacijska platforma za sve postojeće i buduće instrumente, fondove i mehanizme za kibersigurnost.

Amandman 4

Prijedlog uredbe
Uvodna izjava 3.

Tekst koji je predložila Komisija	*Izmjena*
(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe[16], potrebno je povećati otpornost građana, poduzeća i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoć u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o	(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe[16], potrebno je povećati otpornost građana, poduzeća i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoć u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o

kibersigurnosnim prijetnjama i incidentima.

kibersigurnosnim prijetnjama i incidentima***, kao i sposobnost da djeluje proaktivno i da na kibersigurnosne prijetnje i incidente odgovori odlučno***.

---

[16] https://futureu.europa.eu/hr/

---

[16] https://futureu.europa.eu/hr/

Amandman 5

Prijedlog uredbe
Uvodna izjava 4.

Tekst koji je predložila Komisija

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća[17], Preporuku Komisije (EU) 2017/1584[18], Direktivu 2013/40/EU Europskog parlamenta i Vijeća[19] i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[20]. Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

Izmjena

(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća[17], Preporuku Komisije (EU) 2017/1584[18], Direktivu 2013/40/EU Europskog parlamenta i Vijeća[19] i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[20]. Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, ***proaktivno,*** solidarno i koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu. ***Nadalje, Unija je u ožujku 2022. odobrila i pokrenula Strateški kompas za sigurnost i obranu, koji je, među ostalim, usmjeren na jačanje kibersigurnosti i poboljšanje međunarodne suradnje sa saveznicima istomišljenicima i demokratskim partnerima, posebno u tom području. Štoviše, kibersigurnost je središnja točka nedavne Treće zajedničke izjave o suradnji EU-a i NATO-a iz siječnja 2023. Konkretnije, u završnom izvješću o***

procjeni radne skupine EU-a i NATO-a preporučuje se da se u potpunosti iskoristi sinergija između EU-a i NATO-a[1], među ostalim razmjenom najboljih primjera iz prakse između civilnih i vojnih aktera u pogledu provedbe relevantnih politika i zakonodavnih akata povezanih s kibersigurnošću.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[17] 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.).

[18] 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.).

[19] 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.).

[20] 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.).

---

[17] 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.).

[18] 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.).

[19] 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.).

[20] 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.).

Amandman 6

Prijedlog uredbe
Uvodna izjava 6.

Tekst koji je predložila Komisija	*Izmjena*
(6) U Zajedničkoj komunikaciji o politici EU-a o kiberobrani[22] donesenoj 10. studenoga 2022. najavljena je inicijativa EU-a za kibersolidarnost sa sljedećim ciljevima: jačanje zajedničkih kapaciteta EU-a za otkrivanje, informiranost o stanju i odgovor poticanjem uvođenja infrastrukture EU-a za centre za sigurnosne operacije (SOC-ove), podupiranje postupne izgradnje kibersigurnosne pričuve na razini EU-a s uslugama pouzdanih privatnih pružatelja usluga i testiranje kritičnih subjekata na moguće ranjivosti na temelju procjena rizika EU-a.	(6) U Zajedničkoj komunikaciji o politici EU-a o kiberobrani[22] donesenoj 10. studenoga 2022. najavljena je inicijativa EU-a za kibersolidarnost sa sljedećim ciljevima: jačanje zajedničkih kapaciteta EU-a za otkrivanje, informiranost o stanju i odgovor poticanjem uvođenja infrastrukture EU-a za centre za sigurnosne operacije (SOC-ove), podupiranje postupne izgradnje kibersigurnosne pričuve na razini EU-a s uslugama pouzdanih privatnih pružatelja usluga i testiranje kritičnih subjekata na moguće ranjivosti na temelju procjena rizika EU-a. ***Osim toga, kiberprijetnje koje se brzo mijenjaju i brzi tehnološki razvoj također ukazuju na potrebu za poboljšanom civilno-vojnom koordinacijom i suradnjom, kao što je Vijeće naglasilo u svojim Zaključcima o politici kiberobrane EU-a[1].*** ***[1] Zaključci Vijeća o politici kiberobrane EU-a koje je Vijeće odobrilo na sastanku 22. svibnja 2023. (9618/23).***
[22] Zajednička komunikacija Europskom parlamentu i Vijeću „Politika EU-a o kiberobrani”, JOIN/2022/49 final.	[22] Zajednička komunikacija Europskom parlamentu i Vijeću „Politika EU-a o kiberobrani”, JOIN/2022/49 final.

Amandman 7

Prijedlog uredbe
Uvodna izjava 6.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(6.a) S obzirom na nejasne granice između područja civilnih i vojnih pitanja i dvojne namjene kiberalata i tehnologija, potreban je sveobuhvatan i cjelovit pristup digitalnom području. U slučaju kiberincidenata i kiberkriza velikih razmjera koji uključuju više od jedne

	države članice, potrebno je uspostaviti odgovarajuće strukture za upravljanje krizama. U okviru takvih struktura trebala bi se organizirati razmjena informacija, koordinacija i suradnja sa strukturama Unije za upravljanje vojnim krizama i krizama povezanima s vanjskom sigurnosti, kao i s tijelima država članica nadležnima za sigurnost i obranu (zajednica za kiberobranu). To bi se trebalo odnositi i na operacije i misije zajedničke sigurnosne i obrambene politike koje Unija provodi kako bi osigurala mir i stabilnost u svojem susjedstvu i šire.

Amandman 8

Prijedlog uredbe
Uvodna izjava 7.

Tekst koji je predložila Komisija	*Izmjena*
(7) Potrebno je poboljšati otkrivanje kiberprijetnji i kiberincidenata u cijeloj Uniji i informiranost o njihovu stanju te ojačati solidarnost unapređenjem pripravnosti država članica i Unije te njihove sposobnosti za odgovor na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera. Stoga je potrebno uvesti paneuropsku infrastrukturu SOC-ova (europski kiberštit) kako bi se izgradili i poboljšale zajedničke sposobnosti za otkrivanje i informiranost o stanju; trebalo bi uspostaviti mehanizam za izvanredne kibersigurnosne situacije kako bi se državama članicama pomoglo u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih; trebalo bi uspostaviti i mehanizam za istraživanje kibersigurnosnih incidenata kako bi se istražili i procijenili određeni značajni incidenti ili incidenti velikih razmjera. Tim se mjerama ne dovode u pitanje članci 107. i 108. Ugovora o funkcioniranju Europske	(7) Potrebno je poboljšati otkrivanje kiberprijetnji i kiberincidenata u cijeloj Uniji i informiranost o njihovu stanju te ojačati solidarnost unapređenjem pripravnosti država članica i Unije te njihove sposobnosti za odgovor na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera. Stoga je potrebno uvesti paneuropsku infrastrukturu SOC-ova (europski kiberštit) kako bi se izgradili i poboljšale zajedničke sposobnosti za otkrivanje i informiranost o stanju; trebalo bi uspostaviti mehanizam za izvanredne kibersigurnosne situacije kako bi se državama članicama pomoglo u pripremi za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, odgovoru na njih i hitnom oporavku od njih***, uključujući incidente koji obuhvaćaju više od jedne države članice; Kada je to izvedivo i potrebno, u okviru mehanizma za izvanredne kibersigurnosne situacije trebalo bi organizirati razmjenu informacija i suradnju s obrambenim tijelima država***

unije (UFEU).	***članica, uz potporu institucija, tijela i agencija EU-a (zajednica EU-a za kiberobranu)***; trebalo bi uspostaviti i mehanizam za istraživanje kibersigurnosnih incidenata kako bi se istražili i procijenili određeni značajni incidenti ili incidenti velikih razmjera***.*** ***Takve nove strukture također bi trebale podupirati operacije i misije ZSOP-a EU-a***. Tim se mjerama ne dovode u pitanje članci 107. i 108. Ugovora o funkcioniranju Europske unije (UFEU).

Amandman 9

Prijedlog uredbe
Uvodna izjava 11.

Tekst koji je predložila Komisija	*Izmjena*
(11) U svrhu dobrog financijskog upravljanja trebalo bi utvrditi posebna pravila za prijenos neiskorištenih odobrenih sredstava za preuzete obveze i odobrenih sredstava za plaćanje. Uz poštovanje načela da se proračun Unije utvrđuje na godišnjoj razini, ovom bi se Uredbom, zbog nepredvidive, neuobičajene i specifične prirode kibersigurnosnog okruženja, trebao omogućiti prijenos neiskorištenih sredstava koja premašuju ona utvrđena u Financijskoj uredbi, čime bi se maksimalno povećao kapacitet mehanizma za izvanredne kibersigurnosne situacije za potporu državama članicama u djelotvornoj borbi protiv kiberprijetnji.	(11) U svrhu dobrog financijskog upravljanja trebalo bi utvrditi posebna pravila za prijenos neiskorištenih odobrenih sredstava za preuzete obveze i odobrenih sredstava za plaćanje. Uz poštovanje načela da se proračun Unije utvrđuje na godišnjoj razini, ovom bi se Uredbom, zbog nepredvidive, neuobičajene i specifične prirode kibersigurnosnog okruženja, trebao omogućiti prijenos neiskorištenih sredstava koja premašuju ona utvrđena u Financijskoj uredbi, čime bi se maksimalno povećao kapacitet mehanizma za izvanredne kibersigurnosne situacije za potporu državama članicama u djelotvornoj borbi protiv kiberprijetnji. ***Ta posebna pravila ujedno bi omogućila dugoročnu financijsku potporu za zajedničku nabavu ultrasigurnih alata i infrastrukture sljedeće generacije, kako bi se poboljšali zajednički kapaciteti za otkrivanje primjenom najnovije umjetne inteligencije i analize podataka.***

Amandman 10

Prijedlog uredbe
Uvodna izjava 13.

Tekst koji je predložila Komisija	*Izmjena*
(13) Svaka bi država članica trebala na nacionalnoj razini imenovati javnopravno tijelo zaduženo za koordinaciju aktivnosti otkrivanja kiberprijetnji u toj državi članici. Ti nacionalni SOC-ovi trebali bi djelovati kao referentna i pristupna točka na nacionalnoj razini za sudjelovanje u europskom kiberštitu te bi trebali osigurati da se informacije o kiberprijetnjama dobivene od javnih i privatnih subjekata dijele i prikupljaju na nacionalnoj razini na učinkovit i pojednostavnjen način.	(13) Svaka bi država članica trebala na nacionalnoj razini imenovati javnopravno tijelo zaduženo za koordinaciju aktivnosti otkrivanja kiberprijetnji u toj državi članici. Ti nacionalni SOC-ovi trebali bi djelovati kao referentna i pristupna točka na nacionalnoj razini za sudjelovanje u europskom kiberštitu te bi trebali osigurati da se informacije o kiberprijetnjama dobivene od javnih i privatnih subjekata dijele i prikupljaju na nacionalnoj razini na učinkovit i pojednostavnjen način. ***Kada je to izvedivo i potrebno, SOC-ovi bi također trebali omogućiti sudjelovanje obrambenih subjekata, uspostavljajući „obrambeni stup" u smislu upravljanja i vrste informacija koje se dijele, kao što je navedeno u zajedničkoj komunikaciji „Politika EU-a o kiberobrani"[1] i kao što je podržao Visoki predstavnik.***
	[1] Zajednička komunikacija Europskom parlamentu i Vijeću „Politika EU-a o kiberobrani", JOIN/2022/49 final

Amandman 11

Prijedlog uredbe
Uvodna izjava 14.

