Parlamentul European
2019-2024

Comisia pentru afaceri externe

2023/0109(COD)

27.10.2023

AVIZ

al Comisiei pentru afaceri externe

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de regulament al Parlamentului European și al Consiliului de stabilire a unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor
(COM(2023)0209) – C9-0136/2023 – 2023/0109(COD))

Raportor pentru aviz: Dragoş Tudorache

PA_Legam

Amendamentul 1

Propunere de regulament
Considerentul 1

Textul propus de Comisie	*Amendamentul*
(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale în toate sectoarele de activitate economică, întrucât administrațiile publice, întreprinderile și cetățenii sunt astăzi mai interconectați și mai interdependenți decât oricând, între sectoare și dincolo de frontiere.	(1) Utilizarea tehnologiilor informației și comunicațiilor și dependența de aceste tehnologii au devenit aspecte fundamentale în toate sectoarele de activitate economică ***și militară***, întrucât administrațiile publice, întreprinderile și cetățenii***, precum și actorii din domeniul militar și al apărării*** sunt astăzi mai interconectați și mai interdependenți decât oricând, între sectoare și dincolo de frontiere.

Amendamentul 2

Propunere de regulament
Considerentul 2

Textul propus de Comisie	*Amendamentul*
(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt în creștere, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware-ul sau perturbări. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. ***Această amenințare depășește*** agresiunea militară a Rusiei asupra Ucrainei și ***este susceptibilă*** să persiste, având în vedere multitudinea de actori aliniați cu autoritățile guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice	(2) Amploarea, frecvența și impactul incidentelor de securitate cibernetică sunt în creștere, inclusiv numărul atacurilor asupra lanțului de aprovizionare care vizează spionajul cibernetic, ransomware-ul sau perturbări. Acestea reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Având în vedere evoluția rapidă a peisajului amenințărilor, amenințarea unui posibil incident de mare amploare care cauzează perturbări sau daune semnificative infrastructurilor critice necesită o pregătire sporită la toate nivelurile cadrului de securitate cibernetică al Uniunii. ***Gravitatea acestor amenințări a devenit și mai pertinentă ca urmare a revenirii războiului pe continentul nostru. Aceste amenințări depășesc*** agresiunea militară a Rusiei asupra Ucrainei și ***sunt susceptibile*** să persiste, având în vedere multitudinea de actori aliniați cu autoritățile

furnizarea serviciilor publice și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei Uniunii și ar putea avea chiar consecințe asupra sănătății sau asupra vieții. În plus, incidentele de securitate cibernetică sunt imprevizibile, deoarece adesea apar și evoluează în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări.	guvernamentale, de infractori și hacktiviști implicați în tensiunile geopolitice actuale. Astfel de incidente pot să împiedice furnizarea serviciilor publice și desfășurarea activităților economice, inclusiv în sectoarele critice sau deosebit de critice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei Uniunii și ar putea avea chiar consecințe asupra sănătății sau asupra vieții ***în cazul unei eventuale subminări a instalațiilor legate de securitatea locală sau națională***. În plus, incidentele de securitate cibernetică sunt imprevizibile, deoarece adesea apar și evoluează în perioade foarte scurte de timp, nu sunt limitate la o zonă geografică specifică și se produc simultan sau se răspândesc instantaneu în multe țări. ***Securitatea cibernetică este importantă pentru a ne proteja valorile europene și asigură funcționarea democrațiilor noastre, apărându-ne infrastructura electorală și procedurile democratice de orice ingerință străină.***

Amendamentul 3

Propunere de regulament
Considerentul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	(2a) Securitatea cibernetică este esențială pentru a menține siguranța Uniunii noastre și pentru a împiedica actorii răuvoitori, statali și nestatali, să submineze democrația, economia și securitatea noastră. Este necesar să se prevină un peisaj fragmentat, deoarece o astfel de situație nu ar reprezenta o abordare adecvată, în special în fața unui viitor atac cibernetic la scară largă care vizează simultan mai multe state membre sau infrastructuri critice transnaționale. Prin urmare, este nevoie de un organ al Uniunii care să acționeze ca platformă de

coordonare pentru toate instrumentele, fondurile și mecanismele de securitate cibernetică existente și viitoare.

Amendamentul 4

Propunere de regulament
Considerentul 3

Textul propus de Comisie	*Amendamentul*
(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate și sprijinirea transformării digitale a acestora, prin consolidarea nivelului de securitate cibernetică pe piața unică digitală. Astfel cum se recomandă în trei propuneri diferite ale Conferinței privind viitorul Europei[16], este necesar să se sporească reziliența cetățenilor, a întreprinderilor și a entităților care operează infrastructuri critice împotriva amenințărilor cibernetice tot mai mari, care pot avea un impact societal și economic devastator. Prin urmare, sunt necesare investiții în infrastructuri și servicii care vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică.	(3) Este necesară consolidarea poziției competitive a industriei și a sectoarelor serviciilor din Uniune în cadrul economiei digitalizate și sprijinirea transformării digitale a acestora, prin consolidarea nivelului de securitate cibernetică pe piața unică digitală. Astfel cum se recomandă în trei propuneri diferite ale Conferinței privind viitorul Europei[16], este necesar să se sporească reziliența cetățenilor, a întreprinderilor și a entităților care operează infrastructuri critice împotriva amenințărilor cibernetice tot mai mari, care pot avea un impact societal și economic devastator. Prin urmare, sunt necesare investiții în infrastructuri și servicii care vor sprijini detectarea mai rapidă a amenințărilor și incidentelor de securitate cibernetică și răspunsul mai rapid la acestea, iar statele membre au nevoie de asistență pentru a se pregăti mai bine pentru incidentele de securitate cibernetică semnificative și de mare amploare și pentru a reacționa mai bine la acestea. De asemenea, Uniunea ar trebui să își sporească capacitățile în aceste domenii, în special în ceea ce privește colectarea și analiza datelor privind amenințările și incidentele de securitate cibernetică***, precum și capacitatea sa de a acționa în mod proactiv și de a reacționa în mod decisiv în astfel de cazuri***.
[16] https://futureu.europa.eu/ro/?locale=ro.	[16] https://futureu.europa.eu/ro/?locale=ro.

Amendamentul 5

Propunere de regulament
Considerentul 4

Textul propus de Comisie	*Amendamentul*
(4) Uniunea a luat deja o serie de măsuri pentru a reduce vulnerabilitățile și a spori reziliența infrastructurilor și a entităților critice împotriva riscurilor în materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[17], Recomandarea (UE) 2017/1584 a Comisiei[18], Directiva 2013/40/UE a Parlamentului European și a Consiliului[19] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[20]. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient, solidar și coordonat între ele, cu Comisia și cu alte autorități publice relevante, precum și cu entitățile vizate, pentru a spori reziliența infrastructurii critice utilizate pentru a furniza servicii esențiale pe piața internă.	(4) Uniunea a luat deja o serie de măsuri pentru a reduce vulnerabilitățile și a spori reziliența infrastructurilor și a entităților critice împotriva riscurilor în materie de securitate cibernetică, în special Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului[17], Recomandarea (UE) 2017/1584 a Comisiei[18], Directiva 2013/40/UE a Parlamentului European și a Consiliului[19] și Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului[20]. În plus, Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice invită statele membre să ia măsuri urgente și eficace și să coopereze loial, eficient ***și proactiv***, solidar și coordonat între ele, cu Comisia și cu alte autorități publice relevante, precum și cu entitățile vizate, pentru a spori reziliența infrastructurii critice utilizate pentru a furniza servicii esențiale pe piața internă. ***În plus, în martie 2022, Uniunea a aprobat și a lansat Busola strategică pentru securitate și apărare, care se concentrează, printre altele, pe întărirea securității cibernetice și pe consolidarea cooperării internaționale cu aliații care împărtășesc aceeași viziune și cu partenerii democratici, în special în această privință. În plus, securitatea cibernetică a fost un punct central al celei de-a treia declarații comune privind cooperarea UE-NATO din ianuarie 2023. În plus, raportul final de evaluare al grupului operativ UE-NATO a recomandat utilizarea deplină a sinergiilor dintre UE și NATO[1], inclusiv schimbul de bune practici între actorii civili și militari cu privire la punerea în aplicare a politicilor și a legislației pertinente din domeniul cibernetic.***

	[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en
[17] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (JO L 333, 27.12.2022).	[17] Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (JO L 333, 27.12.2022).
[18] Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).	[18] Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare (JO L 239, 19.9.2017, p. 36).
[19] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).	[19] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (JO L 218, 14.8.2013, p. 8).
[20] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).	[20] Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15).

Amendamentul 6

Propunere de regulament
Considerentul 6

Textul propus de Comisie	*Amendamentul*
(6) Comunicarea comună privind	(6) Comunicarea comună privind

politica UE în domeniul apărării cibernetice[22], adoptată la 10 noiembrie 2022, a anunțat o inițiativă a UE privind solidaritatea cibernetică cu următoarele obiective: consolidarea capabilităților comune de detectare, de conștientizare a situației și de răspuns la nivelul UE prin promovarea implementării unei infrastructuri a UE de centre de operațiuni de securitate („SOC”), sprijinirea creării treptate a unei rezerve de securitate cibernetică la nivelul UE cu servicii de la furnizori privați de încredere și testarea entităților critice în vederea identificării vulnerabilităților potențiale pe baza evaluărilor riscurilor la nivelul UE.	politica UE în domeniul apărării cibernetice[22], adoptată la 10 noiembrie 2022, a anunțat o inițiativă a UE privind solidaritatea cibernetică cu următoarele obiective: consolidarea capabilităților comune de detectare, de conștientizare a situației și de răspuns la nivelul UE prin promovarea implementării unei infrastructuri a UE de centre de operațiuni de securitate („SOC”), sprijinirea creării treptate a unei rezerve de securitate cibernetică la nivelul UE cu servicii de la furnizori privați de încredere și testarea entităților critice în vederea identificării vulnerabilităților potențiale pe baza evaluărilor riscurilor la nivelul UE. ***În plus, evoluția rapidă a peisajului amenințărilor cibernetice și ritmul rapid al dezvoltării tehnologice demonstrează, de asemenea, necesitatea unei mai bune coordonări și cooperări civile și militare, astfel cum a subliniat Consiliul în concluziile sale privind politica UE în domeniul apărării cibernetice[1].*** ***[1] Concluziile Consiliului privind politica UE în domeniul apărării cibernetice aprobate de Consiliu în cadrul reuniunii sale din 22 mai 2023, (9618/23).***
[22] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.	[22] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN(2022) 49 final.

