Europski parlament
2019-2024

Odbor za vanjske poslove

2023/0109(COD)

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

PA_Legam

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 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,	(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. ***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

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.	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 kibersigurnosnim prijetnjama i incidentima.	(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***, 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	*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 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.	(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	(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.	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 unije (UFEU).	(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 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	(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.	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 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-	(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 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

ovima) i drugim relevantnim akterima te ih nadopunjuju.	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	(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.

(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 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	(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.

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 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.	(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***, 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) 2022/2555.

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	(20) Prikupljanjem, dijeljenjem i razmjenom podataka europski kiberštit trebao bi povećati tehnološku suverenost***, stratešku autonomiju, konkurentnost i otpornost*** Unije. Objedinjavanje visokokvalitetnih prilagođenih podataka

inteligencije i analitike podataka. To bi trebalo omogućiti povezivanjem europskog kiberštita s paneuropskom infrastrukturom računalstva visokih performansi uspostavljenom Uredbom Vijeća (EU) 2021/1173[25].

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 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	(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[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

trećim zemljama.

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 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	(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.

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 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	(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. ***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***

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.

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 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.

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 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.	(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***, 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 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.	(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***, 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	(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.

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 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.	(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. ***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

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.	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	(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

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.

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 Digitalna Europa („DEP”);	(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”) ***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 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.	Mora moći služiti drugim javnim i privatnim ***te, prema potrebi, vojnim*** organizacijama na nacionalnoj razini kao referentna i pristupna točka za prikupljanje i analiziranje informacija o kibersigurnosnim prijetnjama i incidentima te doprinos prekograničnom SOC-u. Mora biti opremljen najsuvremenijim tehnologijama za otkrivanje, agregiranje i analiziranje podataka relevantnih za kibersigurnosne prijetnje i incidente.

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 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. 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***, 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	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.	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 sektorima u Uniji;	(a) mjere pripravnosti, uključujući koordinirano testiranje pripravnosti subjekata koji djeluju u visokokritičnim 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.	(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.	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 scenarije rizika i metodologije za koordinirana testiranja.	2. Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava izrađuje, u suradnji s Komisijom, ENISA-om***, Visokim predstavnikom, ESVD-om*** i***, 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	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.	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 za hitan oporavak od njih.	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 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	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.	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***,*** ***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 savjetuje s Visokim predstavnikom.	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 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	1. Treće zemlje mogu zatražiti potporu iz kibersigurnosne pričuve EU-a***:***

njihova sudjelovanja u programu Digitalna Europa.

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	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.	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 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;	(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 ***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 Datum imenovanja	Dragoş Tudorache 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