Tekst koji je predložila Komisija	*Izmjena*
(14) U okviru europskog kiberštita trebalo bi uspostaviti niz prekograničnih centara za sigurnosne operacije („prekograničnih SOC-ova"). U njima bi se trebali okupiti nacionalni SOC-ovi iz najmanje triju država članica kako bi se u potpunosti ostvarile koristi od otkrivanja prekograničnih prijetnji te dijeljenja informacija i upravljanja njima. Opći cilj	(14) U okviru europskog kiberštita trebalo bi uspostaviti niz prekograničnih centara za sigurnosne operacije („prekograničnih SOC-ova"). U njima bi se trebali okupiti nacionalni SOC-ovi iz najmanje triju država članica***, uključujući „obrambeni stup",*** kako bi se u potpunosti ostvarile koristi od otkrivanja prekograničnih prijetnji te dijeljenja

prekograničnih SOC-ova trebao bi biti jačanje kapaciteta za analizu, sprečavanje i otkrivanje kibersigurnosnih prijetnji te podupiranje proizvodnje visokokvalitetnih obavještajnih podataka o kibersigurnosnim prijetnjama, osobito dijeljenjem podataka iz različitih izvora, javnih ili privatnih te dijeljenjem i zajedničkom uporabom najsuvremenijih alata i zajedničkim razvojem sposobnosti otkrivanja, analize i sprečavanja u pouzdanom okruženju. Njima bi se trebali osigurati dodatni kapaciteti, koji se temelje na postojećim SOC-ovima i timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovima) i drugim relevantnim akterima te ih nadopunjuju.

informacija i upravljanja njima. Opći cilj prekograničnih SOC-ova trebao bi biti jačanje kapaciteta za analizu, sprečavanje i otkrivanje kibersigurnosnih prijetnji te podupiranje proizvodnje visokokvalitetnih obavještajnih podataka o kibersigurnosnim prijetnjama, osobito dijeljenjem podataka iz različitih izvora, javnih ili privatnih***, a kada je to potrebno i izvedivo, vojnih izvora, uz pružanje dostatnih smjernica za dijeljenje informacija,*** te dijeljenjem i zajedničkom uporabom najsuvremenijih alata i zajedničkim razvojem sposobnosti otkrivanja, analize i sprečavanja u pouzdanom okruženju. Njima bi se trebali osigurati dodatni kapaciteti, koji se temelje na postojećim SOC-ovima i timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovima) i drugim relevantnim akterima te ih nadopunjuju.

Amandman 12

Prijedlog uredbe
Uvodna izjava 15.

Tekst koji je predložila Komisija	*Izmjena*
(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsuvremenijim alatima te doprinosili razvoju sposobnosti i ***tehnološke suverenosti*** Unije.	(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsuvremenijim alatima te doprinosili razvoju sposobnosti i ***otpornosti*** Unije.

Amandman 13

Prijedlog uredbe
Uvodna izjava 16.

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

Amandman 14

Prijedlog uredbe
Uvodna izjava 17.

Tekst koji je predložila Komisija	*Izmjena*
(17) Nužan preduvjet za pripravnost i koordinaciju na razini Unije u pogledu značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera je da relevantna tijela budu jednako informirana o stanju. Direktivom (EU) 2022/2555 uspostavlja se EU-CyCLONe kako bi se omogućilo koordinirano upravljanje kibersigurnosnim	(17) Nužan preduvjet za pripravnost i koordinaciju na razini Unije u pogledu značajnih kibersigurnosnih incidenata i kibersigurnosnih incidenata velikih razmjera je da relevantna tijela budu jednako informirana o stanju. Direktivom (EU) 2022/2555 uspostavlja se EU-CyCLONe kako bi se omogućilo koordinirano upravljanje kibersigurnosnim

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

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

Amandman 15

Prijedlog uredbe
Uvodna izjava 19.

Tekst koji je predložila Komisija	*Izmjena*
(19) Kako bi se omogućilo da se opsežna razmjena podataka o kibersigurnosnim prijetnjama iz različitih izvora odvija u pouzdanom okruženju, subjekti koji sudjeluju u europskom	(19) Kako bi se omogućilo da se opsežna razmjena podataka o kibersigurnosnim prijetnjama iz različitih izvora odvija u pouzdanom okruženju, subjekti koji sudjeluju u europskom

kiberštitu trebali bi biti opremljeni najsuvremenijim i vrlo sigurnim alatima, opremom i infrastrukturom. Time bi se trebalo omogućiti poboljšanje zajedničkih kapaciteta za otkrivanje i pravodobno upozoravanje nadležnih tijela i relevantnih subjekata, posebno uporabom najnovijih tehnologija umjetne inteligencije i analitike podataka.

kiberštitu trebali bi biti opremljeni najsuvremenijim i vrlo sigurnim alatima, opremom i infrastrukturom***, isključujući visokorizične dobavljače kritičnih proizvoda s digitalnim elementima***. 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. ***Pri upotrebi umjetne inteligencije trebalo bi osigurati ljudski nadzor te osigurati dovoljnu razinu pismenosti u području umjetne inteligencije, potrebnu potporu i ovlast za izvršavanje te funkcije.***

Amandman 16

Prijedlog uredbe
Uvodna izjava 19.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(19.a) U skladu s Uredbom [XX/XXXX (Akt o kiberotpornosti)] subjekti koji sudjeluju u europskom kiberštitu trebali bi obuhvaćati i zahtjeve utvrđene ovom Uredbom za sve proizvode s digitalnim elementima. S obzirom na sve veće rizike koji proizlaze iz gospodarske ovisnosti, potrebno je minimizirati izloženost visokorizičnim dobavljačima kritičnih proizvoda uz pomoć zajedničkog strateškog okvira za gospodarsku sigurnost EU-a. Ovisnost o visokorizičnim dobavljačima kritičnih proizvoda s digitalnim elementima predstavlja strateški rizik koji bi trebalo riješiti na razini Unije, posebno pitanje sudjeluje li država u industrijskoj špijunaži ili gospodarskoj prisili te propisuje li njezino zakonodavstvo proizvoljan pristup bilo kojoj vrsti poslovanja ili podataka poduzeća, posebno kada su kritični proizvodi namijenjeni uporabi od strane ključnih subjekata iz Direktive (EU)

Amandman 17

Prijedlog uredbe
Uvodna izjava 20.

Tekst koji je predložila Komisija	*Izmjena*
(20) Prikupljanjem, dijeljenjem i razmjenom podataka europski kiberštit trebao bi povećati tehnološku suverenost Unije. Objedinjavanje visokokvalitetnih prilagođenih podataka trebalo bi doprinijeti i razvoju naprednih tehnologija umjetne inteligencije i analitike podataka. To bi trebalo omogućiti povezivanjem europskog kiberštita s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom Uredbom Vijeća (EU) 2021/1173[25].	(20) Prikupljanjem, dijeljenjem i razmjenom podataka europski kiberštit trebao bi povećati tehnološku suverenost***, strateško autonomiju, konkurentnost i otpornost*** Unije. Objedinjavanje visokokvalitetnih prilagođenih podataka trebalo bi doprinijeti i razvoju naprednih tehnologija umjetne inteligencije i analitike podataka. To bi trebalo omogućiti povezivanjem europskog kiberštita s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom Uredbom Vijeća (EU) 2021/1173[25].
[25] Uredba Vijeća (EU) 2021/1173 od 13. srpnja 2021. o osnivanju Zajedničkog poduzeća za europsko računalstvo visokih performansi te stavljanju izvan snage Uredbe (EU) 2018/1488 (SL L 256, 19.7.2021., str. 3.).	[25] Uredba Vijeća (EU) 2021/1173 od 13. srpnja 2021. o osnivanju Zajedničkog poduzeća za europsko računalstvo visokih performansi te stavljanju izvan snage Uredbe (EU) 2018/1488 (SL L 256, 19.7.2021., str. 3.).

Amandman 18

Prijedlog uredbe
Uvodna izjava 25.

Tekst koji je predložila Komisija	*Izmjena*
(25) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružiti potpora državama članicama te bi se trebale dopuniti njihove vlastite mjere i resursi te druge postojeće mogućnosti potpore u slučaju odgovora na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera i hitnog oporavka od njih, kao što su usluge koje	(25) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se pružiti potpora državama članicama te bi se trebale dopuniti njihove vlastite mjere i resursi te druge postojeće mogućnosti potpore u slučaju odgovora na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera i hitnog oporavka od njih, kao što su usluge koje

pruža Agencija Europske unije za kibersigurnost (ENISA) u skladu sa svojim mandatom, koordinirani odgovor i pomoć mreže CSIRT-ova, potpora za ublažavanje posljedica koju pruža EU-CyCLONe, te uzajamna pomoć među državama članicama, među ostalim u kontekstu članka 42. stavka 7. UEU-a, timovi za brz odgovor na kiberincidente u okviru PESCO-a***[26]*** i timovi za brz odgovor na hibridne prijetnje. Njime bi se trebalo odgovoriti na potrebu da se osigura dostupnost specijaliziranih sredstava za potporu pripravnosti i odgovoru na kibersigurnosne incidente u cijeloj Uniji i u trećim zemljama.

pruža Agencija Europske unije za kibersigurnost (ENISA) u skladu sa svojim mandatom, koordinirani odgovor i pomoć mreže CSIRT-ova, potpora za ublažavanje posljedica koju pruža EU-CyCLONe, te uzajamna pomoć među državama članicama, među ostalim u kontekstu članka 42. stavka 7. UEU-a, timovi za brz odgovor na kiberincidente u okviru ***PESCO-a[1], novi projekt*** PESCO-a ***Koordinacijski centar za kibernetičko i informacijsko područje (CIDCC) i njegov predloženi nasljednik Koordinacijski centar za kiberobranu EU-a (EUCDCC), kao*** i timovi za brz odgovor na hibridne prijetnje. Njime bi se trebalo odgovoriti na potrebu da se osigura dostupnost specijaliziranih sredstava za potporu pripravnosti i odgovoru na kibersigurnosne incidente u cijeloj Uniji i u trećim zemljama***, posebno u onim zemljama kandidatkinjama za članstvo u EU-u koje su usklađene sa zajedničkom vanjskom i sigurnosnom politikom, kako bi im se pružila potpora u izgradnji njihovih kibersposobnosti i jačanju prekogranične i regionalne suradnje među tim zemljama kandidatkinjama u području kiberprostora***.

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

---

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

---

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

Amandman 19

Prijedlog uredbe
Uvodna izjava 26.

Tekst koji je predložila Komisija	*Izmjena*
(26) Ovim se instrumentom ne dovode u pitanje postupci i okviri za koordinaciju odgovora na krizu na razini Unije, posebno Mehanizam Unije za civilnu zaštitu[27], IPCR[28], i Direktiva (EU) 2022/2555. Može doprinijeti ili dopuniti mjere koje su donesene u kontekstu članka 42. stavka 7. UEU-a ili u situacijama definiranima u članku 222. UFEU-a. Uporabu ovog instrumenta trebalo bi***, prema potrebi,*** koordinirati i s provedbom mjera u okviru alata za kiberdiplomaciju.	(26) Ovim se instrumentom ne dovode u pitanje postupci i okviri za koordinaciju odgovora na krizu na razini Unije, posebno Mehanizam Unije za civilnu zaštitu[27], IPCR[28], i Direktiva (EU) 2022/2555. Može doprinijeti ili dopuniti mjere koje su donesene u kontekstu članka 42. stavka 7. UEU-a ili u situacijama definiranima u članku 222. UFEU-a. Uporabu ovog instrumenta trebalo bi koordinirati i s provedbom mjera u okviru alata za kiberdiplomaciju***, čime bi se poboljšala suradnja na strateškoj, operativnoj i tehničkoj razini između kiberobrane i drugih kiberzajednica, posebno kako bi se ojačale sposobnosti za suzbijanje kibersigurnosnih prijetnji koje dolaze izvan Unije, uključujući mjere ograničavanja, koje se mogu upotrijebiti za sprečavanje zlonamjernih kiberaktivnosti i odgovor na njih***.
[27] 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.).	[27] 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.).
[28] Aranžmani za integrirani politički odgovor na krizu (IPCR) u skladu s Preporukom Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera.	[28] Aranžmani za integrirani politički odgovor na krizu (IPCR) u skladu s Preporukom Komisije (EU) 2017/1584 od 13. rujna 2017. o koordiniranom odgovoru na kiberincidente i kiberkrize velikih razmjera.

Amandman 20

Prijedlog uredbe
Uvodna izjava 28.