Amendamentul 7

Propunere de regulament
Considerentul 6 a (nou)

Textul propus de Comisie	*Amendamentul*
	(6a) Având în vedere estomparea liniilor de demarcație dintre domeniul civil și cel militar și caracterul dual al instrumentelor și tehnologiilor cibernetice, este nevoie de o abordare

	cuprinzătoare și holistică a domeniului digital. În cazul unui incident și al unei crize de securitate cibernetică de mare amploare care implică mai multe state membre, ar trebui să se instituie o gestionare și o guvernare adecvate a crizelor. Aceste structuri ar trebui să organizeze schimbul de informații, coordonarea și cooperarea cu structurile de securitate externă și militare de gestionare a crizelor ale Uniunii, precum și cu organele statelor membre responsabile cu securitatea și apărarea (comunitatea de apărare cibernetică). Acest lucru ar trebui să se aplice, de asemenea, operațiunilor și misiunilor din cadrul politicii de securitate și apărare comune desfășurate de Uniune pentru a asigura pacea și stabilitatea în vecinătatea sa și dincolo de aceasta.

Amendamentul 8

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) Este necesar să se consolideze detectarea și conștientizarea situației privind amenințările și incidentele de securitate cibernetică în întreaga Uniune și să se consolideze solidaritatea prin sporirea gradului de pregătire și a capabilităților statelor membre și ale Uniunii de a răspunde la incidentele de securitate cibernetică semnificative și de mare amploare. Prin urmare, ar trebui implementată o infrastructură paneuropeană de SOC (Scutul cibernetic european) pentru a crea și a consolida capabilitățile comune de detectare și de conștientizare a situației; ar trebui instituit un mecanism pentru situații de urgență cibernetică pentru a sprijini statele membre să se pregătească pentru incidente de securitate cibernetică semnificative și de mare amploare***, să răspundă la acestea și***	(7) Este necesar să se consolideze detectarea și conștientizarea situației privind amenințările și incidentele de securitate cibernetică în întreaga Uniune și să se consolideze solidaritatea prin sporirea gradului de pregătire și a capabilităților statelor membre și ale Uniunii de a răspunde la incidentele de securitate cibernetică semnificative și de mare amploare. Prin urmare, ar trebui implementată o infrastructură paneuropeană de SOC (Scutul cibernetic european) pentru a crea și a consolida capabilitățile comune de detectare și de conștientizare a situației; ar trebui instituit un mecanism pentru situații de urgență cibernetică pentru a sprijini statele membre să se pregătească pentru incidente de securitate cibernetică semnificative și de mare amploare***, inclusiv incidente care***

să se redreseze imediat în urma lor; ar trebui instituit un mecanism de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice. Aceste acțiuni nu aduc atingere articolelor 107 și 108 din Tratatul privind funcționarea Uniunii Europene („TFUE”).

implică mai multe state membre; ***Atunci când este fezabil și necesar, un mecanism pentru situații de urgență cibernetică ar trebui să organizeze schimbul de informații și cooperarea cu autoritățile de apărare ale statelor membre și să fie sprijinit de instituțiile, organele și agențiile UE (comunitatea de apărare cibernetică a UE)***; ar trebui instituit un mecanism de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare specifice. ***Astfel de structuri noi ar trebui, de asemenea, să sprijine operațiunile și misiunile PSAC ale UE.*** Aceste acțiuni nu aduc atingere articolelor 107 și 108 din Tratatul privind funcționarea Uniunii Europene („TFUE”).

Amendamentul 9

Propunere de regulament
Considerentul 11

Textul propus de Comisie	*Amendamentul*
(11) În scopul bunei gestiuni financiare, ar trebui stabilite norme specifice pentru reportarea creditelor de angajament și de plată neutilizate. Respectând principiul potrivit căruia bugetul Uniunii este stabilit anual, prezentul regulament ar trebui să prevadă, având în vedere caracterul imprevizibil, excepțional și specific al peisajului securității cibernetice, posibilități de reportare a fondurilor neutilizate dincolo de cele prevăzute în Regulamentul financiar, maximizând astfel capacitatea mecanismului pentru situații de urgență cibernetică de a sprijini statele membre în combaterea eficace a amenințărilor cibernetice.	(11) În scopul bunei gestiuni financiare, ar trebui stabilite norme specifice pentru reportarea creditelor de angajament și de plată neutilizate. Respectând principiul potrivit căruia bugetul Uniunii este stabilit anual, prezentul regulament ar trebui să prevadă, având în vedere caracterul imprevizibil, excepțional și specific al peisajului securității cibernetice, posibilități de reportare a fondurilor neutilizate dincolo de cele prevăzute în Regulamentul financiar, maximizând astfel capacitatea mecanismului pentru situații de urgență cibernetică de a sprijini statele membre în combaterea eficace a amenințărilor cibernetice. ***Aceste norme specifice ar permite, de asemenea, acordarea de sprijin financiar pe termen mai lung pentru achizițiile publice comune de instrumente și infrastructuri foarte sigure de generație următoare, pentru a îmbunătăți capacitățile de***

	detectare colectivă prin utilizarea celor mai recente tehnologii de inteligență artificială (IA) și de analiză a datelor.

Amendamentul 10

Propunere de regulament
Considerentul 13

Textul propus de Comisie	*Amendamentul*
(13) Fiecare stat membru ar trebui să desemneze un organism public la nivel național însărcinat cu coordonarea activităților de detectare a amenințărilor cibernetice în statul membru respectiv. Aceste SOC naționale ar trebui să acționeze ca punct de referință și punct de acces la nivel național pentru participarea la Scutul cibernetic european și ar trebui să se asigure că informațiile privind amenințările cibernetice provenite de la entități publice și private sunt partajate și colectate la nivel național într-un mod eficace și raționalizat.	(13) Fiecare stat membru ar trebui să desemneze un organism public la nivel național însărcinat cu coordonarea activităților de detectare a amenințărilor cibernetice în statul membru respectiv. Aceste SOC naționale ar trebui să acționeze ca punct de referință și punct de acces la nivel național pentru participarea la Scutul cibernetic european și ar trebui să se asigure că informațiile privind amenințările cibernetice provenite de la entități publice și private sunt partajate și colectate la nivel național într-un mod eficace și raționalizat. ***Atunci când este fezabil și necesar, SOC ar trebui să permită, de asemenea, participarea entităților din domeniul apărării, instituind un „pilon al apărării” în ceea ce privește guvernarea și tipul de informații partajate, astfel cum se prevede în comunicarea comună privind politica UE în materie de apărare cibernetică[1] și cu sprijinul Înaltului Reprezentant.*** ***[1] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN/2022/49 final***

Amendamentul 11

Propunere de regulament
Considerentul 14

Textul propus de Comisie	*Amendamentul*
(14) În cadrul Scutului cibernetic european ar trebui înființate o serie de centre de operațiuni transfrontaliere în materie de securitate cibernetică („SOC transfrontaliere”). Acestea ar trebui să reunească SOC naționale din cel puțin trei state membre, astfel încât beneficiile detectării amenințărilor transfrontaliere și ale schimbului și gestionării informațiilor să poată fi realizate pe deplin. Obiectivul general al SOC transfrontaliere ar trebui să fie consolidarea capacităților de analiză, prevenire și detectare a amenințărilor la adresa securității cibernetice și sprijinirea producerii de informații de înaltă calitate privind amenințările cibernetice, în special prin schimbul de date din diferite surse, publice sau private, precum și prin partajarea și utilizarea în comun a instrumentelor de ultimă generație și prin dezvoltarea în comun a capabilităților de detectare, analiză și prevenire într-un mediu de încredere. Acestea ar trebui să ofere noi capacități suplimentare, pe baza și în completarea SOC-urilor existente și a echipelor de intervenție în caz de incidente de securitate informatică („CSIRT”) și a altor actori relevanți.	(14) În cadrul Scutului cibernetic european ar trebui înființate o serie de centre de operațiuni transfrontaliere în materie de securitate cibernetică („SOC transfrontaliere”). Acestea ar trebui să reunească SOC naționale din cel puțin trei state membre, ***incluzând un „pilon al apărării”,*** astfel încât beneficiile detectării amenințărilor transfrontaliere și ale schimbului și gestionării informațiilor să poată fi realizate pe deplin. Obiectivul general al SOC transfrontaliere ar trebui să fie consolidarea capacităților de analiză, prevenire și detectare a amenințărilor la adresa securității cibernetice și sprijinirea producerii de informații de înaltă calitate privind amenințările cibernetice, în special prin schimbul de date din diferite surse, publice sau private ***și, atunci când este necesar și fezabil, militare, cu orientări suficiente pentru schimbul de informații,*** precum și prin partajarea și utilizarea în comun a instrumentelor de ultimă generație și prin dezvoltarea în comun a capabilităților de detectare, analiză și prevenire într-un mediu de încredere. Acestea ar trebui să ofere noi capacități suplimentare, pe baza și în completarea SOC-urilor existente și a echipelor de intervenție în caz de incidente de securitate informatică („CSIRT”) și a altor actori relevanți.

Amendamentul 12

Propunere de regulament
Considerentul 15

Textul propus de Comisie	*Amendamentul*
(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac	(15) La nivel național, monitorizarea, detectarea și analiza amenințărilor cibernetice sunt, de regulă, asigurate de SOC ale entităților publice și private, în combinație cu CSIRT. În plus, CSIRT fac

schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă capabilitate care să fie complementară rețelei CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, sporind valoarea acestor date prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a ***suveranității tehnologice ale*** Uniunii.

schimb de informații în contextul rețelei CSIRT, în conformitate cu Directiva (UE) 2022/2555. SOC transfrontaliere ar trebui să constituie o nouă capabilitate care să fie complementară rețelei CSIRT, prin punerea în comun și schimbul de date privind amenințările cibernetice provenite de la entități publice și private, sporind valoarea acestor date prin analize de specialitate și infrastructuri achiziționate în comun și prin instrumente de ultimă generație și contribuind la dezvoltarea capabilităților și a ***rezilienței*** Uniunii.