Tekst koji je predložila Komisija	*Izmjena*
(28) Prema Direktivi (EU) 2022/2555 države članice dužne su imenovati ili uspostaviti jedno ili više tijela za	(28) Prema Direktivi (EU) 2022/2555 države članice dužne su imenovati ili uspostaviti jedno ili više tijela za

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

Amandman 21

Prijedlog uredbe
Uvodna izjava 29.

Tekst koji je predložila Komisija	*Izmjena*
(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni	(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni

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

kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. ***Po potrebi, Europska služba za vanjsko djelovanje (ESVD), posebno putem Obavještajnog i situacijskog centra EU-a (INTCEN) i njegove jedinice za otkrivanje hibridnih prijetnji, uz potporu Obavještajne uprave Vojnog stožera Europske unije (EUMS) u okviru Službe za jedinstvenu obavještajnu analizu (SIAC), također bi trebala biti uključena kako bi osigurala ažurne procjene i time doprinijela utvrđivanju sektora*** ili ***podsektora koje*** bi ***trebalo*** odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti"). Koordinirane vježbe testiranja trebale bi se temeljiti na zajedničkim scenarijima i metodama procjene rizika***. Te vježbe mogu imati važnu ulogu i u poboljšanju suradnje civilnih i vojnih subjekata. Komisija, ESVD i ENISA stoga bi pri organiziranju vježbi trebali sustavno razmatrati uključivanje sudionika iz drugih kiberzajednica, kao što su Europska obrambena agencija (EDA) i drugi relevantni subjekti.*** Pri odabiru sektora i razvoju scenarija rizika trebalo bi uzeti u obzir relevantne procjene rizika i scenarije rizika na razini Unije, uključujući potrebu za izbjegavanjem njihova udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje trebaju provesti Komisija, Visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, u koordinaciji s relevantnim civilnim i vojnim tijelima i

jačanje otpornosti kritične infrastrukture.

agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za elektroničke komunikacije (BEREC), koordinirane procjene rizika koje treba provesti na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i ***Vijeća[1]***. Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

[1] 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.

---

[29] 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.

[29] 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.

Amandman 22

Prijedlog uredbe
Uvodna izjava 32.

Tekst koji je predložila Komisija	*Izmjena*
(32) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se podupirati pomoć koju države članice pružaju državi članici pogođenoj	(32) Mehanizmom za izvanredne kibersigurnosne situacije trebala bi se podupirati pomoć koju države članice pružaju državi članici pogođenoj

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

značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera, među ostalim u okviru mreže CSIRT-ova utvrđene u članku 15. Direktive (EU) 2022/2555. Državama članicama koje pružaju pomoć trebalo bi dopustiti podnošenje zahtjeva za pokrivanje troškova povezanih sa slanjem timova stručnjaka u okviru pružanja uzajamne pomoći***, osiguravajući učinkovitu koordinaciju relevantnih programa i instrumenata EU-a, među ostalim Europskog instrumenta mirovne pomoći (EPF), ZVSP-a i Instrumenta za susjedstvo, razvoj i međunarodnu suradnju, prilikom pružanja pomoći trećim zemljama, posebno Ukrajini i Moldovi***. Prihvatljivi troškovi mogli bi uključivati putne troškove, troškove smještaja i dnevnice stručnjaka za kibersigurnost.

Amandman 23

Prijedlog uredbe
Uvodna izjava 33.

Tekst koji je predložila Komisija	*Izmjena*
(33) Na razini Unije trebalo bi postupno uspostaviti kibersigurnosnu pričuvu koja bi se sastojala od usluga privatnih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i hitne mjere oporavka u slučajevima značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera. Kibersigurnosna pričuva EU-a trebala bi osigurati dostupnost i spremnost usluga. Usluge iz kibersigurnosne pričuve EU-a trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima koji djeluju u kritičnim ili visokokritičnim sektorima te nadopunjavati njihovo djelovanje na nacionalnoj razini. Pri podnošenju zahtjeva za potporu iz kibersigurnosne pričuve EU-a države članice trebale bi navesti vrstu potpore	(33) Na razini Unije trebalo bi postupno uspostaviti kibersigurnosnu pričuvu koja bi se sastojala od usluga privatnih pružatelja upravljanih sigurnosnih usluga kako bi se poduprli odgovor i hitne mjere oporavka u slučajevima značajnih kibersigurnosnih incidenata ili kibersigurnosnih incidenata velikih razmjera. Kibersigurnosna pričuva EU-a trebala bi osigurati dostupnost i spremnost usluga. Usluge iz kibersigurnosne pričuve EU-a trebale bi služiti kao potpora nacionalnim tijelima u pružanju pomoći pogođenim subjektima koji djeluju u kritičnim ili visokokritičnim sektorima te nadopunjavati njihovo djelovanje na nacionalnoj razini. Pri podnošenju zahtjeva za potporu iz kibersigurnosne pričuve EU-a države članice trebale bi navesti vrstu potpore

pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni zahtjeva države članice. Usluge iz kibersigurnosne pričuve EU-a mogu služiti i za potporu institucijama, tijelima i agencijama Unije pod sličnim uvjetima.

pruženu pogođenom subjektu na nacionalnoj razini, koju bi trebalo uzeti u obzir pri procjeni zahtjeva države članice. Usluge iz kibersigurnosne pričuve EU-a mogu služiti i za potporu institucijama, tijelima i agencijama Unije***, uključujući misije ZSOP-a,*** pod sličnim uvjetima.

Amandman 24

Prijedlog uredbe
Uvodna izjava 34.

Tekst koji je predložila Komisija	*Izmjena*
(34) U svrhu odabira privatnih pružatelja usluga koji će pružati usluge u kontekstu kibersigurnosne pričuve EU-a potrebno je utvrditi skup minimalnih kriterija koje bi trebalo uključiti u poziv na podnošenje ponuda za odabir tih pružatelja, kako bi se ispunile potrebe tijela i subjekata država članica koji djeluju u kritičnim ili visokokritičnim sektorima.	(34) U svrhu odabira privatnih pružatelja usluga koji će pružati usluge u kontekstu kibersigurnosne pričuve EU-a potrebno je utvrditi skup minimalnih kriterija koje bi trebalo uključiti u poziv na podnošenje ponuda za odabir tih pružatelja, kako bi se ispunile potrebe tijela i subjekata država članica koji djeluju u kritičnim ili visokokritičnim sektorima***, uzimajući u obzir i rizike povezane sa sudjelovanjem pružatelja iz zemalja strateških konkurenata, koji mogu dovesti do rizika za gospodarsku sigurnost, te posljedice za stratešku sigurnost Unije***.

Amandman 25

Prijedlog uredbe
Uvodna izjava 36.

Tekst koji je predložila Komisija	*Izmjena*
(36) Kako bi se poduprli ciljevi ove Uredbe koji se odnose na promicanje zajedničke informiranosti o stanju, jačanje otpornosti Unije i omogućivanje djelotvornog odgovora na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, mreža EU-CyCLONe, mreža CSIRT-ova ili Komisija trebali bi moći zatražiti od ENISA-e da istraži i procijeni prijetnje, ranjivosti i	(36) Kako bi se poduprli ciljevi ove Uredbe koji se odnose na promicanje zajedničke informiranosti o stanju, jačanje otpornosti Unije i omogućivanje djelotvornog odgovora na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, mreža EU-CyCLONe, mreža CSIRT-ova ili Komisija trebali bi moći zatražiti od ENISA-e da istraži i procijeni prijetnje, ranjivosti i

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

mjere ublažavanja povezane s određenim značajnim kibersigurnosnim incidentom ili kibersigurnosnim incidentom velikih razmjera. ***S obzirom na razvoj sigurnog sustava povezivosti koji se temelji na europskoj kvantnoj komunikacijskoj infrastrukturi (EuroQCI) i državnim satelitskim komunikacijama Europske unije (GOVSATCOM), a posebno provedbu GNSS-a GALILEO za korisnike u obrani, pri svakom budućem eventualnom razvoju trebalo bi uzeti u obzir pojavu „hiper rata" u kojem se objedinjuju brzina i sofisticiranost kvantnog računalstva s visokoautonomnim vojnim sustavima.*** Nakon dovršetka istraživanja i procjene incidenta ENISA bi trebala pripremiti izvješće o istraživanju incidenta u suradnji s relevantnim dionicima, uključujući predstavnike iz privatnog sektora, države članice, Komisiju i druge relevantne institucije, tijela i agencije EU-a. Kad je riječ o privatnom sektoru, ENISA razvija kanale za razmjenu informacija sa specijaliziranim pružateljima usluga, uključujući pružatelje upravljanih sigurnosnih rješenja i dobavljače, kako bi ostvarila svoju misiju postizanja visoke zajedničke razine kibersigurnosti u Uniji. Na temelju suradnje s dionicima, uključujući privatni sektor, izvješće o istraživanju određenih incidenata trebalo bi biti usmjereno na procjenu uzroka, učinaka i mjera ublažavanja posljedica incidenta nakon što se on dogodio. Posebnu pozornost trebalo bi posvetiti informacijama i iskustvima koje dijele pružatelji upravljanih sigurnosnih usluga koji ispunjavaju uvjete najvišeg profesionalnog integriteta, nepristranosti i potrebnog tehničkog stručnog znanja u skladu s ovom Uredbom. Izvješće bi trebalo dostaviti i mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji te bi ga oni trebali uzeti u obziru u svom radu. Ako se incident odnosi na treću zemlju, Komisija bi izvješće trebala poslati Visokom predstavniku***, ESVD-u i svakoj misiji***

ZSOP-a u zemlji pogođenoj incidentom putem njezinog sjedišta.

Amandman 26

Prijedlog uredbe
Uvodna izjava 37.

Tekst koji je predložila Komisija	*Izmjena*
(37) S obzirom na nepredvidivu prirodu kibernapada i činjenicu da ti napadi često nisu ograničeni na određeno zemljopisno područje te da postoji visok rizik od prelijevanja, jačanje otpornosti susjednih zemalja i njihove sposobnosti da učinkovito odgovore na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera doprinosi zaštiti Unije u cjelini. Stoga treće zemlje pridružene programu Digitalna Europa ***mogu*** primiti potporu iz kibersigurnosne pričuve EU-a, ***ako*** je ***to predviđeno odgovarajućim sporazumom o pridruživanju programu Digitalna Europa***. Unija bi trebala podupirati financiranje pridruženih trećih zemalja u okviru relevantnih partnerstava i instrumenata financiranja za te zemlje. Potpora bi trebala obuhvaćati usluge za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera te hitnog oporavka od njih. Uvjeti za kibersigurnosnu pričuvu EU-a i pouzdane pružatelje usluga utvrđeni u ovoj Uredbi trebali bi se primjenjivati pri pružanju potpore trećim zemljama pridruženima programu Digitalna Europa.	(37) S obzirom na nepredvidivu prirodu kibernapada i činjenicu da ti napadi često nisu ograničeni na određeno zemljopisno područje te da postoji visok rizik od prelijevanja, jačanje otpornosti susjednih zemalja***, osobito Ukrajine i Moldove,*** i njihove sposobnosti da učinkovito odgovore na značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera doprinosi zaštiti Unije u cjelini. Stoga ***bi*** treće zemlje pridružene programu Digitalna Europa ***trebale*** primiti potporu iz kibersigurnosne pričuve EU-a***. Potpora bi se trebala primijeniti i na one treće zemlje u kojima je raspoređena misija ZSOP-a s posebnim mandatom za jačanje otpornosti na hibridne prijetnje***, ***među ostalim kiberprijetnje, ili u kojima*** je ***usvojena mjera pomoći u okviru Europskog instrumenta mirovne pomoći za jačanje kiberotpornosti te zemlje***. Unija bi trebala podupirati financiranje pridruženih trećih zemalja u okviru relevantnih partnerstava i instrumenata financiranja za te zemlje. Potpora bi trebala obuhvaćati usluge za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera te hitnog oporavka od njih. Uvjeti za kibersigurnosnu pričuvu EU-a i pouzdane pružatelje usluga utvrđeni u ovoj Uredbi trebali bi se primjenjivati pri pružanju potpore trećim zemljama pridruženima programu Digitalna Europa.