Amendamentul 13

Propunere de regulament
Considerentul 16

Textul propus de Comisie	*Amendamentul*
(16) SOC-urile transfrontaliere ar trebui să acționeze ca un punct central care să permită o punere în comun pe scară largă a datelor relevante și a informațiilor privind amenințările cibernetice, să permită răspândirea informațiilor privind amenințările în rândul unui set mare și divers de actori [de exemplu, echipe de intervenție în caz de urgență informatică („CERT”), CSIRT, centre de schimb de informații și de analiză („ISAC”), operatori de infrastructuri critice]. Informațiile schimbate între participanții la un SOC transfrontalier ar putea include date provenite de la rețele și senzori, fluxuri de informații privind amenințările cibernetice, indicatori de compromis și informații contextualizate cu privire la incidente, amenințări și vulnerabilități. În plus, SOC-urile transfrontaliere ar trebui să încheie acorduri de cooperare cu alte SOC-uri transfrontaliere.	(16) SOC-urile transfrontaliere ar trebui să acționeze ca un punct central care să permită o punere în comun pe scară largă a datelor relevante și a informațiilor privind amenințările cibernetice, să permită răspândirea informațiilor privind amenințările în rândul unui set mare și divers de actori [de exemplu, echipe de intervenție în caz de urgență informatică („CERT”), CSIRT, centre de schimb de informații și de analiză („ISAC”), operatori de infrastructuri critice]***, precum și comunitatea de apărare cibernetică***. Informațiile schimbate între participanții la un SOC transfrontalier ar putea include date provenite de la rețele și senzori, fluxuri de informații privind amenințările cibernetice, indicatori de compromis și informații contextualizate cu privire la incidente, amenințări și vulnerabilități. În plus, SOC-urile transfrontaliere ar trebui să încheie acorduri de cooperare cu alte SOC-uri transfrontaliere ***și cu rețeaua operațională pentru milCERT (MICNET), atunci când va fi înființată***.

Amendamentul 14

Propunere de regulament
Considerentul 17

Textul propus de Comisie	*Amendamentul*
(17) Conștientizarea comună a situației în rândul autorităților relevante reprezintă o condiție prealabilă indispensabilă pentru pregătirea și coordonarea la nivelul Uniunii în ceea ce privește incidentele de securitate cibernetică semnificative și de mare amploare. Directiva (UE) 2022/2555 instituie EU-CyCLONe pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organele și agențiile Uniunii. Recomandarea (UE) 2017/1584 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare abordează rolul tuturor actorilor relevanți. Directiva (UE) 2022/2555 reamintește, de asemenea, responsabilitățile Comisiei în cadrul mecanismului de protecție civilă al Uniunii („UCPM”) instituit prin Decizia 1313/2013/UE a Parlamentului European și a Consiliului, precum și de a furniza rapoarte analitice pentru mecanismul integrat pentru un răspuns politic la crize („IPCR”) în temeiul Deciziei de punere în aplicare (UE) 2018/1993. Prin urmare, în situațiile în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea ar trebui să furnizeze informații relevante către EU-CyCLONe, rețelei CSIRT și Comisiei. În funcție de situație, informațiile care urmează să fie partajate ar putea include în special informații tehnice, informații cu privire la natura și motivele atacatorului sau ale atacatorului potențial, precum și	(17) Conștientizarea comună a situației în rândul autorităților relevante reprezintă o condiție prealabilă indispensabilă pentru pregătirea și coordonarea la nivelul Uniunii în ceea ce privește incidentele de securitate cibernetică semnificative și de mare amploare. Directiva (UE) 2022/2555 instituie EU-CyCLONe pentru a sprijini gestionarea coordonată, la nivel operațional, a incidentelor de securitate cibernetică de mare amploare și a crizelor și pentru a asigura schimbul periodic de informații relevante între statele membre și instituțiile, organele și agențiile Uniunii. Recomandarea (UE) 2017/1584 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare abordează rolul tuturor actorilor relevanți. Directiva (UE) 2022/2555 reamintește, de asemenea, responsabilitățile Comisiei în cadrul mecanismului de protecție civilă al Uniunii („UCPM”) instituit prin Decizia 1313/2013/UE a Parlamentului European și a Consiliului, precum și de a furniza rapoarte analitice pentru mecanismul integrat pentru un răspuns politic la crize („IPCR”) în temeiul Deciziei de punere în aplicare (UE) 2018/1993. Prin urmare, în situațiile în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea ar trebui să furnizeze informații relevante către EU-CyCLONe, rețelei CSIRT***, comunității de apărare cibernetică*** și Comisiei. În funcție de situație, informațiile care urmează să fie partajate ar putea include în special informații tehnice, informații cu privire la natura și motivele atacatorului sau ale

informații fără caracter tehnic de nivel superior cu privire la un incident de securitate cibernetică de mare amploare potențial sau în curs. În acest context, ar trebui să se acorde atenția cuvenită principiului necesității de a cunoaște și caracterului potențial sensibil al informațiilor partajate.	atacatorului potențial, precum și informații fără caracter tehnic de nivel superior cu privire la un incident de securitate cibernetică de mare amploare potențial sau în curs. În acest context, ar trebui să se acorde atenția cuvenită principiului necesității de a cunoaște și caracterului potențial sensibil al informațiilor partajate.

Amendamentul 15

Propunere de regulament
Considerentul 19

Textul propus de Comisie	*Amendamentul*
(19) Pentru a permite schimbul de date privind amenințările cibernetice din diferite surse, la scară largă, într-un mediu de încredere, entitățile care participă la Scutul cibernetic european ar trebui să fie echipate cu instrumente, echipamente și infrastructuri de ultimă generație și de înaltă securitate. Acest lucru ar trebui să permită îmbunătățirea capacităților de detectare colectivă și avertizarea în timp util a autorităților și a entităților relevante, în special prin utilizarea celor mai recente tehnologii de inteligență artificială și de analiză a datelor.	(19) Pentru a permite schimbul de date privind amenințările cibernetice din diferite surse, la scară largă, într-un mediu de încredere, entitățile care participă la Scutul cibernetic european ar trebui să fie echipate cu instrumente, echipamente și infrastructuri de ultimă generație și de înaltă securitate***, excluzând furnizorii de mare risc de produse critice cu elemente digitale***. Acest lucru ar trebui să permită îmbunătățirea capacităților de detectare colectivă și avertizarea în timp util a autorităților și a entităților relevante, în special prin utilizarea celor mai recente tehnologii de inteligență artificială și de analiză a datelor. ***Utilizarea IA ar trebui să fie supusă supravegherii umane, iar persoanele care exercită această funcție ar trebui să dispună de un nivel suficient de cunoștințe în domeniul IA, precum și de sprijinul și de autoritatea necesare.***

Amendamentul 16

Propunere de regulament
Considerentul 19 a (nou)

Textul propus de Comisie	*Amendamentul*
	(19a) În concordanță cu Regulamentul [XX/XXXX (Actul privind reziliența

cibernetică)], entitățile care participă la Scutul cibernetic european ar trebui să îndeplinească, de asemenea, cerințele prevăzute în prezentul regulament pentru toate produsele cu elemente digitale. Având în vedere riscurile tot mai mari generate de dependențele economice, este necesar să se reducă la minimum expunerea la furnizorii cu risc ridicat de produse critice, prin intermediul unui cadru strategic comun pentru securitatea economică a UE. Dependențele de furnizorii cu grad ridicat de risc de produse critice cu elemente digitale prezintă un risc strategic care ar trebui abordat la nivelul Uniunii, în special dacă o țară se angajează în spionaj economic sau în constrângere economică, iar legislația sa impune accesul arbitrar la orice tip de operațiuni sau date ale întreprinderii, în special atunci când produsele critice sunt destinate utilizării de către entitățile esențiale menționate în Directiva (UE) 2022/2555.

Amendamentul 17

Propunere de regulament
Considerentul 20

Textul propus de Comisie	*Amendamentul*
(20) Prin colectarea, partajarea și schimbul de date, Scutul cibernetic european ar trebui să consolideze suveranitatea tehnologică a Uniunii. Punerea în comun a datelor actualizate de înaltă calitate ar trebui să contribuie și la dezvoltarea unor tehnologii avansate de inteligență artificială și de analiză a datelor. Aceasta ar trebui facilitată prin conectarea Scutului cibernetic european cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173 al Consiliului[25].	(20) Prin colectarea, partajarea și schimbul de date, Scutul cibernetic european ar trebui să consolideze suveranitatea tehnologică a Uniunii***, autonomia, competitivitatea și reziliența strategice ale sale***. Punerea în comun a datelor actualizate de înaltă calitate ar trebui să contribuie și la dezvoltarea unor tehnologii avansate de inteligență artificială și de analiză a datelor. Aceasta ar trebui facilitată prin conectarea Scutului cibernetic european cu infrastructura paneuropeană de calcul de înaltă performanță instituită prin Regulamentul (UE) 2021/1173 al Consiliului[25].

[25] Regulamentul (UE) 2021/1173 al Consiliului din 13 iulie 2021 privind instituirea întreprinderii comune pentru calculul european de înaltă performanță și de abrogare a Regulamentului (UE) 2018/1488 (JO L 256, 19.7.2021, p. 3).

[25] Regulamentul (UE) 2021/1173 al Consiliului din 13 iulie 2021 privind instituirea întreprinderii comune pentru calculul european de înaltă performanță și de abrogare a Regulamentului (UE) 2018/1488 (JO L 256, 19.7.2021, p. 3).

Amendamentul 18

Propunere de regulament
Considerentul 25

Textul propus de Comisie	*Amendamentul*
(25) Mecanismul pentru situații de urgență cibernetică ar trebui să ofere sprijin statelor membre în completarea propriilor măsuri și resurse, precum și a altor opțiuni de sprijin existente în cazul răspunsului la incidentele de securitate cibernetică semnificative și de mare amploare și al redresării imediate în urma acestora, cum ar fi serviciile furnizate de Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”) în conformitate cu mandatul său, răspunsul coordonat și asistența din partea rețelei CSIRT, sprijinul pentru atenuare din partea EU-CyCLONe, precum și asistența reciprocă între statele membre, inclusiv în contextul articolului 42 alineatul (7) din TUE, echipele de răspuns rapid în domeniul cibernetic din cadrul PESCO***[26]*** și echipele de răspuns rapid în caz de amenințări hibride. Acesta ar trebui să abordeze necesitatea de a se asigura că sunt disponibile mijloace specializate pentru a sprijini pregătirea în vederea incidentelor de securitate cibernetică în întreaga Uniune și în țările terțe și răspunsul la acestea.	(25) Mecanismul pentru situații de urgență cibernetică ar trebui să ofere sprijin statelor membre în completarea propriilor măsuri și resurse, precum și a altor opțiuni de sprijin existente în cazul răspunsului la incidentele de securitate cibernetică semnificative și de mare amploare și al redresării imediate în urma acestora, cum ar fi serviciile furnizate de Agenția Uniunii Europene pentru Securitate Cibernetică („ENISA”) în conformitate cu mandatul său, răspunsul coordonat și asistența din partea rețelei CSIRT, sprijinul pentru atenuare din partea EU-CyCLONe, precum și asistența reciprocă între statele membre, inclusiv în contextul articolului 42 alineatul (7) din TUE, echipele de răspuns rapid în domeniul cibernetic din cadrul PESCO***[1], noul Centru de coordonare a domeniului de informații cibernetice (CIDCC) al proiectului PESCO și succesorul său propus, Centrul de coordonare a apărării cibernetice al UE (EUCDCC)*** și echipele de răspuns rapid în caz de amenințări hibride. Acesta ar trebui să abordeze necesitatea de a se asigura că sunt disponibile mijloace specializate pentru a sprijini pregătirea în vederea incidentelor de securitate cibernetică în întreaga Uniune și în țările terțe și răspunsul la acestea***, îndeosebi în țările candidate la UE aliniate la politica***

externă și de securitate comună și la politica de securitate și apărare comună ale UE, sprijinindu-le în dezvoltarea capacităților lor cibernetice și consolidând cooperarea transfrontalieră și regională între aceste țări candidate în domeniul cibernetic.

[1] Decizia (PESC) 2017/2315 a Consiliului din 11 decembrie 2017 de stabilire a cooperării structurate permanente (PESCO) și de adoptare a listei statelor membre participante.

---

[26] Decizia (PESC) 2017/2315 a Consiliului din 11 decembrie 2017 de stabilire a cooperării structurate permanente (PESCO) și de adoptare a listei statelor membre participante.

[26] Decizia (PESC) 2017/2315 a Consiliului din 11 decembrie 2017 de stabilire a cooperării structurate permanente (PESCO) și de adoptare a listei statelor membre participante.

Amendamentul 19

Propunere de regulament
Considerentul 26

Textul propus de Comisie	*Amendamentul*
(26) Acest instrument nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special UCPM[27], IPCR[28], și Directivei (UE) 2022/2555. Acesta poate contribui la acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din TUE sau în situațiile definite la articolul 222 din TFUE sau poate completa aceste acțiuni. Utilizarea acestui instrument ar trebui, de asemenea, să fie coordonată cu punerea în aplicare a măsurilor din setul de instrumente pentru diplomația cibernetică, ***după caz***.	(26) Acest instrument nu aduce atingere procedurilor și cadrelor de coordonare a răspunsului la crize la nivelul Uniunii, în special UCPM[27], IPCR[28], și Directivei (UE) 2022/2555. Acesta poate contribui la acțiunile puse în aplicare în contextul articolului 42 alineatul (7) din TUE sau în situațiile definite la articolul 222 din TFUE sau poate completa aceste acțiuni. Utilizarea acestui instrument ar trebui, de asemenea, să fie coordonată cu punerea în aplicare a măsurilor din setul de instrumente pentru diplomația cibernetică, ***consolidând cooperarea la nivel strategic, operațional și tehnic între apărarea cibernetică și alte comunități cibernetice, în special în vederea consolidării capacităților împotriva amenințărilor la adresa securității cibernetice din afara Uniunii, inclusiv a măsurilor restrictive,***

	care pot fi utilizate pentru a preveni și a răspunde la activitățile cibernetice rău intenționate.
[27] Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).	[27] Decizia nr. 1313/2013/UE a Parlamentului European și a Consiliului din 17 decembrie 2013 privind un mecanism de protecție civilă al Uniunii (JO L 347, 20.12.2013, p. 924).
[28] Mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) și în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.	[28] Mecanismul integrat al UE pentru un răspuns politic la crize (IPCR) și în conformitate cu Recomandarea (UE) 2017/1584 a Comisiei din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

Amendamentul 20

Propunere de regulament
Considerentul 28

Textul propus de Comisie	*Amendamentul*
(28) Directiva (UE) 2022/2555 impune statelor membre să desemneze sau să înființeze una sau mai multe autorități de gestionare a crizelor cibernetice și să se asigure că acestea dispun de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace și eficient. De asemenea, aceasta impune statelor membre să identifice capacitățile, activele și procedurile care pot fi utilizate în cazul unei crize, precum și să adopte un plan național de răspuns la incidente de securitate cibernetică de mare amploare și crize, în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor de securitate cibernetică de mare amploare și a crizelor. Statele membre au, de asemenea, obligația de a înființa una sau mai multe CSIRT însărcinate cu responsabilități de administrare a incidentelor în conformitate cu un proces bine definit și care să acopere cel puțin	(28) Directiva (UE) 2022/2555 impune statelor membre să desemneze sau să înființeze una sau mai multe autorități de gestionare a crizelor cibernetice și să se asigure că acestea dispun de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace și eficient. De asemenea, aceasta impune statelor membre să identifice capacitățile, activele și procedurile care pot fi utilizate în cazul unei crize, precum și să adopte un plan național de răspuns la incidente de securitate cibernetică de mare amploare și crize, în care sunt stabilite obiectivele și modalitățile de gestionare a incidentelor de securitate cibernetică de mare amploare și a crizelor. Statele membre au, de asemenea, obligația de a înființa una sau mai multe CSIRT însărcinate cu responsabilități de administrare a incidentelor în conformitate cu un proces bine definit și care să acopere cel puțin

sectoarele, subsectoarele și tipurile de entități care intră în domeniul de aplicare al directivei respective, precum și de a se asigura că acestea dispun de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace. Prezentul regulament nu aduce atingere rolului Comisiei în asigurarea respectării de către statele membre a obligațiilor prevăzute în Directiva (UE) 2022/2555. Mecanismul pentru situații de urgență cibernetică ar trebui să ofere asistență pentru acțiunile menite să consolideze pregătirea, precum și pentru acțiunile de răspuns la incidente pentru a atenua impactul incidentelor de securitate cibernetică semnificative și de mare amploare, pentru a sprijini redresarea imediată și/sau pentru a restabili funcționarea serviciilor esențiale.	sectoarele, subsectoarele și tipurile de entități care intră în domeniul de aplicare al directivei respective, precum și de a se asigura că acestea dispun de resurse adecvate pentru a-și îndeplini sarcinile în mod eficace. Prezentul regulament nu aduce atingere rolului Comisiei în asigurarea respectării de către statele membre a obligațiilor prevăzute în Directiva (UE) 2022/2555. Mecanismul pentru situații de urgență cibernetică ar trebui să ofere asistență pentru acțiunile menite să consolideze pregătirea, precum și pentru acțiunile de răspuns la incidente pentru a atenua impactul incidentelor de securitate cibernetică semnificative și de mare amploare, pentru a sprijini redresarea imediată și/sau pentru a restabili funcționarea serviciilor esențiale***, utilizând în mod corespunzător întreaga gamă de opțiuni defensive aflate la dispoziția comunităților civile și militare***.

Amendamentul 21

Propunere de regulament
Considerentul 29

Textul propus de Comisie	*Amendamentul*
(29) În cadrul acțiunilor de pregătire, pentru a promova o abordare coerentă și a consolida securitatea în întreaga Uniune și pe piața sa internă, ar trebui să se acorde sprijin pentru testarea și evaluarea în mod coordonat a securității cibernetice a entităților care își desfășoară activitatea în sectoare deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. ***Sectoarele sau subsectoarele*** ar trebui să fie selectate din anexa I la	(29) În cadrul acțiunilor de pregătire, pentru a promova o abordare coerentă și a consolida securitatea în întreaga Uniune și pe piața sa internă, ar trebui să se acorde sprijin pentru testarea și evaluarea în mod coordonat a securității cibernetice a entităților care își desfășoară activitatea în sectoare deosebit de critice identificate în temeiul Directivei (UE) 2022/2555. În acest scop, Comisia, cu sprijinul ENISA și în cooperare cu Grupul de cooperare NIS instituit prin Directiva (UE) 2022/2555, ar trebui să identifice periodic sectoarele sau subsectoarele relevante care ar trebui să fie eligibile pentru a primi sprijin financiar pentru testarea coordonată la nivelul Uniunii. ***Atunci când este cazul, Serviciul European de Acțiune Externă (SEAE), în***

Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). Exercițiile de testare coordonată ar trebui să se bazeze pe scenarii și metodologii de risc comune. Selectarea sectoarelor și elaborarea scenariilor de risc ar trebui să țină seama de evaluările riscurilor și de scenariile de risc relevante la nivelul Uniunii, inclusiv de necesitatea de a evita suprapunerile, cum ar fi evaluarea riscurilor și scenariile de risc solicitate în concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene, care urmează să fie efectuate de Comisie, de Înaltul Reprezentant și de Grupul de cooperare NIS, în coordonare cu organismele și agențiile civile și militare relevante și cu rețelele instituite, inclusiv EU-CyCLONe, precum și de evaluarea riscurilor pentru rețelele și infrastructurile de comunicații, solicitată prin Apelul ministerial comun de la Nevers și realizată de Grupul de cooperare NIS, cu sprijinul Comisiei și al ENISA și în cooperare cu Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), de evaluările coordonate ale riscurilor care urmează să fie efectuate în temeiul articolului 22 din Directiva (UE) 2022/2555 și de testarea rezilienței operaționale digitale, astfel cum se prevede în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului***[29]***. Selectarea sectoarelor ar trebui, de asemenea, să țină seama de Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice.