Amandman 27

Prijedlog uredbe
Članak 1. – stavak 1. – točka c

Tekst koji je predložila Komisija	*Izmjena*
(c) uspostavom europskog mehanizma za istraživanje kibersigurnosnih incidenata radi istraživanja i procjenjivanja značajnih incidenata ili incidenata velikih razmjera.	(c) uspostavom europskog mehanizma za istraživanje kibersigurnosnih incidenata radi istraživanja i procjenjivanja značajnih incidenata ili ***prijetnji ili*** incidenata ***ili prijetnji*** velikih razmjera.

Amandman 28

Prijedlog uredbe
Članak 1. – stavak 2. – točka a

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

Amandman 29

Prijedlog uredbe
Članak 1. – stavak 2. – točka b

Tekst koji je predložila Komisija	*Izmjena*
(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu	(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu

Digitalna Europa („DEP”);	Digitalna Europa („DEP”) ***ili onim trećim zemljama koje su kandidati za pristupanje Uniji i nisu u suprotnosti sa sigurnosnim i obrambenim interesima Unije i država članica, kako je utvrđeno u okviru ZVSP-a u skladu s glavom V. UEU-a***; ***Države članice trebale bi aktivni program kiberobrane smatrati dijelom svoje nacionalne strategije za kibersigurnost koja uključuje redovite zajedničke vježbe osposobljavanja među državama članicama i u međunarodnim organizacijama. Takvim bi se programom trebao osigurati sinkronizirani kapacitet u stvarnom vremenu za otkrivanje, utvrđivanje, analizu i ublažavanje prijetnji.***

Amandman 30

Prijedlog uredbe
Članak 1. – stavak 2.a (novi)

Tekst koji je predložila Komisija	*Izmjena*
	2.a smanjenje sustavnih kibersigurnosnih rizika zbog ovisnosti o kritičnoj opremi iz zemalja koje bi bile u suprotnosti sa sigurnosnim i obrambenim interesima Unije i njezinih država članica kako je utvrđeno u okviru ZVSP-a u skladu s glavom V. UEU-a;

Amandman 31

Prijedlog uredbe
Članak 2. – stavak 2.a (novi)

Tekst koji je predložila Komisija	*Izmjena*
	„zajednica za kiberobranu” znači tijela za obranu država članica uz potporu institucija, tijela i agencija EU-a kako je navedeno u Zajedničkoj komunikaciji „Politika EU-a o kiberobrani”[1]
	[1] Zajednička komunikacija Europskom

parlamentu i Vijeću „Politika EU-a o kiberobrani”, JOIN/2022/49 final

Amandman 32

Prijedlog uredbe
Članak 3. – stavak 2. − podstavak 1. − točka ba (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(ba) pruža pomoć u modernizaciji svih sustava kiberobrane, povećanju kvalitete kapaciteta za kiberobranu uvođenjem sustava umjetne inteligencije i ubrzanju razmjene informacija među nacionalnim SOC-ovima i prekograničnim SOC-ovima;

Amandman 33

Prijedlog uredbe
Članak 3. – stavak 2. − podstavak 1. − točka da (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(da) pregledava i ocjenjuje kritične kibersigurnosne tehnologije i opremu kojima se koriste SOC-ovi u odgovoru na kibersigurnosne incidente za sustavne rizike od kontrole zemalja nad visokorizičnim pružateljima koje bi bile u suprotnosti sa sigurnosnim i obrambenim interesima Unije i njezinih država članica kako je utvrđeno u okviru ZVSP-a u skladu s glavom V. UEU-a;

Amandman 34

Prijedlog uredbe
Članak 4. – stavak 1. – podstavak 2.

Tekst koji je predložila Komisija	*Izmjena*
Mora moći služiti drugim javnim i privatnim organizacijama na nacionalnoj razini kao referentna i pristupna točka za	Mora moći služiti drugim javnim i privatnim ***te, prema potrebi, vojnim*** organizacijama na nacionalnoj razini kao

prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. Mora biti opremljen najsuvremenijim tehnologijama za otkrivanje, agregiranje i analiziranje podataka relevantnih za kibersigurnosne prijetnje i incidente.	referentna i pristupna točka za prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. Mora biti opremljen najsuvremenijim tehnologijama za otkrivanje, agregiranje i analiziranje podataka relevantnih za kibersigurnosne prijetnje i incidente.

Amandman 35

Prijedlog uredbe
Članak 4. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Nakon poziva na iskaz interesa Europski stručni centar u području kibersigurnosti („ECCC”) odabire nacionalne SOC-ove za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može odabranim nacionalnim SOC-ovima dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski doprinos Unije pokriva do 50 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva država članica. Prije pokretanja postupka nabave alata i infrastrukture ECCC i nacionalni SOC sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.	2. Nakon poziva na iskaz interesa Europski stručni centar u području kibersigurnosti („ECCC”) odabire nacionalne SOC-ove za sudjelovanje u zajedničkoj nabavi alata i infrastrukture s ECCC-om. ECCC može odabranim nacionalnim SOC-ovima dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture***, pod strogim uvjetom da te alate i infrastrukturu osiguravaju pouzdani pružatelji u skladu s člankom 16***. Financijski doprinos Unije pokriva do 50 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva država članica. Prije pokretanja postupka nabave alata i infrastrukture ECCC i nacionalni SOC sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.

Amandman 36

Prijedlog uredbe
Članak 5. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Nakon poziva na iskaz interesa ECCC odabire konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata i	2. Nakon poziva na iskaz interesa ECCC odabire konzorcij domaćin za sudjelovanje u zajedničkoj nabavi alata i

infrastrukture s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture. Financijski doprinos Unije pokriva do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva konzorcij domaćin. Prije pokretanja postupka nabave alata i infrastrukture ECCC i konzorcij domaćin sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.	infrastrukture s ECCC-om. ECCC može konzorciju domaćinu dodijeliti bespovratna sredstva za financiranje rada tih alata i infrastrukture***, pod strogim uvjetom da te alate i infrastrukturu osiguravaju pouzdani pružatelji u skladu s člankom 16***. Financijski doprinos Unije pokriva do 75 % troškova nabave alata i infrastrukture te do 50 % operativnih troškova, a preostale troškove pokriva konzorcij domaćin. Prije pokretanja postupka nabave alata i infrastrukture ECCC i konzorcij domaćin sklapaju ugovor o smještaju i korištenju kojim se uređuje korištenje alata i infrastrukture.

Amandman 37

Prijedlog uredbe
Članak 5. – stavak 2.a (novi)

Tekst koji je predložila Komisija	*Izmjena*
	2.a Automatski se isključuje svaka infrastruktura ili pružatelj usluga koji potječu iz visokorizične treće zemlje.

Amandman 38

Prijedlog uredbe
Članak 6. – stavak 1. – točka ba (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(ba) izravno podupire jačanje vojnih i obrambenih kapaciteta članova sudionika ili sprečava izravnu i neposrednu prijetnju njihovoj sigurnosti; s obzirom na to da iskorištavanje ranjivosti u obrambenom sektoru može prouzročiti znatne poremećaje i štetu, za kibersigurnost obrambene industrije potrebne su posebne mjere kako bi se zajamčila sigurnost lanaca opskrbe, posebno subjekata niže u lancima opskrbe, kojima nije potreban pristup klasificiranim podacima, ali koji bi mogli predstavljati ozbiljan rizik za

	cijeli sektor; posebnu pozornost trebalo bi posvetiti utjecaju bilo kojeg kršenja i prijetnji od bilo koje potencijalne manipulacije mrežnim podacima koja bi ključne obrambene resurse mogla učiniti beskorisnima ili čak nadvladati njihov operativni sustav, čineći ih ranjivima na protupravno oduzimanje;

Amandman 39

Prijedlog uredbe
Članak 6. – stavak 1. – točka ba (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(bb) podržava osnaživanje obrambenih kapaciteta članova sudionika ili sprečava izravnu i neposrednu prijetnju njegovoj sigurnosti, čime jamči sigurnost lanaca opskrbe, posebno subjekata niže u lancima opskrbe, kojima nije potreban pristup klasificiranim podacima, ali koji bi mogli predstavljati ozbiljan rizik za cijeli sektor.

Amandman 40

Prijedlog uredbe
Članak 7. – stavak 1.

Tekst koji je predložila Komisija	*Izmjena*
1. Ako prekogranični SOC-ovi dobiju informacije o potencijalnom ili aktualnom kibersigurnosnom incidentu velikih razmjera, oni bez nepotrebne odgode dostavljaju relevantne informacije mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji prema njihovim ulogama u upravljanju krizama u skladu s Direktivom (EU) 2022/2555.	1. Ako prekogranični SOC-ovi dobiju informacije o potencijalnom ili aktualnom kibersigurnosnom incidentu velikih razmjera, oni bez nepotrebne odgode dostavljaju relevantne informacije mreži EU-CyCLONe, mreži CSIRT-ova i Komisiji***, kao i Visokom predstavniku i ESVD-u ako se tiče treće zemlje,*** prema njihovim ulogama u upravljanju krizama u skladu s Direktivom (EU) 2022/2555.

Amandman 41

Prijedlog uredbe
Članak 8. – stavak 1.

Tekst koji je predložila Komisija	*Izmjena*
1. Države članice koje sudjeluju u europskom kiberštitu osiguravaju visoku razinu sigurnosti podataka i fizičke sigurnosti infrastrukture europskog kiberštita te primjereno upravljanje i kontrolu nad tom infrastrukturom kako bi je se zaštitilo od prijetnji i kako bi bila zajamčena njezina sigurnost i sigurnost sustava, uključujući ***podatke*** koji se razmjenjuju s pomoću te infrastrukture.	1. Države članice koje sudjeluju u europskom kiberštitu osiguravaju visoku razinu sigurnosti podataka i fizičke sigurnosti infrastrukture europskog kiberštita te primjereno upravljanje i kontrolu nad tom infrastrukturom kako bi je se zaštitilo od prijetnji i kako bi bila zajamčena njezina sigurnost i sigurnost sustava, ***smanjujući rizike i promičući tehnološke prednosti EU-a u kritičnim sektorima,*** uključujući ***mjere za ograničavanje ili isključivanje visokorizičnih dobavljača, kao i za zaštitu podataka*** koji se razmjenjuju s pomoću te infrastrukture.

Amandman 42

Prijedlog uredbe
Članak 8. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Države članice koje sudjeluju u europskom kiberštitu osiguravaju da dijeljenje informacija u okviru europskog kiberštita sa subjektima koji nisu javna tijela države članice ne šteti sigurnosnim interesima Unije.	2. Države članice koje sudjeluju u europskom kiberštitu osiguravaju da dijeljenje informacija u okviru europskog kiberštita sa subjektima koji nisu javna tijela države članice ne šteti sigurnosnim interesima Unije ***te da je svako dijeljenje informacija s visokorizičnim pružateljima ograničeno i da ne dovodi u pitanje sigurnost i strateške interese Unije***.

Amandman 43

Prijedlog uredbe
Članak 8. – stavak 3.

Tekst koji je predložila Komisija	*Izmjena*
3. Komisija može donijeti provedbene akte kojima se utvrđuju tehnički zahtjevi za ispunjavanje obveze država članica propisane u stavcima 1. i 2. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2. ove Uredbe. Kako bi se olakšala suradnja s vojnim akterima, Komisija pritom, uz podršku Visokog predstavnika, uzima u obzir relevantne obrambene sigurnosne standarde.	3. Komisija može donijeti provedbene akte kojima se utvrđuju tehnički zahtjevi za ispunjavanje obveze država članica propisane u stavcima 1. i 2. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 21. stavka 2. ove Uredbe. Kako bi se olakšala suradnja s vojnim akterima, Komisija pritom, uz podršku Visokog predstavnika, uzima u obzir relevantne obrambene sigurnosne standarde***, uz odgovarajuću uporabu čitavog niza obrambenih mogućnosti dostupnih civilnoj i vojnoj zajednici za širu sigurnost i obranu EU-a, te obavješćuje Europski parlament***.

Amandman 44

Prijedlog uredbe
Članak 9. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Djelovanja radi primjene mehanizma za izvanredne kibersigurnosne situacije podupiru se sredstvima iz programa Digitalna Europa i provode u skladu s Uredbom (EU) 2021/694, osobito njezinim specifičnim ciljem 3.	2. Djelovanja radi primjene mehanizma za izvanredne kibersigurnosne situacije podupiru se sredstvima iz programa Digitalna Europa i provode u skladu s Uredbom (EU) 2021/694, osobito njezinim specifičnim ciljem 3. ***te sredstvima iz Europskog instrumenta mirovne pomoći ako se osiguravaju mjere za pomoć trećim zemljama, posebno Ukrajini i Moldovi.***

Amandman 45

Prijedlog uredbe
Članak 10. – stavak 1. – točka a

Tekst koji je predložila Komisija	*Izmjena*
(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim	(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim

sektorima u Uniji;	sektorima***, kao što su javna infrastruktura, izborna infrastruktura, promet, zdravstvo, financije, telekomunikacije, opskrba hranom i sigurnost hrane*** u ***cijeloj*** Uniji;

Amandman 46

Prijedlog uredbe
Članak 10. – stavak 1. – točka c

Tekst koji je predložila Komisija	*Izmjena*
(c) mjere uzajamne pomoći koje se sastoje od pomoći nacionalnih tijela jedne države članice drugoj državi članici, osobito kako je utvrđeno u članku 11. stavku 3. točki (f) Direktive (EU) 2022/2555.	(c) mjere uzajamne pomoći koje se sastoje od pomoći nacionalnih tijela jedne države članice drugoj državi članici, osobito kako je utvrđeno u članku 11. stavku 3. točki (f) Direktive (EU) 2022/2555 ***te u kontekstu članka 42. stavka 7. UEU-a i članka 222. UFEU-a***.

Amandman 47

Prijedlog uredbe
Članak 10. – stavak 1. – točka ca (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(ca) zamjena i postupno uklanjanje kritične opreme od visokorizičnih dobavljača, koji bi bili u suprotnosti sa sigurnosnim i obrambenim interesima Unije i njezinih država članica kako je utvrđeno u okviru ZVSP-a u skladu s glavom V. UEU-a.

Amandman 48

Prijedlog uredbe
Članak 11. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava izrađuje, u suradnji s Komisijom, ENISA-om i ***Visokim predstavnikom***, zajedničke	2. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava izrađuje, u suradnji s Komisijom, ENISA-om***, Visokim predstavnikom, ESVD-om*** i***,***

scenarije rizika i metodologije za koordinirana testiranja.	***prema potrebi, EDA-om***, zajedničke scenarije rizika i metodologije za koordinirana testiranja.

Amandman 49

Prijedlog uredbe
Članak 12. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Kibersigurnosnu pričuvu EU-a čine usluge odgovora na incidente koje pružaju pouzdani pružatelji odabrani u skladu s kriterijima iz članka 16. Pričuva obuhvaća unaprijed dogovorene usluge. Pružanje tih usluga mora biti moguće u svim državama članicama.	2. Kibersigurnosnu pričuvu EU-a čine usluge odgovora na incidente koje pružaju pouzdani pružatelji odabrani u skladu s kriterijima iz članka 16. Pričuva obuhvaća unaprijed dogovorene usluge. Pružanje tih usluga mora biti moguće u svim državama članicama ***i trećim zemljama koje zadovoljavaju primjenjive uvjete iz ove Uredbe***.

Amandman 50

Prijedlog uredbe
Članak 12. – stavak 3. – točka b

Tekst koji je predložila Komisija	*Izmjena*
(b) institucije, tijela i agencije Unije.	(b) institucije, tijela i agencije Unije***, uključujući misije ZSOP-a***.

Amandman 51

Prijedlog uredbe
Članak 12. – stavak 4.

Tekst koji je predložila Komisija	*Izmjena*
4. Korisnici iz stavka 3. točke (a) usluge iz kibersigurnosne pričuve EU-a koriste za odgovor ili potporu odgovoru na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera koji utječu na subjekte koji djeluju u kritičnim ili visokokritičnim sektorima te	4. Korisnici iz stavka 3. točke (a) usluge iz kibersigurnosne pričuve EU-a koriste za odgovor ili potporu odgovoru na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera koji utječu na subjekte koji djeluju u kritičnim ili visokokritičnim sektorima***, kao što su javna infrastruktura, izborna***

za hitan oporavak od njih.

infrastruktura, promet, zdravstvo, financije, telekomunikacije, opskrba hranom i sigurnost, te za hitan oporavak od njih.

Amandman 52

Prijedlog uredbe
Članak 12. – stavak 5.

Tekst koji je predložila Komisija	*Izmjena*
5. Komisija je općenito odgovorna za primjenu kibersigurnosne pričuve EU-a. Komisija određuje prioritete i razvoj kibersigurnosne pričuve EU-a u skladu sa zahtjevima korisnika iz stavka 3. i nadzire njezinu primjenu te se brine za komplementarnost, dosljednost, sinergije i veze s drugim mjerama potpore na temelju ove Uredbe, kao i s drugim mjerama i ***programima*** Unije.	5. Komisija je općenito odgovorna za primjenu kibersigurnosne pričuve EU-a. Komisija određuje prioritete i razvoj kibersigurnosne pričuve EU-a u skladu sa zahtjevima korisnika iz stavka 3. i nadzire njezinu primjenu te se brine za komplementarnost, dosljednost, sinergije i veze s drugim mjerama ***programima*** i ***ciljevima*** Unije***, posebno strateškim ciljem smanjenja ovisnosti o visokorizičnim dobavljačima, koji bi bili u suprotnosti sa sigurnosnim i obrambenim interesima Unije i njezinih država članica kako je utvrđeno u okviru ZSOP-a u skladu s glavom V. UEU-a***.

Amandman 53

Prijedlog uredbe
Članak 12. – stavak 7.

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

savjetuje s Visokim predstavnikom.	predstavnikom.

Amandman 54

Prijedlog uredbe
Članak 14. – stavak 2. – točka aa (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(aa) učinak incidenta na sigurnost i obranu Unije;

Amandman 55

Prijedlog uredbe
Članak 15. – stavak 3.

Tekst koji je predložila Komisija	*Izmjena*
3. Uz savjetovanje s Visokim predstavnikom, potpora u okviru mehanizma za izvanredne kibersigurnosne situacije može biti dopuna pomoći koja se pruža u kontekstu zajedničke vanjske i sigurnosne politike te zajedničke sigurnosne i obrambene politike, među ostalim putem timova za brz odgovor na kiberincidente. Također može biti dopuna ili doprinos pomoći koju jedna država članica pruža drugoj državi članici u kontekstu članka 42. stavka 7. Ugovora o Europskoj uniji.	3. Uz savjetovanje s Visokim predstavnikom, potpora u okviru mehanizma za izvanredne kibersigurnosne situacije može biti dopuna pomoći koja se pruža u kontekstu zajedničke vanjske i sigurnosne politike te zajedničke sigurnosne i obrambene politike, među ostalim putem timova za brz odgovor na kiberincidente ***radi boljeg pružanja potpore državama članicama EU-a, misijama i operacijama ZSOP-a i onim trećim zemljama koje su usklađene sa zajedničkom vanjskom i sigurnosnom politikom te zajedničkom sigurnosnom i obrambenom politikom EU-a u njihovim nastojanjima za izgradnju kapaciteta u području kiberobrane, posebno Ukrajini i Moldovi***. Također može biti dopuna ili doprinos pomoći koju jedna država članica pruža drugoj državi članici u kontekstu članka 42. stavka 7. Ugovora o Europskoj uniji.

Amandman 56

Prijedlog uredbe

Članak 16. – stavak 2. − točka ba (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(aa) pružatelj usluga dokazuje da njegove odluke i upravljačke strukture nisu ni pod kakvim neprimjerenim utjecajem vlada država koji bi bio u suprotnosti sa sigurnosnim i obrambenim interesima Unije i njezinih država članica kako je utvrđeno u okviru ZVSP-a u skladu s glavom V. UEU-a;

Amandman 57

Prijedlog uredbe
Članak 16. – stavak 2. – točka f

Tekst koji je predložila Komisija	*Izmjena*
(f) pružatelj mora biti opremljen hardverskom i softverskom tehničkom opremom koja omogućuje traženu uslugu;	(f) pružatelj mora biti opremljen hardverskom i softverskom tehničkom opremom koja omogućuje traženu uslugu ***i ispunjava zahtjeve iz članka X. Uredbe XX/XXXX (Akt o kiberotpornosti)***;

Amandman 58

Prijedlog uredbe
Članak 16. – stavak 2. − točka ja (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(ja) nijedan dobavljač koji potječe iz visokorizične treće zemlje ne smije biti dopušten;

Amandman 59

Prijedlog uredbe
Članak 16. – stavak 2. – točka jb (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(jb) pružatelj usluga blisko surađuje s relevantnim MSP-ovima, ako je to

moguće;

Amandman 60

Prijedlog uredbe
Članak 17. – stavak 1.

Tekst koji je predložila Komisija	*Izmjena*
1. Treće zemlje mogu zatražiti potporu iz kibersigurnosne pričuve EU-a ako je tako uređeno sporazumima o pridruživanju sklopljenima u pogledu njihova sudjelovanja u programu Digitalna Europa.	1. Treće zemlje mogu zatražiti potporu iz kibersigurnosne pričuve EU-a***:***
	a) ako je tako uređeno sporazumima o pridruživanju sklopljenima u pogledu njihova sudjelovanja u programu Digitalna Europa;
	b) ako je riječ o trećim zemljama u kojima je raspoređena misija ZSOP-a s posebnim mandatom za jačanje otpornosti na hibridne prijetnje, među ostalim kiberprijetnje, ili u kojima je usvojena mjera pomoći u okviru Europskog instrumenta mirovne pomoći za jačanje kiberotpornosti te zemlje.

Amandman 61

Prijedlog uredbe
Članak 17. – stavak 2.

Tekst koji je predložila Komisija	*Izmjena*
2. Potpora iz kibersigurnosne pričuve EU-a mora biti u skladu s ovom Uredbom i svim posebnim uvjetima utvrđenima u sporazumima o pridruživanju iz stavka 1.	2. Potpora iz kibersigurnosne pričuve EU-a mora biti u skladu s ovom Uredbom i svim posebnim uvjetima utvrđenima u sporazumima o pridruživanju iz stavka***,*** ***osim za one treće zemlje koje su obuhvaćene odredbama iz stavka*** 1. ***točke (b).***

Amandman 62

Prijedlog uredbe
Članak 18. – stavak 1.

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

Amandman 63

Prijedlog uredbe
Članak 18. – stavak 3.a (novi)

Tekst koji je predložila Komisija	*Izmjena*
	3.a Izvješće se dijeli s Europskim parlamentom u skladu s pravom Unije ili nacionalnim pravom o zaštiti osjetljivih klasificiranih podataka.

Amandman 64

Prijedlog uredbe
Članak 19. – stavak 1. − točka 1. − podtočka a − podtočka 1.
Uredba (EU) 2021/694
Članak 6. – stavak 1.

Tekst koji je predložila Komisija	*Izmjena*
(aa) pružanje potpore razvoju kiberštita	(aa) pružanje potpore razvoju kiberštita

EU-a, što uključuje razvoj, uvođenje i rad nacionalnih i prekograničnih platformi centara za sigurnosne operacije koje doprinose informiranosti o stanju u Uniji i jačanju kapaciteta Unije za prikupljanje podataka o kiberprijetnjama;	EU-a, što uključuje razvoj, uvođenje i rad nacionalnih i prekograničnih platformi centara za sigurnosne operacije koje doprinose informiranosti o stanju u Uniji i jačanju kapaciteta Unije za prikupljanje podataka o kiberprijetnjama ***te smanjenju ovisnosti Unije o visokorizičnim dobavljačima kritične kibersigurnosne opreme ili njezinih komponenti, što je u suprotnosti sa sigurnosnim i obrambenim interesima Unije i njezinih država članica kako je utvrđeno u okviru ZSOP-a u skladu s glavom V. UEU-a***;

Amandman 65

Prijedlog uredbe
Članak 20. – stavak 1.