special prin intermediul Centrului de informații al UE (INTCEN) și al Celulei sale de fuziune împotriva amenințărilor hibride, cu sprijinul Direcției de informații a Statului-Major al Uniunii Europene (EUMS) din cadrul Capacității unice de analiză a informațiilor (SIAC), ar trebui, de asemenea, să fie asociat pentru a furniza evaluări actualizate și, astfel, să contribuie la identificarea sectoarelor sau a subsectoarelor care ar trebui să fie selectate din anexa I la Directiva (UE) 2022/2555 („Sectoare cu o importanță critică ridicată”). Exercițiile de testare coordonată ar trebui să se bazeze pe scenarii și metodologii de risc comune. ***Aceste exerciții ar trebui să joace, de asemenea, un rol important în îmbunătățirea cooperării dintre entitățile civile și militare. Prin urmare, atunci când organizează exerciții, Comisia, SEAE și ENISA ar trebui să ia în considerare în mod sistematic includerea participanților din alte comunități cibernetice, cum ar fi Agenția Europeană de Apărare (AEA) și alte entități pertinente.*** Selectarea sectoarelor și elaborarea scenariilor de risc ar trebui să țină seama de evaluările riscurilor și de scenariile de risc relevante la nivelul Uniunii, inclusiv de necesitatea de a evita suprapunerile, cum ar fi evaluarea riscurilor și scenariile de risc solicitate în concluziile Consiliului privind dezvoltarea poziției cibernetice a Uniunii Europene, care urmează să fie efectuate de Comisie, de Înaltul Reprezentant și de Grupul de cooperare NIS, în coordonare cu organismele și agențiile civile și militare relevante și cu rețelele instituite, inclusiv EU-CyCLONe, precum și de evaluarea riscurilor pentru rețelele și infrastructurile de comunicații, solicitată prin Apelul ministerial comun de la Nevers și realizată de Grupul de cooperare NIS, cu sprijinul Comisiei și al ENISA și în cooperare cu Organismul Autorităților Europene de Reglementare în Domeniul Comunicațiilor Electronice (OAREC), de evaluările

coordonate ale riscurilor care urmează să fie efectuate în temeiul articolului 22 din Directiva (UE) 2022/2555 și de testarea rezilienței operaționale digitale, astfel cum se prevede în Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului***[1]***. Selectarea sectoarelor ar trebui, de asemenea, să țină seama de Recomandarea Consiliului privind o abordare coordonată la nivelul Uniunii în vederea consolidării rezilienței infrastructurii critice.

[1] Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011.

---

[29] Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011.

[29] Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011.

Amendamentul 22

Propunere de regulament
Considerentul 32

Textul propus de Comisie	*Amendamentul*
(32) Mecanismul pentru situații de urgență cibernetică ar trebui să sprijine asistența acordată de statele membre, inclusiv de rețeaua CSIRT prevăzută la articolul 15 din Directiva (UE) 2022/2555, unui stat membru afectat de un incident de securitate cibernetică semnificativ sau de mare amploare. Statele membre care acordă asistență ar trebui să aibă	(32) Mecanismul pentru situații de urgență cibernetică ar trebui să sprijine asistența acordată de statele membre, inclusiv de rețeaua CSIRT prevăzută la articolul 15 din Directiva (UE) 2022/2555, unui stat membru afectat de un incident de securitate cibernetică semnificativ sau de mare amploare. Statele membre care acordă asistență ar trebui să aibă

posibilitatea de a depune cereri pentru a acoperi costurile legate de trimiterea echipelor de experți în cadrul asistenței reciproce. Costurile eligibile ar putea include cheltuielile de deplasare, cazare și diurnă ale experților în securitate cibernetică.	posibilitatea de a depune cereri pentru a acoperi costurile legate de trimiterea echipelor de experți în cadrul asistenței reciproce***, asigurând o coordonare eficientă între programele și instrumentele pertinente ale UE, printre care Instrumentul european pentru pace (IEP), PESC și IVCDCI, atunci când acordă asistență țărilor terțe, în special Ucrainei și Moldovei.*** Costurile eligibile ar putea include cheltuielile de deplasare, cazare și diurnă ale experților în securitate cibernetică.

Amendamentul 23

Propunere de regulament
Considerentul 33

Textul propus de Comisie	*Amendamentul*
(33) Ar trebui instituită treptat o rezervă de securitate cibernetică la nivelul Uniunii, care să constea în servicii furnizate de furnizori privați de servicii de securitate gestionate pentru a sprijini răspunsul și acțiunile imediate de redresare în cazul unor incidente de securitate cibernetică semnificative sau de mare amploare. Rezerva UE pentru securitate cibernetică ar trebui să asigure disponibilitatea și promptitudinea serviciilor. Serviciile din rezerva UE pentru securitate cibernetică ar trebui să servească la sprijinirea autorităților naționale în ceea ce privește furnizarea de asistență entităților afectate care își desfășoară activitatea în sectoare critice sau deosebit de critice, în completarea propriilor acțiuni la nivel național. Atunci când solicită sprijin din rezerva UE pentru securitate cibernetică, statele membre ar trebui să specifice sprijinul acordat entității afectate la nivel național, care ar trebui luat în considerare atunci când se evaluează cererea statului membru. Serviciile din rezerva UE pentru securitate cibernetică pot servi, de asemenea, la sprijinirea instituțiilor, a	(33) Ar trebui instituită treptat o rezervă de securitate cibernetică la nivelul Uniunii, care să constea în servicii furnizate de furnizori privați de servicii de securitate gestionate pentru a sprijini răspunsul și acțiunile imediate de redresare în cazul unor incidente de securitate cibernetică semnificative sau de mare amploare. Rezerva UE pentru securitate cibernetică ar trebui să asigure disponibilitatea și promptitudinea serviciilor. Serviciile din rezerva UE pentru securitate cibernetică ar trebui să servească la sprijinirea autorităților naționale în ceea ce privește furnizarea de asistență entităților afectate care își desfășoară activitatea în sectoare critice sau deosebit de critice, în completarea propriilor acțiuni la nivel național. Atunci când solicită sprijin din rezerva UE pentru securitate cibernetică, statele membre ar trebui să specifice sprijinul acordat entității afectate la nivel național, care ar trebui luat în considerare atunci când se evaluează cererea statului membru. Serviciile din rezerva UE pentru securitate cibernetică pot servi, de asemenea, la sprijinirea instituțiilor, a

organelor și a agențiilor Uniunii, în condiții similare.	organelor și a agențiilor Uniunii, ***inclusiv a misiunilor PSAC,*** în condiții similare.

Amendamentul 24

Propunere de regulament
Considerentul 34

Textul propus de Comisie	*Amendamentul*
(34) În scopul selectării furnizorilor privați de servicii care să furnizeze servicii în contextul rezervei UE pentru securitate cibernetică, este necesar să se stabilească un set de criterii minime care ar trebui incluse în cererea de oferte pentru selectarea acestor furnizori, astfel încât să se asigure că sunt îndeplinite nevoile autorităților și entităților din statele membre care își desfășoară activitatea în sectoare critice sau deosebit de critice.	(34) În scopul selectării furnizorilor privați de servicii care să furnizeze servicii în contextul rezervei UE pentru securitate cibernetică, este necesar să se stabilească un set de criterii minime care ar trebui incluse în cererea de oferte pentru selectarea acestor furnizori, astfel încât să se asigure că sunt îndeplinite nevoile autorităților și entităților din statele membre care își desfășoară activitatea în sectoare critice sau deosebit de critice***, luând în considerare, de asemenea, riscurile asociate participării furnizorilor din țările concurente strategice, care pot genera riscuri de securitate economică, precum și implicațiile pentru securitatea strategică a Uniunii***.

Amendamentul 25

Propunere de regulament
Considerentul 36

Textul propus de Comisie	*Amendamentul*
(36) Pentru a sprijini obiectivele prezentului regulament de promovare a conștientizării comune a situației, de consolidare a rezilienței Uniunii și de facilitare a unui răspuns eficace la incidentele de securitate cibernetică semnificative și de mare amploare, EU-CyCLONe, rețeaua CSIRT sau Comisia ar trebui să poată solicita ENISA să revizuiască și să evalueze amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un anumit incident de	(36) Pentru a sprijini obiectivele prezentului regulament de promovare a conștientizării comune a situației, de consolidare a rezilienței Uniunii și de facilitare a unui răspuns eficace la incidentele de securitate cibernetică semnificative și de mare amploare, EU-CyCLONe, rețeaua CSIRT sau Comisia ar trebui să poată solicita ENISA să revizuiască și să evalueze amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un anumit incident de

securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și evaluări a unui incident, ENISA ar trebui să elaboreze un raport de examinare a incidentelor, în colaborare cu părțile interesate relevante, inclusiv cu reprezentanți ai sectorului privat, ai statelor membre, ai Comisiei și ai altor instituții, organisme și agenții relevante ale UE. În ceea ce privește sectorul privat, ENISA dezvoltă canale pentru schimbul de informații cu furnizorii specializați, inclusiv cu furnizorii de soluții de securitate gestionate și cu vânzătorii, pentru a contribui la misiunea ENISA de a atinge un nivel comun ridicat de securitate cibernetică în întreaga Uniune. Pe baza colaborării cu părțile interesate, inclusiv cu sectorul privat, raportul de examinare privind incidentele specifice ar trebui să vizeze evaluarea cauzelor, a impactului și a atenuării unui incident, după producerea acestuia. Ar trebui să se acorde o atenție deosebită contribuțiilor și învățămintelor împărtășite de furnizorii de servicii de securitate gestionate care îndeplinesc condițiile de maximă integritate profesională, imparțialitate și cunoștințe tehnice necesare, astfel cum se prevede în prezentul regulament. Raportul ar trebui să fie prezentat rețelelor EU-CyCLONe și CSIRT și Comisiei și să contribuie a activitatea acestora. În cazul în care incidentul se referă la o țară terță, acesta va fi, de asemenea, transmis de către Comisie Înaltului Reprezentant.

securitate cibernetică semnificativ sau de mare amploare. ***În vederea dezvoltării unui sistem de conectivitate securizat, bazat pe infrastructura europeană de comunicații cuantice (EuroQCI) și pe programul de comunicare guvernamentală prin satelit a Uniunii Europene (GOVSATCOM), îndeosebi pe punerea în aplicare a GNSS GALILEO pentru utilizatorii din domeniul apărării, orice eventuală dezvoltare viitoare ar trebui să ia în considerare apariția "hiperrăzboiului", care îmbină viteza și sofisticarea informaticii cuantice cu sisteme militare extrem de autonome.*** După finalizarea unei analize și evaluări a unui incident, ENISA ar trebui să elaboreze un raport de examinare a incidentelor, în colaborare cu părțile interesate relevante, inclusiv cu reprezentanți ai sectorului privat, ai statelor membre, ai Comisiei și ai altor instituții, organisme și agenții relevante ale UE. În ceea ce privește sectorul privat, ENISA dezvoltă canale pentru schimbul de informații cu furnizorii specializați, inclusiv cu furnizorii de soluții de securitate gestionate și cu vânzătorii, pentru a contribui la misiunea ENISA de a atinge un nivel comun ridicat de securitate cibernetică în întreaga Uniune. Pe baza colaborării cu părțile interesate, inclusiv cu sectorul privat, raportul de examinare privind incidentele specifice ar trebui să vizeze evaluarea cauzelor, a impactului și a atenuării unui incident, după producerea acestuia. Ar trebui să se acorde o atenție deosebită contribuțiilor și învățămintelor împărtășite de furnizorii de servicii de securitate gestionate care îndeplinesc condițiile de maximă integritate profesională, imparțialitate și cunoștințe tehnice necesare, astfel cum se prevede în prezentul regulament. Raportul ar trebui să fie prezentat rețelelor EU-CyCLONe și CSIRT și Comisiei și să contribuie a activitatea acestora. În cazul în care incidentul se referă la o țară terță, acesta va fi, de asemenea, transmis de către Comisie Înaltului Reprezentant***, SEAE și oricărei***

misiuni PSAC din țara afectată de incident, prin intermediul sediului lor central.