Tekst koji je predložila Komisija	*Izmjena*
Komisija do ***[četiri*** godine od datuma početka primjene ove ***Uredbe]*** Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe.	Komisija do ***[tri*** godine od datuma početka primjene ove ***Uredbe i svake dvije godine nakon toga]*** Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe.

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Utvrđivanje mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
Referentni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 1.6.2023
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	AFET 1.6.2023
Izvjestitelj(ica) za mišljenje	Dragoş Tudorache

Datum imenovanja	16.6.2023
Razmatranje u odboru	18.9.2023
Datum usvajanja	24.10.2023
Rezultat konačnog glasovanja	+: 39 –: 4 0: 0
Zastupnici nazočni na konačnom glasovanju	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Zamjenici nazočni na konačnom glasovanju	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Korišteni znakovi:
+ : za
- : protiv
0 : suzdržani

25.10.2023

MIŠLJENJE ODBORA ZA PROMET I TURIZAM

upućeno Odboru za industriju, istraživanje i energetiku

o Prijedlogu uredbe Europskog parlamenta i Vijeća o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Izvjestitelj za mišljenje: Gheorghe Falcă

KRATKO OBRAZLOŽENJE

Organizacije pogođene kibernapadima, među ostalim u prometnom sektoru, rijetko ih prijavljuju, posebno kada je riječ o poduzećima iz privatnog sektora, jer ih obično smatraju „lošim publicitetom”. Većina organizacija napade radije rješava interno, dok ih napadači često iznose u javnost. Dobra je vijest za EU da će se stupanjem na snagu Direktive 2022/2555 o sigurnosti mreže (poznate kao „Direktiva NIS 2”), koju države članice moraju prenijeti u svoja zakonodavstva do listopada 2024., uskladiti obveze prijavljivanja incidenata u svim državama članicama. Stoga će se u narednim godinama vjerojatno bolje razumjeti priroda i razmjer tog problema.

Agencija Europske unije za kibersigurnost (ENISA) nedavno je objavila izvješće[1] koje sadržava informacije o kibersigurnosnim prijetnjama u prometnom sektoru i u kojem se naglašava da su kiberkriminalci odgovorni za više od polovine incidenata zabilježenih u izvještajnom razdoblju 2022. (55 %) te da su ti napadi većinom bili motivirani financijskom dobiti. Također se napominje da je većina kibernapada u prometnom sektoru usmjerena na IT sustave i da uzrokuje prekide u radu.

Kad je riječ o pripravnosti i odgovoru na kibersigurnosne incidente, potpora na razini Unije i solidarnost među državama članicama trenutno su ograničene. U zaključcima Vijeća iz svibnja 2022. istaknuta je potreba za uklanjanjem tih nedostataka i Komisija je pozvana da predstavi prijedlog o novom **Fondu za odgovor na hitne situacije u području kibersigurnosti**[2].

Predmetnom uredbom provodi se **Strategija EU-a za kibersigurnost** donesena u prosincu 2020. u kojoj je najavljena uspostava **europskog kiberštita**, kojim bi se ojačali kapaciteti za otkrivanje kiberprijetnji i razmjenu informacija u Europskoj uniji putem saveza nacionalnih i prekograničnih centara za sigurnosne operacije (SOC-ovi). Mjere iz te uredbe podupirat će se **financiranjem u okviru strateškog cilja „Kibersigurnost” programa Digitalna Europa.**

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

Jedan dio od tih dodatnih 100 milijuna EUR iskoristit će se za povećanje proračuna kojim upravlja Europski stručni centar u području kibersigurnosti kako bi se provele mjere za SOC-ove i pripravnost u okviru njihovih programa rada. Nadalje, dodatna sredstva poslužit će za potporu uspostavi kibersigurnosne pričuve EU-a. Njima se dopunjuje proračun koji je već predviđen za slična djelovanja u glavnom programu Digitalna Europa i programu rada u

[1] „Understanding Cyber Threats in Transport” (Razumijevanje kiberprijetnji u prometu), ENISA, objavljeno 21. ožujka 2023.
[2] Zaključci Vijeća o razvoju položaja Europske unije u pogledu kiberprostora od 23. svibnja 2022., (9364/22).

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

Stajalište izvjestitelja

Izvjestitelj pozdravlja novi prijedlog i smatra da će on donijeti znatne koristi raznim dionicima. Izvjestitelj naglašava da je potrebno bolje razumjeti potrebe i zahtjeve u pogledu kibersigurnosti u prometu, kao i osigurati da ključni subjekti u području prometa imaju pristup odgovarajućim financijskim sredstvima za pripravnost, djelovanje i rješavanje incidenata.

Izvjestitelj podržava „skup alata za kibersigurnost u prometu" kojim se nastoji doprinijeti većoj razini osviještenosti o kibersigurnosti i kiberhigijeni, posebno u području prometnog sektora. Namijenjen je organizacijama u prometnom sektoru, bez obzira na njihovu veličinu i područje djelovanja, i njime se također uzimaju u obzir ključna prometna infrastruktura i vojna mobilnost, posebno s obzirom na rat u Ukrajini, te je posebno, ali ne i isključivo, usmjeren na:

- zračne prijevoznike, upravljačka tijela zračnih luka, osnovne zračne luke, centre upravljanja zračnim prometom i kontrole zračnog prometa, Agenciju Europske unije za sigurnost zračnog prometa i Eurocontrol;
- upravitelje infrastrukture, željezničke prijevoznike i Europski sustav za upravljanje željezničkim prometom (ERTMS);
- kompanije za prijevoz putnika i tereta unutarnjim plovnim putovima, morem i duž obale, upravljačka tijela luka, uključujući njihove lučke objekte, subjekte koji upravljaju poslovima i opremom u lukama, operatore službe za nadzor i upravljanje prometovanjem plovila;
- tijela nadležna za ceste odgovorna za kontrolu upravljanja prometom, operatore inteligentnih prometnih sustava;
- poštanske i kurirske usluge.

Izvjestitelj smatra da će iznos proračuna za funkcioniranje **Fonda za odgovor na hitne situacije u području kibersigurnosti** (ERFC) odrediti njegovu uspješnost; stoga bi on trebao biti dovoljno velik kako bi se državama članicama pomoglo u **pripremi** za značajne kibersigurnosne incidente i kibersigurnosne incidente velikih razmjera, **odgovoru na njih i hitnom oporavku od njih**. Potpora za odgovor na incidente stavlja se na raspolaganje i institucijama, tijelima, uredima i agencijama Unije.

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

AMANDMANI

Odbor za promet i turizam poziva Odbor za industriju, istraživanje i energetiku da kao nadležni odbor uzme u obzir sljedeće:

Amandman 1

Prijedlog uredbe
Uvodna izjava 2.

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

mnogim zemljama ili se brzo šire na mnoge zemlje.

Amandman 2

Prijedlog uredbe
Uvodna izjava 2.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(2a) Sve ozbiljniju kibersigurnosnu prijetnju prometnom sektoru predstavljaju akteri pod pokroviteljstvom države, kiberkriminalci i haktivisti kojima su mete nadležna tijela, operatori, proizvođači, dobavljači i pružatelji usluga u zračnom, pomorskom, željezničkom i cestovnom prometu. Agencija Europske unije za kibersigurnost (ENISA) zabilježila je 2022. povećanje prosječnog mjesečnog broja prijavljenih incidenata koji utječu na prometni sektor za 25 % u odnosu na razine iz 2021. Većina napada na prometni sektor usmjerena je na sustave informacijske tehnologije (IT), a oni mogu uzrokovati prekide u radu[14a].
	[14b] ENISA (2023.), Izvješće ENISA-e o prijetnjama: Prometni sektor, stranice 7. i 17.

Amandman 3

Prijedlog uredbe
Uvodna izjava 2.b (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(2b) Ničim izazvana ruska invazija na Ukrajinu dovela je do znatnog povećanja kibersigurnosnih incidenata, uključujući distribuirane kibernapade uskraćivanjem usluga (DDoS), usmjerene na prometni sektor u EU-u i područjima u blizini EU-a, uglavnom zračne luke, željeznice i tijela nadležna za promet[14b]. Vrlo je vjerojatno

da će se taj porast napada nastaviti.

[14b] ENISA (2023.), Izvješće ENISA-e o prijetnjama: Prometni sektor, stranica 9.

Amandman 4

Prijedlog uredbe
Uvodna izjava 2.c (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(2c) Kibernapadi su usmjereni na tijela vlasti i tijela u svim prometnim podsektorima, pri čemu su pogođeni željeznički prijevoznici i upravitelji infrastrukture, kao i lučka poduzeća. Kad je riječ o cestovnom sektoru, ciljani su bili proizvođači originalne opreme, dobavljači i pružatelji usluga, kao i javni prijevoznici. U zrakoplovnom sektoru glavni su ciljevi bili zračni prijevoznici i upravitelji zračnih luka, a slijede ih pružatelji usluga, operateri površinskog prijevoza i lanac opskrbe[14c].

[14c] ENISA (2023.), Izvješće ENISA-e o prijetnjama: Prometni sektor, stranica 17.

Amandman 5

Prijedlog uredbe
Uvodna izjava 3.

Tekst koji je predložila Komisija	*Izmjena*
(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe[16] , potrebno je povećati	(3) Neophodno je ojačati konkurentni položaj industrije i uslužnih sektora u Uniji u cijelom digitaliziranom gospodarstvu i poduprijeti njihovu digitalnu transformaciju povećanjem razine kibersigurnosti na jedinstvenom digitalnom tržištu. Kako je preporučeno u trima različitim prijedlozima Konferencije o budućnosti Europe[16] , potrebno je povećati

otpornost građana, poduzeća i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoć u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibersigurnosnim prijetnjama i incidentima.	otpornost građana, poduzeća***, prijevoznika*** i subjekata koji upravljaju kritičnim infrastrukturama na sve veće kibersigurnosne prijetnje koje mogu imati razorne društvene i gospodarske posljedice. Stoga su potrebna ulaganja u infrastrukturu i usluge kojima će se omogućiti brže otkrivanje kibersigurnosnih prijetnji i incidenata i odgovor na njih, a državama članicama potrebna je pomoć u boljoj pripremi za značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera i odgovoru na njih. Unija bi isto tako trebala povećati svoje kapacitete u tim područjima, posebno u pogledu prikupljanja i analize podataka o kibersigurnosnim prijetnjama i incidentima ***te o stanju i razvoju tržišta rada u području kibersigurnosti jer ima ključnu ulogu u pružanju potrebnih usluga otkrivanja i odgovora***.
[16] https://futureu.europa.eu/hr/	[16] https://futureu.europa.eu/hr/

Amandman 6

Prijedlog uredbe
Uvodna izjava 4.

Tekst koji je predložila Komisija	*Izmjena*
(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća[17], Preporuku Komisije (EU) 2017/1584[18] , Direktivu 2013/40/EU Europskog parlamenta i Vijeća[19] i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[20] . Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i	(4) Unija je već poduzela niz mjera za smanjenje ranjivosti i povećanje otpornosti kritičnih infrastruktura i subjekata u pogledu kibersigurnosnih rizika, koje posebice uključuju Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća[17] , Preporuku Komisije (EU) 2017/1584[18] , Direktivu 2013/40/EU Europskog parlamenta i Vijeća[19] i Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća[20], ***kao i Prijedlog uredbe o smjernicama za razvoj transeuropske prometne mreže te Prijedlog uredbe o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima (Akt o kiberotpornosti)***.

koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

Naposljetku, u Preporuci Vijeća o koordiniranom pristupu na razini Unije radi jačanja otpornosti kritične infrastrukture države članice se pozivaju da poduzmu hitne i učinkovite mjere te da surađuju lojalno, učinkovito, solidarno i koordinirano međusobno, s Komisijom i drugim relevantnim javnim tijelima te predmetnim subjektima kako bi se povećala otpornost kritične infrastrukture koja se koristi za pružanje osnovnih usluga na unutarnjem tržištu.

---

[17] 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.).

[18] 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.).

[19] 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.).

[20] 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.).

[17] 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.).

[18] 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.).

[19] 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.).

[20] 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.).

Amandman 7

Prijedlog uredbe
Uvodna izjava 4.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(4a) Iako pozdravlja skup alata Europske komisije za kibersigurnost u prometu[2a], koji sadržava osnovne informacije o prijetnjama koje mogu utjecati na prometne organizacije (širenje zlonamjernog softvera, uskraćivanje usluge, neovlašten pristup i krađa te manipulacija softverom) i u kojem se navode dobre prakse ublažavanja, prijevoznici bi trebali dobiti odgovarajuće osposobljavanje o kibersigurnosti i odgovarajuće alate za sprečavanje kiberprijetnji. Proračun Unije trebao bi pokrivati i potporu, kao što je osposobljavanje, koju pruža ENISA kako bi se prijevoznicima omogućila učinkovita provedba najboljih praksi ublažavanja uključenih u taj skup alata.
	[1a] Izvješće ENISA-e o prijetnjama: prometni sektor/ENISA, ožujak 2023.
	[2a] Europska komisija (2021.). Skup alata za kibersigurnost u prometu, dostupan na https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_hr

Amandman 8

Prijedlog uredbe
Uvodna izjava 4.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(4a) Koordinirani pristup na razini Unije za jačanje pripravnosti i otpornosti kritične infrastrukture, kao što je prometna infrastruktura, temelji se na izgradnji kapaciteta država članica. Kako je potvrđeno u nedavnoj komunikaciji Komisije Europskom parlamentu i Vijeću naslovljenoj „Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije”[19a], sigurnost EU-a nije moguće

zajamčiti bez sudjelovanja njezina najvrednijeg kapitala: njezinih stanovnika.

[19a] Komunikacija Komisije Europskom parlamentu i Vijeću: Povećanjem broja stručnjaka za kibersigurnost do veće konkurentnosti, rasta i otpornosti Unije („Akademija za vještine u području kibersigurnosti”) COM(2023) 207 final

Amandman 9

Prijedlog uredbe
Uvodna izjava 12.

Tekst koji je predložila Komisija	*Izmjena*
(12) Kako bi se učinkovitije spriječile i procijenile kiberprijetnje i kiberincidenti te na njih odgovorilo, potrebno je steći sveobuhvatnije znanje o prijetnjama ključnim resursima i infrastrukturi na području Unije, uključujući njihovu geografsku raspoređenost, međusobnu povezanost i potencijalne posljedice u slučaju kibernapada koji pogađaju te infrastrukture. Trebalo bi uvesti opsežnu infrastrukturu EU-a za SOC-ove („europski kiberštit”), koja se sastoji od nekoliko interoperabilnih prekograničnih platformi, od kojih svaka okuplja nekoliko nacionalnih SOC-ova. Ta bi infrastruktura trebala služiti kibersigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijom tehnologijom za napredne alate za prikupljanje i analizu podataka, jačajući kapacitete otkrivanja i upravljanja kibertehnologijama i osiguravajući informiranost o stanju u stvarnom vremenu. Ta bi infrastruktura trebala služiti za bolje otkrivanje kibersigurnosnih prijetnji i incidenata te na taj način dopunjavati i podržavati subjekte i mreže Unije odgovorne za upravljanje krizama u Uniji, posebno Europsku mrežu	(12) Kako bi se učinkovitije spriječile i procijenile kiberprijetnje i kiberincidenti te na njih odgovorilo, potrebno je steći sveobuhvatnije znanje o prijetnjama ključnim resursima i infrastrukturi na području Unije, uključujući njihovu geografsku raspoređenost, međusobnu povezanost i potencijalne posljedice u slučaju kibernapada koji pogađaju te infrastrukture. ***Ti kritični resursi i infrastrukture uključuju inteligentne prometne sustave, koji, iako su ključni za automatiziranu i multimodalnu mobilnost, djeluju na temelju ključnih razmjena osjetljivih podataka.*** Trebalo bi uvesti opsežnu infrastrukturu EU-a za SOC-ove („europski kiberštit”), koja se sastoji od nekoliko interoperabilnih prekograničnih platformi, od kojih svaka okuplja nekoliko nacionalnih SOC-ova. Ta bi infrastruktura trebala služiti kibersigurnosnim interesima i potrebama na nacionalnoj razini i razini Unije, koristeći se najsuvremenijom tehnologijom za napredne alate za prikupljanje i analizu podataka, jačajući kapacitete otkrivanja i upravljanja kibertehnologijama i osiguravajući informiranost o stanju u stvarnom vremenu. Ta bi infrastruktura

organizacija za vezu za kiberkrize („EU-CyCLONe”), kako je definirana u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća[24].

trebala služiti za bolje otkrivanje kibersigurnosnih prijetnji i incidenata te na taj način dopunjavati i podržavati subjekte i mreže Unije odgovorne za upravljanje krizama u Uniji, posebno Europsku mrežu organizacija za vezu za kiberkrize („EU-CyCLONe”), kako je definirana u Direktivi (EU) 2022/2555 Europskog parlamenta i Vijeća[24].

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

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

Amandman 10

Prijedlog uredbe
Uvodna izjava 14.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(14a) Prometni sektor sve više postaje jedno od najunosnijih područja poslovanja za kiberkriminalce, pri čemu se podaci o kupcima smatraju vrlo vrijednom robom, a sve se više cilja na lanac opskrbe u prijevozu. Zbog toga bi se prometna infrastruktura koju karakterizira prekogranična priroda ili razmjena podataka bežičnim tehnologijama trebala smatrati ključnim predmetom analize i praćenja za nacionalne, a posebno za prekogranične SOC-ove. Na primjer, nedavni prijedlog revizije Uredbe o mreži TEN-T zahtijeva veću solidarnost i suradnju u razmjeni informacija o prekograničnim kiberprijetnjama s kojima bi se ta transnacionalna mreža mogla suočiti. Isto tako, inteligentni prometni sustavi (ITS) ključni su za sigurniji, učinkovitiji i održiviji promet, ali zbog njih su prometni

	sustavi osjetljiviji na kibernapade koji mogu prouzročiti nesreće, prometne gužve ili uzrokovati gospodarske gubitke i privatnim i javnim subjektima. Kako bi se osigurala sigurnost putnika te zaštita podataka korisnika i pružatelja usluga i izbjegla financijska šteta, ključno je da program provedbe revidirane direktive o inteligentnim prometnim sustavima sadržava odredbe i alate za jačanje suradnje među državama članicama u otkrivanju kibersigurnosnih prijetnji i incidenata te pripremi za njih i odgovaranju na njih.

Amandman 11

Prijedlog uredbe
Uvodna izjava 15.

Tekst koji je predložila Komisija	*Izmjena*
(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsuvremenijim alatima te doprinosili razvoju sposobnosti i tehnološke suverenosti Unije.	(15) Na nacionalnoj razini praćenje, otkrivanje i analizu kiberprijetnji obično osiguravaju SOC-ovi javnih i privatnih subjekata, u kombinaciji sa CSIRT-ovima. Osim toga, CSIRT-ovi razmjenjuju informacije u kontekstu mreže CSIRT-ova, u skladu s Direktivom (EU) 2022/2555. Prekogranični SOC-ovi trebali bi predstavljati nove kapacitete koji su komplementarni mreži CSIRT-ova jer bi objedinjavali i dijelili podatke o kibersigurnosnim prijetnjama dobivene od javnih i privatnih subjekata, povećavali vrijednost takvih podataka stručnom analizom i zajednički nabavljenom infrastrukturom i najsuvremenijim alatima te doprinosili razvoju sposobnosti i tehnološke suverenosti Unije. ***U tom pogledu, kako bi se ojačala autonomija Unije u području kibersigurnosti i s obzirom na članak 47. stavak 4. Prijedloga uredbe o smjernicama za razvoj transeuropske prometne mreže (COM(2021)0812), potrebno je i spriječiti pristup podacima koji dovode do kiberprijetnji provedbom čvrstog***

regulatornog okvira kojim se uređuju strano vlasništvo i ulaganja u kritičnu infrastrukturu, kao što je promet.

Amandman 12

Prijedlog uredbe
Uvodna izjava 21.

Tekst koji je predložila Komisija	*Izmjena*
(21) Iako je europski kiberštit civilni projekt, zajednica za kiberobranu mogla bi imati koristi od bolje sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture. Prekogranični SOC-ovi, uz potporu Komisije i Europskog stručnog centra u području kibersigurnosti (ECCC) te u suradnji s Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”), trebali bi postupno razvijati namjenske protokole i standarde kako bi se omogućila suradnja sa zajednicom za kiberobranu, uključujući uvjete provjere i sigurnosti. Razvoj europskog kiberštita trebao bi biti popraćen razmatranjem načina na koji bi se omogućila buduća suradnja s mrežama i platformama odgovornima za dijeljenje informacija u zajednici za kiberobranu, u bliskoj suradnji s Visokim predstavnikom.	(21) Iako je europski kiberštit civilni projekt, zajednica za kiberobranu mogla bi imati koristi od bolje sposobnosti za civilno otkrivanje i informiranost o stanju koji su razvijeni za zaštitu kritične infrastrukture. Prekogranični SOC-ovi, uz potporu Komisije i Europskog stručnog centra u području kibersigurnosti (ECCC) te u suradnji s Visokim predstavnikom Unije za vanjske poslove i sigurnosnu politiku („Visoki predstavnik”), trebali bi postupno razvijati namjenske protokole i standarde kako bi se omogućila suradnja sa zajednicom za kiberobranu, uključujući uvjete provjere i sigurnosti. Razvoj europskog kiberštita trebao bi biti popraćen razmatranjem načina na koji bi se omogućila buduća suradnja s mrežama i platformama odgovornima za dijeljenje informacija u zajednici za kiberobranu, u bliskoj suradnji s Visokim predstavnikom. ***Njime bi se također trebale omogućiti sinergije s Akcijskim planom za vojnu mobilnost 2.0. Funkcionalna mreža vojne mobilnosti mora biti otporna, među ostalim u okolnostima kiberprijetnji i drugih hibridnih prijetnji koje bi mogle utjecati na ključna čvorišta u prometnom sustavu s dvojnom namjenom. Na primjer, kibernapad na sustave koji se upotrebljavaju u zračnim lukama, lukama ili željeznicama ili kibernapad na vojna sredstva mogao bi imati znatne posljedice. Stoga će digitalizacija procesa i postupaka, među ostalim za potrebnu civilnu i vojnu suradnju, zahtijevati jačanje računalnih informacijskih sustava***

za borbu protiv kiberprijetnji.

Amandman 13

Prijedlog uredbe
Uvodna izjava 21.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(21a) U slučaju kibersigurnosne krize učinkovita razmjena informacija ključna je za osiguravanje informiranosti o stanju u vojnom i civilnom prometnom sektoru. Tom razmjenom informacija trebala bi se poticati i suradnja između relevantnih sektorskih tijela odgovornih za promet, nadležnih tijela za kibersigurnost, SOC-ova i CSIRT-ova.

Amandman 14

Prijedlog uredbe
Uvodna izjava 29.