Amendamentul 26

Propunere de regulament
Considerentul 37

Textul propus de Comisie	*Amendamentul*
(37) Având în vedere caracterul imprevizibil al atacurilor de securitate cibernetică și faptul că, adesea, acestea nu sunt limitate la o anumită zonă geografică și prezintă un risc ridicat de propagare, consolidarea rezilienței țărilor învecinate și a capacității lor de a răspunde în mod eficace la incidentele de securitate cibernetică semnificative și de mare amploare contribuie la protecția Uniunii în ansamblu. Prin urmare, țările terțe asociate la DEP ***pot fi*** sprijinite din rezerva UE pentru securitate cibernetică***, în cazul în care acest lucru este prevăzut în acordul de asociere la DEP respectiv***. Finanțarea pentru țările terțe asociate ar trebui să fie sprijinită de Uniune în cadrul parteneriatelor și al instrumentelor de finanțare relevante pentru țările respective. Sprijinul ar trebui să acopere serviciile din domeniul răspunsului la incidentele de securitate cibernetică semnificative sau de mare amploare și al redresării imediate în urma acestora. Condițiile stabilite pentru rezerva UE pentru securitate cibernetică și pentru furnizorii de încredere în prezentul regulament ar trebui să se aplice atunci când se acordă sprijin țărilor terțe asociate la DEP.	(37) Având în vedere caracterul imprevizibil al atacurilor de securitate cibernetică și faptul că, adesea, acestea nu sunt limitate la o anumită zonă geografică și prezintă un risc ridicat de propagare, consolidarea rezilienței țărilor învecinate***, îndeosebi Ucraina și Moldova,*** și a capacității lor de a răspunde în mod eficace la incidentele de securitate cibernetică semnificative și de mare amploare contribuie la protecția Uniunii în ansamblu. Prin urmare, țările terțe asociate la DEP ***ar trebui să fie*** sprijinite din rezerva UE pentru securitate cibernetică***. Sprijinul ar trebui să se aplice, de asemenea, țărilor terțe în care este desfășurată o misiune PSAC cu un mandat specific de întărire a rezilienței la amenințările hibride, inclusiv cele cibernetice, sau în care a fost adoptată o măsură de asistență a IEP pentru a întări reziliența cibernetică a țării***. Finanțarea pentru țările terțe asociate ar trebui să fie sprijinită de Uniune în cadrul parteneriatelor și al instrumentelor de finanțare relevante pentru țările respective. Sprijinul ar trebui să acopere serviciile din domeniul răspunsului la incidentele de securitate cibernetică semnificative sau de mare amploare și al redresării imediate în urma acestora. Condițiile stabilite pentru rezerva UE pentru securitate cibernetică și pentru furnizorii de încredere în prezentul regulament ar trebui să se aplice atunci când se acordă sprijin țărilor terțe asociate la DEP.

Amendamentul 27

Propunere de regulament
Articolul 1 – alineatul 1 – litera c

Textul propus de Comisie	*Amendamentul*
(c) instituirea unui mecanism european de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele semnificative sau de mare amploare.	(c) instituirea unui mecanism european de reexaminare a incidentelor de securitate cibernetică pentru a examina și a evalua incidentele ***sau amenințările*** semnificative sau de mare amploare.

Amendamentul 28

Propunere de regulament
Articolul 1 – alineatul 2 – litera a

Textul propus de Comisie	*Amendamentul*
(a) de a consolida detectarea și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel consolidarea poziției competitive a industriei și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la ***suveranitatea*** tehnologică a Uniunii în domeniul securității cibernetice;	(a) de a consolida detectarea și conștientizarea comună a situației la nivelul Uniunii cu privire la amenințările și incidentele de securitate cibernetică, permițând astfel consolidarea poziției competitive a industriei și a sectorului serviciilor din Uniune în întreaga economie digitală, și de a contribui la ***reziliența*** tehnologică a Uniunii în domeniul securității cibernetice;

Amendamentul 29

Propunere de regulament
Articolul 1 – alineatul 2 – litera b

Textul propus de Comisie	*Amendamentul*
(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau	(b) de a consolida gradul de pregătire al entităților care își desfășoară activitatea în sectoare critice și deosebit de critice din întreaga Uniune și de a consolida solidaritatea prin dezvoltarea unor capacități de răspuns comune la incidentele de securitate cibernetică semnificative sau

de mare amploare, inclusiv prin punerea la dispoziția țărilor terțe asociate la programul „Europa digitală” („DEP”) a sprijinului din partea UE pentru răspunsul la incidentele de securitate cibernetică;	de mare amploare, inclusiv prin punerea la dispoziția țărilor terțe asociate la programul „Europa digitală” („DEP”) ***sau a țărilor terțe care sunt candidate la aderare și care nu contravin intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în conformitate cu titlul V din TUE; Statele membre ar trebui să considere că un program activ de apărare cibernetică face parte din strategia lor națională în materie de securitate cibernetică, care include exerciții de instruire comune periodice între statele membre și între organizațiile internaționale. Un astfel de program ar trebui să ofere o capacitate în timp real, sincronizată, de a descoperi, detecta, analiza și atenua amenințările***;

Amendamentul 30

Propunere de regulament
Articolul 1 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. să reducă riscurile sistemice în materie de securitate cibernetică reprezentate de dependențele de echipamente critice din țări care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE;.

Amendamentul 31

Propunere de regulament
Articolul 2 – punctul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	„comunitate de apărare cibernetică” înseamnă autoritățile de apărare ale statelor membre și sprijinite de instituțiile,

organismele și agențiile UE, astfel cum se prevede în comunicarea comună privind politica UE în domeniul apărării cibernetice[1];

[1] Comunicare comună către Parlamentul European și Consiliu, Politica UE în domeniul apărării cibernetice, JOIN/2022/49 final

Amendamentul 32

Propunere de regulament
Articolul 3 – alineatul 2 – paragraful 1 – litera ba (nouă)

Textul propus de Comisie	*Amendamentul*
	(ba) să contribuie la modernizarea întregului sistem de apărare cibernetică, îmbunătățind calitatea capacităților de apărare cibernetică prin implementarea sistemelor de IA și să accelereze schimbul de informații între SOC naționale și SOC transfrontaliere;

Amendamentul 33

Propunere de regulament
Articolul 3 – alineatul 2 – paragraful 1 – litera da (nouă)

Textul propus de Comisie	*Amendamentul*
	(da) să examineze și să evalueze tehnologiile și echipamentele critice de securitate cibernetică utilizate de SOC pentru a răspunde la incidentele de securitate cibernetică în ceea ce privește riscurile sistemice generate de controlul exercitat de țări asupra furnizorilor cu risc ridicat, care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE.

Amendamentul 34

Propunere de regulament
Articolul 4 – alineatul 1 – paragraful 2

Textul propus de Comisie	*Amendamentul*
Acesta are capacitatea de a acționa ca punct de referință și punct de acces către alte organizații publice și private de la nivel național pentru colectarea și analizarea informațiilor privind amenințările și incidentele de securitate cibernetică și pentru contribuția la un SOC transfrontalier. Acesta este echipat cu tehnologii de ultimă generație capabile să detecteze, să reunească și să analizeze datele relevante pentru amenințările și incidentele de securitate cibernetică.	Acesta are capacitatea de a acționa ca punct de referință și punct de acces către alte organizații publice și private ***și, după caz, militar,*** de la nivel național pentru colectarea și analizarea informațiilor privind amenințările și incidentele de securitate cibernetică și pentru contribuția la un SOC transfrontalier. Acesta este echipat cu tehnologii de ultimă generație capabile să detecteze, să reunească și să analizeze datele relevante pentru amenințările și incidentele de securitate cibernetică.

Amendamentul 35

Propunere de regulament
Articolul 4 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. În urma unei cereri de exprimare a interesului, SOC naționale sunt selectate de către Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) pentru a participa la o achiziție de instrumente și infrastructuri în comun cu ECCC. ECCC poate acorda granturi SOC-urilor naționale selectate pentru a finanța funcționarea acestor instrumente și infrastructuri. Contribuția financiară a Uniunii acoperă până la 50 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de statul membru. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și SOC național încheie un acord de găzduire și utilizare care reglementează	2. În urma unei cereri de exprimare a interesului, SOC naționale sunt selectate de către Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică („ECCC”) pentru a participa la o achiziție de instrumente și infrastructuri în comun cu ECCC. ECCC poate acorda granturi SOC-urilor naționale selectate pentru a finanța funcționarea acestor instrumente și infrastructuri***, cu condiția strictă ca astfel de instrumente și infrastructuri să fie furnizate de furnizori de încredere în conformitate cu articolul 16***. Contribuția financiară a Uniunii acoperă până la 50 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de statul membru.

utilizarea instrumentelor și a infrastructurilor.	Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și SOC național încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.

Amendamentul 36

Propunere de regulament
Articolul 5 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. În urma unei cereri de exprimare a interesului, un consorțiu-gazdă este selectat de către ECCC pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC. ECCC poate acorda un grant consorțiului-gazdă pentru a finanța funcționarea instrumentelor și a infrastructurilor. Contribuția financiară a Uniunii acoperă până la 75 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de către consorțiul-gazdă. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și consorțiul-gazdă încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.	2. În urma unei cereri de exprimare a interesului, un consorțiu-gazdă este selectat de către ECCC pentru a participa la o achiziție comună de instrumente și infrastructuri cu ECCC. ECCC poate acorda un grant consorțiului-gazdă pentru a finanța funcționarea instrumentelor și a infrastructurilor***, cu condiția strictă ca astfel de instrumente și infrastructuri să fie furnizate de furnizori de încredere în conformitate cu articolul 16***. Contribuția financiară a Uniunii acoperă până la 75 % din costurile de achiziție a instrumentelor și infrastructurilor și până la 50 % din costurile de funcționare, restul costurilor urmând să fie acoperite de către consorțiul-gazdă. Înainte de lansarea procedurii de achiziție a instrumentelor și a infrastructurilor, ECCC și consorțiul-gazdă încheie un acord de găzduire și utilizare care reglementează utilizarea instrumentelor și a infrastructurilor.

Amendamentul 37

Propunere de regulament
Articolul 5 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. Orice infrastructură sau furnizor originar dintr-o țară terță cu grad ridicat

de risc este exclus în mod automat.

Amendamentul 38

Propunere de regulament
Articolul 6 – alineatul 1 – litera ba (nouă)

Textul propus de Comisie	*Amendamentul*
	(ba) sprijină în mod direct întărirea capacităților militare și de apărare ale membrilor participanți sau împiedică o amenințare directă și iminentă la adresa securității acestora. Deși exploatarea vulnerabilităților din sectorul apărării poate cauza perturbări și daune semnificative, securitatea cibernetică a sectorului apărării necesită măsuri speciale pentru a asigura securitatea lanțurilor de aprovizionare, îndeosebi a entităților aflate în poziții inferioare în lanțurile de aprovizionare, care nu necesită acces la informații clasificate, dar care ar putea prezenta riscuri grave pentru întregul sector. Ar trebui să se acorde o atenție deosebită impactului oricărei încălcări și amenințării cu o eventuală manipulare a datelor de rețea care ar putea face ca mijloacele de apărare esențiale să devină inutile sau chiar să le neutralizeze sistemele de operare, făcându-le vulnerabile la acte de piraterie.

Amendamentul 39

Propunere de regulament
Articolul 6 – alineatul 1 – litera bb (nouă)

Textul propus de Comisie	*Amendamentul*
	(bb) sprijină întărirea capacităților de apărare ale membrilor participanți sau împiedică o amenințare directă și iminentă la adresa securității acestora, asigurând securitatea lanțurilor de aprovizionare, în special a acelor entități

	aflate la un nivel inferior în lanțurile de aprovizionare, care nu necesită acces la informații clasificate, dar care ar putea implica riscuri grave pentru întregul sector.

Amendamentul 40

Propunere de regulament
Articolul 7 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. În cazul în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea furnizează, fără întârzieri nejustificate, informații relevante rețelelor EU-CyCLONe și CSIRT și Comisiei, având în vedere rolurile lor respective de gestionare a crizelor în conformitate cu Directiva (UE) 2022/2555.	1. În cazul în care SOC-urile transfrontaliere obțin informații referitoare la un incident de securitate cibernetică de mare amploare potențial sau în curs, acestea furnizează, fără întârzieri nejustificate, informații relevante rețelelor EU-CyCLONe și CSIRT și Comisiei, ***inclusiv Înaltului Reprezentant și SEAE atunci când se referă la o țară terță,*** având în vedere rolurile lor respective de gestionare a crizelor în conformitate cu Directiva (UE) 2022/2555.

Amendamentul 41

Propunere de regulament
Articolul 8 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Statele membre care participă la Scutul cibernetic european asigură un nivel ridicat de securitate a datelor și de securitate fizică a infrastructurii Scutului cibernetic european și se asigură că infrastructura este gestionată și controlată în mod adecvat, astfel încât să fie protejată de amenințări și să se garanteze securitatea sa și a sistemelor, inclusiv ***a*** datelor schimbate prin intermediul infrastructurii.	1. Statele membre care participă la Scutul cibernetic european asigură un nivel ridicat de securitate a datelor și de securitate fizică a infrastructurii Scutului cibernetic european și se asigură că infrastructura este gestionată și controlată în mod adecvat, astfel încât să fie protejată de amenințări și să se garanteze securitatea sa și a sistemelor, ***reducerea riscurilor și promovarea avantajului tehnologic al UE în sectoarele critice,*** inclusiv ***măsuri de restricționare sau excludere a furnizorilor cu grad ridicat de risc, precum și de protejare a securității*** datelor schimbate

prin intermediul infrastructurii.

Amendamentul 42

Propunere de regulament
Articolul 8 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Statele membre care participă la Scutul cibernetic european se asigură că schimbul de informații în cadrul Scutului cibernetic european cu entități care nu sunt organisme publice ale statelor membre nu afectează în mod negativ interesele de securitate ale Uniunii.	2. Statele membre care participă la Scutul cibernetic european se asigură că schimbul de informații în cadrul Scutului cibernetic european cu entități care nu sunt organisme publice ale statelor membre nu afectează în mod negativ interesele de securitate ale Uniunii ***și că orice schimb de informații cu furnizorii cu grad ridicat de risc are un domeniu de aplicare limitat și nu aduce atingere intereselor strategice și de securitate ale Uniunii***.

Amendamentul 43

Propunere de regulament
Articolul 8 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice pentru ca statele membre să își respecte obligațiile care le revin în temeiul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament. În acest sens, Comisia, sprijinită de Înaltul Reprezentant, ține seama de standardele de securitate relevante la nivel de apărare, pentru a facilita cooperarea cu actorii militari.	3. Comisia poate adopta acte de punere în aplicare de stabilire a cerințelor tehnice pentru ca statele membre să își respecte obligațiile care le revin în temeiul alineatelor (1) și (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 21 alineatul (2) din prezentul regulament. În acest sens, Comisia, sprijinită de Înaltul Reprezentant, ține seama de standardele de securitate relevante la nivel de apărare, pentru a facilita cooperarea cu actorii militari***, utilizând în mod adecvat întreaga gamă de opțiuni defensive aflate la dispoziția comunităților civile și militare pentru securitatea și apărarea mai largă a UE, și informează Parlamentul European***.

Amendamentul 44

Propunere de regulament
Articolul 9 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Acțiunile de punere în aplicare a mecanismului pentru situații de urgență cibernetică sunt sprijinite prin finanțare din DEP și sunt puse în aplicare în conformitate cu Regulamentul (UE) 2021/694, în special cu obiectivul specific nr. 3.	2. Acțiunile de punere în aplicare a mecanismului pentru situații de urgență cibernetică sunt sprijinite prin finanțare din DEP și sunt puse în aplicare în conformitate cu Regulamentul (UE) 2021/694, în special cu obiectivul specific nr. 3***, și prin Instrumentul european pentru pace (IEP), atunci când furnizează măsuri de asistență țărilor terțe, îndeosebi Ucrainei și Moldovei;***

Amendamentul 45

Propunere de regulament
Articolul 10 – alineatul 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice în cadrul Uniunii;	(a) acțiuni de pregătire, inclusiv testarea coordonată a pregătirii entităților care își desfășoară activitatea în sectoare deosebit de critice***, cum ar fi infrastructura publică, infrastructura electorală, transporturile, asistența medicală, finanțele, telecomunicațiile, aprovizionarea cu alimente și securitatea*** în cadrul Uniunii;

Amendamentul 46

Propunere de regulament
Articolul 10 – alineatul 1 – litera c

Textul propus de Comisie	*Amendamentul*
(c) acțiuni de asistență reciprocă constând în furnizarea de asistență din partea autorităților naționale ale unui stat	(c) acțiuni de asistență reciprocă constând în furnizarea de asistență din partea autorităților naționale ale unui stat

membru unui alt stat membru, în special astfel cum se prevede la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555.	membru unui alt stat membru, în special astfel cum se prevede la articolul 11 alineatul (3) litera (f) din Directiva (UE) 2022/2555 ***și în contextul articolului 42 alineatul (7) din TUE și al articolului 222 din TFUE;***

Amendamentul 47

Propunere de regulament
Articolul 10 – alineatul 1 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) înlocuirea și eliminarea treptată a echipamentelor critice provenite de la furnizorii cu risc ridicat, ceea ce ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE;

Amendamentul 48

Propunere de regulament
Articolul 11 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Grupul de cooperare NIS, în colaborare cu Comisia, ENISA ***și*** Înaltul Reprezentant, elaborează scenarii de risc și metodologii comune pentru exercițiile de testare coordonate.	2. Grupul de cooperare NIS, în colaborare cu Comisia, ENISA***,*** Înaltul Reprezentant, ***SEAE și, după caz, AEA,*** elaborează scenarii de risc și metodologii comune pentru exercițiile de testare coordonate.

Amendamentul 49

Propunere de regulament
Articolul 12 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Rezerva UE pentru securitate cibernetică constă în servicii de răspuns la	2. Rezerva UE pentru securitate cibernetică constă în servicii de răspuns la

incidente furnizate de furnizori de încredere selectați în conformitate cu criteriile prevăzute la articolul 16. Rezerva include servicii angajate în prealabil. Serviciile trebuie să poată fi desfășurate în toate statele membre.	incidente furnizate de furnizori de încredere selectați în conformitate cu criteriile prevăzute la articolul 16. Rezerva include servicii angajate în prealabil. Serviciile trebuie să poată fi desfășurate în toate statele membre ***și în țările terțe care îndeplinesc cerințele aplicabile ale prezentului regulament***.

Amendamentul 50

Propunere de regulament
Articolul 12 – alineatul 3 – litera b

Textul propus de Comisie	*Amendamentul*
(b) instituțiile, organele și agențiile Uniunii.	(b) instituțiile, organele și agențiile Uniunii***, inclusiv misiunile PSAC***.

Amendamentul 51

Propunere de regulament
Articolul 12 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Utilizatorii menționați la alineatul (3) litera (a) utilizează serviciile din rezerva UE pentru securitate cibernetică pentru a răspunde sau a oferi sprijin pentru răspunsul la incidentele semnificative sau de mare amploare care afectează entitățile care își desfășoară activitatea în sectoare critice sau deosebit de critice ***și pentru redresarea imediată în urma acestora***.	4. Utilizatorii menționați la alineatul (3) litera (a) utilizează serviciile din rezerva UE pentru securitate cibernetică pentru a răspunde sau a oferi sprijin pentru răspunsul la incidentele semnificative sau de mare amploare care afectează entitățile care își desfășoară activitatea în sectoare critice sau deosebit de critice***, precum infrastructura publică, infrastructura electorală, transporturile, asistența medicală, finanțele, telecomunicațiile, aprovizionarea cu alimente și securitatea***.