Tekst koji je predložila Komisija	*Izmjena*
(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti”). Koordinirane vježbe testiranja trebale bi se temeljiti na	(29) U okviru mjera pripravnosti, radi promicanja dosljednog pristupa i jačanja sigurnosti u cijeloj Uniji i na njezinu unutarnjem tržištu, trebalo bi pružiti potporu koordiniranom testiranju i procjeni kibersigurnosti subjekata koji djeluju u visokokritičnim sektorima utvrđenima u skladu s Direktivom (EU) 2022/2555. U tu bi svrhu Komisija, uz potporu ENISA-e i u suradnji sa Skupinom za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovanom Direktivom (EU) 2022/2555, trebala redovito utvrđivati relevantne sektore ili podsektore koji bi trebali biti prihvatljivi za primanje financijske potpore za koordinirano testiranje na razini Unije. Sektore ili podsektore trebalo bi odabrati iz Priloga I. Direktivi (EU) 2022/2555 („Sektori visoke kritičnosti”). ***Posebnu pozornost trebalo bi posvetiti prometnom***

zajedničkim scenarijima i metodama procjene rizika. Pri odabiru sektora i razvoju scenarija rizika trebalo bi uzeti u obzir relevantne procjene rizika i scenarije rizika na razini Unije, uključujući potrebu za izbjegavanjem njihova udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje trebaju provesti Komisija, Visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za elektroničke komunikacije (BEREC), koordinirane procjene rizika koje treba provesti na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća[29] . Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

sektoru i njegovim podsektorima (zračnom, željezničkom, vodnom i cestovnom) jer uključuju kritičnu infrastrukturu u kojoj bi kiberincidenti i kibernapadi mogli ozbiljno ugroziti sigurnost putnika i prijevoznika.
Koordinirane vježbe testiranja trebale bi se temeljiti na zajedničkim scenarijima i metodama procjene rizika. Pri odabiru sektora i razvoju scenarija rizika trebalo bi uzeti u obzir relevantne procjene rizika i scenarije rizika na razini Unije, uključujući potrebu za izbjegavanjem njihova udvostručavanja, kao što su procjena rizika i scenariji rizika zatraženi u Zaključcima Vijeća o razvoju položaja Europske unije u pogledu kiberprostora koje trebaju provesti Komisija, Visoki predstavnik i Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, u koordinaciji s relevantnim civilnim i vojnim tijelima i agencijama te uspostavljenim mrežama, uključujući mrežu EU-CyCLONe, procjena rizika komunikacijskih mreža i infrastruktura koju je zatražila Zajednička ministarska skupina u Neversu i koju je provela Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava, uz potporu Komisije i ENISA-e te u suradnji s Tijelom europskih regulatora za elektroničke komunikacije (BEREC), koordinirane procjene rizika koje treba provesti na temelju članka 22. Direktive (EU) 2022/2555 i testiranje digitalne operativne otpornosti predviđeno Uredbom (EU) 2022/2554 Europskog parlamenta i Vijeća[29] . Pri odabiru sektora trebalo bi uzeti u obzir i Preporuku Vijeća o koordiniranom pristupu na razini Unije za jačanje otpornosti kritične infrastrukture.

[29] 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

[29] 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.	(EU) 2016/1011.

Amandman 15

Prijedlog uredbe
Uvodna izjava 30.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(30a) S obzirom na kritičnost sektora i posljedice kiberprijetnji na mobilnost, a time i na živote putnika i pješaka, prometni sektor trebao bi imati prioritet u pogledu koordiniranog testiranja pripravnosti subjekata.

Amandman 16

Prijedlog uredbe
Uvodna izjava 35.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(35a) S obzirom na povećane zadaće i odgovornosti koje su ENISA-i dodijeljene ovim prijedlogom i prijedlogom Akta o kiberotpornosti, potrebno je donijeti izmjenu proračuna 1/2022 ENISA-e za pilot-provedbu potpornog djelovanja u području kibersigurnosti. Nadalje, s obzirom na relevantne interese Unije, ENISA-i bi trebalo dodijeliti dodatne financijske i ljudske resurse.

Amandman 17

Prijedlog uredbe
Uvodna izjava 38.a (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(38a) Stoga bi razvoj vještina i kompetencija trebao biti u središtu pozornosti u svim sektorima, posebno onima koji su osjetljivi na kibersigurnosne prijetnje, kao što je

	osoblje koje radi na infrastrukturama masovnog tranzita ili kritičnim infrastrukturama, uključujući sustave kontrole vlakova i digitalne alate za planiranje prometa za sve vrste prijevoza. Uvođenje i daljnji razvoj kulture kibersigurnosti stoga su ključni za uspjeh provedbe ove Uredbe, kako u smislu osviještenosti građana tako i u smislu stručnog znanja u svim sektorima kritične infrastrukture.

Amandman 18

Prijedlog uredbe
Članak 1. – stavak 2. – točka a

Tekst koji je predložila Komisija	*Izmjena*
(a) poboljšanje zajedničkog otkrivanja kiberprijetnji i kiberincidenata te zajedničke informiranosti o njihovu stanju u Uniji da bi se omogućilo učvršćivanje konkurentnog položaja industrijskog i uslužnog sektora u Uniji u cijelom digitalnom gospodarstvu te doprinijelo tehnološkom suverenitetu Unije u području kibersigurnosti;	(a) poboljšanje zajedničkog otkrivanja kiberprijetnji i kiberincidenata te zajedničke informiranosti o njihovu stanju u Uniji da bi se omogućilo učvršćivanje konkurentnog položaja industrijskog sektora***, sektora prometne infrastrukture*** i uslužnog sektora u Uniji u cijelom digitalnom gospodarstvu te doprinijelo tehnološkom suverenitetu Unije u području kibersigurnosti;

Amandman 19

Prijedlog uredbe
Članak 1. – stavak 2. – točka b

Tekst koji je predložila Komisija	*Izmjena*
(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera, među ostalim stavljanjem potpore Unije za odgovor na kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu	(b) podizanje pripravnosti subjekata koji djeluju u kritičnim i visokokritičnim sektorima u Uniji i jačanje solidarnosti razvojem zajedničkih kapaciteta za odgovor na značajne kibersigurnosne incidente ili kibersigurnosne incidente velikih razmjera***, uz posvećivanje posebne pozornosti kritičnoj IT i fizičkoj infrastrukturi,*** među ostalim stavljanjem potpore Unije za odgovor na

Digitalna Europa („DEP”);	kibersigurnosne incidente na raspolaganje trećim zemljama pridruženima programu Digitalna Europa („DEP”);

Amandman 20

Prijedlog uredbe
Članak 1. – stavak 2. – točka ca (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(ca) jačanje pripravnosti, suradnje i učinkovitosti Unije u zaštiti prometne infrastrukture i usluga u državama članicama od kiberincidenata kako bi se osigurali kontinuirano funkcioniranje prometnog sektora, integritet lanaca opskrbe i mobilnost diljem Unije.

Amandman 21

Prijedlog uredbe
Članak 3. – stavak 2. − podstavak 1. − točka c

Tekst koji je predložila Komisija	*Izmjena*
(c) doprinosi boljoj zaštiti i odgovoru na kiberprijetnje***;***	(c) doprinosi boljoj zaštiti i odgovoru na kiberprijetnje***, među ostalim za prometnu infrastrukturu prekogranične prirode, kao što je mreža TEN-T, ili prometnu infrastrukturu kojoj je svojstvena razmjena podataka bežičnim tehnologijama, kao što su inteligentni prometni sustavi.***

Amandman 22

Prijedlog uredbe
Članak 3. – stavak 2. – podstavak 2.

Tekst koji je predložila Komisija	*Izmjena*
Razvija se u suradnji s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom na temelju Uredbe (EU) 2021/1173.	Razvija se u suradnji s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom na temelju Uredbe (EU) 2021/1173. ***Njime se putem***

	posebnih protokola i standarda omogućuje suradnja sa zajednicom za kiberobranu kako bi se osigurao razvoj snažnijih sposobnosti civilnog otkrivanja i informiranosti o stanju za zaštitu kritične infrastrukture. U tom pogledu razvijaju se sinergije i s Akcijskim planom za vojnu mobilnost 2.0 te se osigurava učinkovita razmjena informacija kako bi se pružila informiranost o stanju u vojnom i civilnom prometnom sektoru.

Amandman 23

Prijedlog uredbe
Članak 8. – stavak 2.a (novi)

Tekst koji je predložila Komisija	*Izmjena*
	2.a Komisija uključuje europski kiberštit, a posebno prekogranične SOC-ove, u svoje mišljenje upućeno državama članicama u okviru Prijedloga uredbe o transeuropskoj prometnoj mreži (COM(2021)0812) kad god bi sudjelovanje ili doprinos bilo koje vrste fizičke osobe iz treće zemlje ili poduzeća iz treće zemlje mogli utjecati na kibersigurnost prekogranične kritične infrastrukture, kao što je TEN-T.

Amandman 24

Prijedlog uredbe
Članak 10. – stavak 1. – točka a

Tekst koji je predložila Komisija	*Izmjena*
(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim sektorima u Uniji;	(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim sektorima u Uniji***, s posebnim naglaskom na prometnoj infrastrukturi i njezinim podsektorima iz Priloga I. Direktivi (EU) 2022/255***;

Amandman 25

Prijedlog uredbe
Članak 18. – stavak 2.

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

Amandman 26

Prijedlog uredbe
Članak 19. – stavak 1. − točka 1. − podtočka b
Uredba (EU) 2021/694
Članak 6. – stavak 2.a (novi)

Tekst koji je predložila Komisija	*Izmjena*
	2.a S obzirom na relevantne interese Unije, u vezi s odgovornostima ENISA-e za pripremu prijedloga programa certifikacije u skladu s Uredbom (EU) 2019/881, njezinim odgovornostima za preispitivanje i procjenu kiberprijetnji i ranjivosti te njihovo ublažavanje, pripremu izvješća o istraživanju incidenata za mehanizam za istraživanje kibersigurnosnih incidenata, kao i za pružanje osposobljavanja operatora kritične infrastrukture protiv kibernapada i incidenata te s obzirom na odgovornosti koje su joj nedavno dodijeljene u okviru

Prijedloga akta o kiberotpornosti, ENISA-i se u skladu s primjenjivim zakonodavstvom osiguravaju potrebna sredstva iz proračuna Unije.

Amandman 27

Prijedlog uredbe
Članak 19. – stavak 1. – točka 1.a (nova)
Uredba (EU) 2021/694
Članak 7. – stavak 1. – točka ca (nova)

Tekst koji je predložila Komisija	*Izmjena*
	(1a) članak 7. mijenja se kako slijedi:
	(a) stavak 1. mijenja se kako slijedi:
	(1) umeće se sljedeća točka (ca):
	(ca) podupiranje visokokvalitetnog osposobljavanja prijevoznika te upravitelja i radne snage u području kritične infrastrukture u sektoru prometa, među ostalim u cilju učinkovite razmjene i provedbe praksi ublažavanja u slučaju kibernapada ili incidenta u području kritične infrastrukture, kao što su one koje pruža skup alata za kibersigurnost u prometu.

POSTUPAK U ODBORU KOJI DAJE MIŠLJENJE

Naslov	Utvrđivanje mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih
Referentni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 1.6.2023
Odbori koji su dali mišljenje Datum objave na plenarnoj sjednici	TRAN 1.6.2023
Izvjestitelj(ica) za mišljenje Datum imenovanja	Gheorghe Falcă 7.7.2023
Datum usvajanja	25.10.2023

Rezultat konačnog glasovanja	+: 38 –: 0 0: 0
Zastupnici nazočni na konačnom glasovanju	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Zamjenici nazočni na konačnom glasovanju	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Korišteni znakovi:
+ : za
- : protiv
0 : suzdržani

POSTUPAK U NADLEŽNOM ODBORU

Naslov	Utvrđivanje mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibersigurnosnih prijetnji i incidenata, pripremu za njih i odgovor na njih			
Referentni dokumenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Datum podnošenja EP-u	19.4.2023			
Nadležni odbor Datum objave na plenarnoj sjednici	ITRE 1.6.2023			
Odbori koji daju mišljenje Datum objave na plenarnoj sjednici	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Odbori koji nisu dali mišljenje Datum odluke	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Izvjestitelji Datum imenovanja	Lina Gálvez Muñoz 2.5.2023			
Razmatranje u odboru	19.9.2023			
Datum usvajanja	7.12.2023			
Rezultat konačnog glasovanja	+: –: 0:	43 10 1		
Zastupnici nazočni na konačnom glasovanju	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Zamjenici nazočni na konačnom glasovanju	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Zamjenici nazočni na konačnom glasovanju prema čl. 209. st. 7.	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Datum podnošenja	8.12.2023			

POIMENIČNO KONAČNO GLASOVANJE U ODBORU KOJI DAJE MIŠLJENJE

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Korišteni znakovi:
+ : za
- : protiv
0 : suzdržani