Amendamentul 52

Propunere de regulament
Articolul 12 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Comisia are responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică. Comisia stabilește prioritățile și evoluția rezervei UE pentru securitate cibernetică, în conformitate cu cerințele utilizatorilor menționați la alineatul (3), supraveghează punerea sa în aplicare și asigură complementaritatea, coerența, sinergiile și legăturile cu alte acțiuni de sprijin în temeiul prezentului regulament, precum și cu alte acțiuni ***și*** programe ale Uniunii.	5. Comisia are responsabilitatea generală pentru punerea în aplicare a rezervei UE pentru securitate cibernetică. Comisia stabilește prioritățile și evoluția rezervei UE pentru securitate cibernetică, în conformitate cu cerințele utilizatorilor menționați la alineatul (3), supraveghează punerea sa în aplicare și asigură complementaritatea, coerența, sinergiile și legăturile cu alte acțiuni de sprijin în temeiul prezentului regulament, precum și cu alte acțiuni***,*** programe ***și obiective*** ale Uniunii***, în special obiectivul strategic de reducere a dependenței de furnizorii cu risc ridicat, care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în temeiul titlului V din TUE***.

Amendamentul 53

Propunere de regulament
Articolul 12 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. Pentru a sprijini Comisia în instituirea rezervei UE pentru securitate cibernetică, ENISA elaborează o cartografiere a serviciilor necesare, după consultarea statelor membre și a Comisiei. ENISA elaborează o cartografiere similară, după consultarea Comisiei, pentru a identifica nevoile țărilor terțe eligibile pentru sprijin din rezerva UE pentru securitate cibernetică în temeiul articolului 17. După caz, Comisia consultă Înaltul Reprezentant.	7. Pentru a sprijini Comisia în instituirea rezervei UE pentru securitate cibernetică, ENISA elaborează o cartografiere a serviciilor necesare, după consultarea statelor membre și a Comisiei. ENISA elaborează o cartografiere similară, după consultarea Comisiei, pentru a identifica nevoile țărilor terțe eligibile pentru sprijin din rezerva UE pentru securitate cibernetică în temeiul articolului 17***, cu sprijinul SEAE***. După caz, Comisia consultă Înaltul Reprezentant.

Amendamentul 54

Propunere de regulament
Articolul 14 – alineatul 2 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) impactul incidentului asupra securității și a apărării Uniunii;

Amendamentul 55

Propunere de regulament
Articolul 15 – alineatul 3

Textul propus de Comisie	*Amendamentul*
3. În consultare cu Înaltul Reprezentant, sprijinul acordat în cadrul mecanismului pentru situații de urgență cibernetică poate completa asistența acordată în contextul politicii externe și de securitate comune și al politicii de securitate și apărare comune, inclusiv prin intermediul echipelor de răspuns rapid în domeniul cibernetic. De asemenea, acesta poate completa asistența acordată de un stat membru unui alt stat membru în contextul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană sau poate contribui la aceasta.	3. În consultare cu Înaltul Reprezentant, sprijinul acordat în cadrul mecanismului pentru situații de urgență cibernetică poate completa asistența acordată în contextul politicii externe și de securitate comune și al politicii de securitate și apărare comune, inclusiv prin intermediul echipelor de răspuns rapid în domeniul cibernetic ***(CRRT), cu scopul de a sprijini mai bine statele membre ale UE, misiunile și operațiunile PSAC și țările terțe aliniate la politica externă și de securitate comună a UE și la politica de securitate și apărare comună în eforturile lor de consolidare a capacităților de apărare cibernetică, îndeosebi Ucraina și Moldova***. De asemenea, acesta poate completa asistența acordată de un stat membru unui alt stat membru în contextul articolului 42 alineatul (7) din Tratatul privind Uniunea Europeană sau poate contribui la aceasta.

Amendamentul 56

Propunere de regulament
Articolul 16 – alineatul 2 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) furnizorul demonstrează că structurile sale decizionale și de gestionare nu sunt supuse niciunei influențe necuvenite din partea

	guvernelor statelor, ceea ce ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum se prevede în cadrul PESC în temeiul titlului V din TUE;

Amendamentul 57

Propunere de regulament
Articolul 16 – alineatul 2 – litera f

Textul propus de Comisie	*Amendamentul*
(f) furnizorul este dotat cu echipamentele tehnice hardware și software necesare pentru a sprijini serviciul solicitat;	(f) furnizorul este dotat cu echipamentele tehnice hardware și software necesare pentru a sprijini serviciul solicitat ***și îndeplinește cerințele prevăzute la articolul X din Regulamentul XX/XXXX (Actul privind reziliența cibernetică)***;

Amendamentul 58

Propunere de regulament
Articolul 16 – alineatul 2 – litera ja (nouă)

Textul propus de Comisie	*Amendamentul*
	(ja) Nu poate fi admis niciun furnizor originar dintr-o țară terță cu grad ridicat de risc.

Amendamentul 59

Propunere de regulament
Articolul 16 – alineatul 2 – litera jb (nouă)

Textul propus de Comisie	*Amendamentul*
	(jb) furnizorul este în strânsă cooperare cu IMM-urile relevante, dacă este posibil;

Amendamentul 60

Propunere de regulament
Articolul 17 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. Țările terțe pot solicita sprijin din rezerva UE pentru securitate cibernetică în cazul în care acordurile de asociere încheiate cu privire la participarea lor la DEP prevăd acest lucru.	1. Țările terțe pot solicita sprijin din rezerva UE pentru securitate cibernetică în cazul în care***:***
	(a) acordurile de asociere încheiate cu privire la participarea lor la DEP prevăd acest lucru***;***
	(b) țările terțe în care este desfășurată o misiune PSAC cu un mandat specific pentru a întări reziliența la amenințările hibride, inclusiv cele cibernetice, sau în care a fost adoptată o măsură de asistență a IEP pentru a întări reziliența cibernetică a țării.

Amendamentul 61

Propunere de regulament
Articolul 17 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Sprijinul din rezerva UE pentru securitate cibernetică este în conformitate cu prezentul regulament și respectă toate condițiile specifice prevăzute în acordurile de asociere menționate la ***alineatul (1)***.	2. Sprijinul din rezerva UE pentru securitate cibernetică este în conformitate cu prezentul regulament și respectă toate condițiile specifice prevăzute în acordurile de asociere menționate la ***alineat***, ***cu excepția țărilor terțe care fac obiectul dispozițiilor prevăzute la alineatul (1) litera (b)***.

Amendamentul 62

Propunere de regulament
Articolul 18 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. La cererea Comisiei, a EU-CyCLONe sau a rețelei CSIRT, ENISA analizează și evaluează amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un incident specific de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și a unei evaluări a unui incident, ENISA transmite rețelei CSIRT, EU-CyCLONe și Comisiei un raport de evaluare a incidentelor, pentru a le sprijini în îndeplinirea sarcinilor care le revin, având-le în vedere în special pe cele prevăzute la articolele 15 și 16 din Directiva (UE) 2022/2555. Dacă este cazul, Comisia transmite raportul Înaltului Reprezentant.	1. La cererea Comisiei, a EU-CyCLONe sau a rețelei CSIRT, ENISA analizează și evaluează amenințările, vulnerabilitățile și acțiunile de atenuare în ceea ce privește un incident specific de securitate cibernetică semnificativ sau de mare amploare. După finalizarea unei analize și a unei evaluări a unui incident, ENISA transmite rețelei CSIRT, EU-CyCLONe și Comisiei un raport de evaluare a incidentelor, pentru a le sprijini în îndeplinirea sarcinilor care le revin, având-le în vedere în special pe cele prevăzute la articolele 15 și 16 din Directiva (UE) 2022/2555. Dacă este cazul, ***în special atunci când incidentul se referă la o țară terță,*** Comisia transmite raportul Înaltului Reprezentant ***și SEAE***.

Amendamentul 63

Propunere de regulament
Articolul 18 – alineatul 3 a (nou)

Textul propus de Comisie	*Amendamentul*
	3a. Raportul este transmis Parlamentului European în concordanță cu dreptul Uniunii sau cu dreptul intern în domeniul protecției informațiilor sensibile clasificate.

Amendamentul 64

Propunere de regulament
Articolul 19 – paragraful 1 – punctul 1 – litera a – punctul 1 (nou)
Regulamentului (UE) 2021/694
Articolul 6 – alineatul 1

Textul propus de Comisie	*Amendamentul*
(aa) sprijinirea dezvoltării unui Scut cibernetic al UE, inclusiv dezvoltarea, implementarea și operarea platformelor	(aa) sprijinirea dezvoltării unui Scut cibernetic al UE, inclusiv dezvoltarea, implementarea și operarea platformelor

SOC naționale și transfrontaliere care contribuie la conștientizarea situației în Uniune și la consolidarea capacităților de informații privind amenințările cibernetice ale Uniunii;	SOC naționale și transfrontaliere care contribuie la conștientizarea situației în Uniune și la consolidarea capacităților de informații privind amenințările cibernetice ale Uniunii ***și reducerea dependenței Uniunii de furnizorii cu grad ridicat de risc de echipamente sau componente critice de securitate cibernetică care ar contraveni intereselor de securitate și apărare ale Uniunii și ale statelor sale membre, astfel cum au fost stabilite în cadrul PESC în conformitate cu titlul V din TUE***;

Amendamentul 65

Propunere de regulament
Articolul 20 – paragraful 1

Textul propus de Comisie	*Amendamentul*
Până la [***patru*** ani de la data de la care se aplică prezentul regulament] Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament.	Până la [***trei*** ani de la data de la care se aplică prezentul regulament ***și, ulterior, o dată la doi ani***], Comisia transmite Parlamentului European și Consiliului un raport privind evaluarea și reexaminarea prezentului regulament.

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Stabilirea unor măsuri de consolidare a solidarității și a capacităților de la nivelul Uniunii pentru detectarea amenințărilor și a incidentelor de securitate cibernetică, pregătirea legată de acestea și contracararea lor
Referințe	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Comisie competentă Data anunțului în plen	ITRE 1.6.2023
Aviz emis de către Data anunțului în plen	AFET 1.6.2023
Raportor pentru aviz Data numirii	Dragoş Tudorache 16.6.2023
Examinare în comisie	18.9.2023
Data adoptării	24.10.2023
Rezultatul votului final	+: 39 –: 4 0: 0
Membri titulari prezenți la votul final	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
Membri supleanți prezenți la votul final	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

VOT FINAL PRIN APEL NOMINAL ÎN COMISIA SESIZATĂ PENTRU AVIZ

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

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri