Europos Parlamentas
2019-2024

Užsienio reikalų komitetas

2023/0109(COD)

27.10.2023

NUOMONĖ

Užsienio reikalų komiteto

pateikta Pramonės, mokslinių tyrimų ir energetikos komitetui

dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonės
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Nuomonės referentas: Dragoş Tudorache

PA_Legam

Pakeitimas 1

Pasiūlymas dėl reglamento
1 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(1) informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo esminiais visų ekonominės veiklos sektorių aspektais, nes mūsų viešojo administravimo institucijos, įmonės ir piliečiai įvairiuose sektoriuose ir įvairiose valstybėse labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, nei bet kada anksčiau;	(1) informacinių ir ryšių technologijų naudojimas ir priklausomumas nuo jų tapo esminiais visų ekonominės ***ir karinės*** veiklos sektorių aspektais, nes mūsų viešojo administravimo institucijos, įmonės ir piliečiai***, taip pat kariniai ir gynybos subjektai*** įvairiuose sektoriuose ir įvairiose valstybėse labiau susieti tarpusavyje ir vieni nuo kitų priklausomi, nei bet kada anksčiau;

Pakeitimas 2

Pasiūlymas dėl reglamento
2 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinė įranga arba veiklos sutrikdymas, mastas, dažnumas ir poveikis didėja. Tai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Turint omenyje sparčiai kintančias grėsmių aplinkybes, dėl galimų didelio masto incidentų, dėl kurių gali kilti didelių sutrikimų ar būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti parengtį visais Sąjungos kibernetinio saugumo sistemos lygmenimis. ***Ši grėsmė*** yra ***susijusi*** ne vien su Rusijos karine agresija prieš Ukrainą ir, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų. Tokie incidentai gali trukdyti teikti viešąsias paslaugas ir vykdyti ekonominę veiklą, be kita ko, ypatingos svarbos ar itin	(2) kibernetinio saugumo incidentų, įskaitant tiekimo grandinės išpuolius, kurių tikslas – kibernetinis šnipinėjimas, išpirkos reikalavimo programinė įranga arba veiklos sutrikdymas, mastas, dažnumas ir poveikis didėja. Tai kelia didelę grėsmę tinklų ir informacinių sistemų veikimui. Turint omenyje sparčiai kintančias grėsmių aplinkybes, dėl galimų didelio masto incidentų, dėl kurių gali kilti didelių sutrikimų ar būti padaryta žala ypatingos svarbos infrastruktūros objektams, grėsmės reikia didinti parengtį visais Sąjungos kibernetinio saugumo sistemos lygmenimis. ***Šių grėsmių rimtumas tapo dar aktualesnis, nes mūsų žemyne vėl prasidėjo karas. Šios grėsmės*** yra ***susijusios*** ne vien su Rusijos karine agresija prieš Ukrainą ir, tikėtina, išliks, atsižvelgiant į tai, kad dabartinę geopolitinę įtampą lemia daugybė su valstybe susijusių subjektų, nusikaltėlių ir įsilaužėlių aktyvistų. Tokie incidentai gali

svarbiuose sektoriuose, sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelės žalos Sąjungos ekonomikai ir jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei. Be to, kibernetinio saugumo incidentai yra nenuspėjami, nes dažnai kyla ir išsiplėtoja per labai trumpą laiką, nėra susiję su jokia konkrečia geografine teritorija ir vyksta vienu metu arba akimirksniu išplinta daugelyje šalių;	trukdyti teikti viešąsias paslaugas ir vykdyti ekonominę veiklą, be kita ko, ypatingos svarbos ar itin svarbiuose sektoriuose, sukelti didelių finansinių nuostolių, pakenkti naudotojų pasitikėjimui, padaryti didelės žalos Sąjungos ekonomikai ir ***saugumui ir*** jų padariniai gali būti pavojingi net žmonių sveikatai ar gyvybei***, galimai pakenkdami su vietos ar nacionaliniu saugumu susijusiems įrenginiams***. Be to, kibernetinio saugumo incidentai yra nenuspėjami, nes dažnai kyla ir išsiplėtoja per labai trumpą laiką, nėra susiję su jokia konkrečia geografine teritorija ir vyksta vienu metu arba akimirksniu išplinta daugelyje šalių; ***kibernetinis saugumas yra svarbus siekiant apsaugoti mūsų europines vertybes ir užtikrinti mūsų demokratijos veikimą apsaugant mūsų rinkimų infrastruktūrą ir demokratines procedūras nuo užsienio šalių kišimosi;***

Pakeitimas 3

Pasiūlymas dėl reglamento
2 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(2a) kibernetinis saugumas yra labai svarbus siekiant užtikrinti, kad mūsų Sąjunga būtų saugi, ir neleisti, kad piktavaliai valstybiniai ir nevalstybiniai subjektai pakenktų mūsų demokratijai, ekonomikai ir saugumui. Svarbu užkirsti kelią sistemos susiskaidymui, nes tokia padėtis nebūtų tinkama, ypač susidūrus su iššūkiais, keliamais būsimų didelio masto kibernetinių išpuolių, nukreiptų prieš kelias valstybes nares tuo pačiu metu arba ypatingos svarbos tarpvalstybinę infrastruktūrą. Todėl reikalinga ES įstaiga, kuri veiktų kaip visų esamų ir būsimų kibernetinio saugumo priemonių, fondų ir mechanizmų koordinavimo platforma;

Pakeitimas 4

Pasiūlymas dėl reglamento
3 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(3) būtina stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį skaitmeninėje ekonomikoje ir remti jų skaitmeninę transformaciją, didinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Kaip rekomenduojama trijuose skirtinguose Konferencijos dėl Europos ateities[16] pasiūlymuose, būtina didinti piliečių, įmonių ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas, kurios padėtų greičiau aptikti kibernetinio saugumo grėsmes bei incidentus ir į juos reaguoti, o valstybėms narėms reikia pagalbos geriau pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. Sąjunga taip pat turėtų didinti savo pajėgumus ***šiose srityse***, visų pirma susijusius su duomenų apie kibernetinio saugumo grėsmes ir incidentus rinkimu ir analize;	(3) būtina stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį skaitmeninėje ekonomikoje ir remti jų skaitmeninę transformaciją, didinant kibernetinio saugumo lygį bendrojoje skaitmeninėje rinkoje. Kaip rekomenduojama trijuose skirtinguose Konferencijos dėl Europos ateities[16] pasiūlymuose, būtina didinti piliečių, įmonių ir subjektų, valdančių ypatingos svarbos infrastruktūros objektus, atsparumą didėjančioms kibernetinio saugumo grėsmėms, kurios gali turėti pražūtingą poveikį visuomenei ir ekonomikai. Todėl reikia investuoti į infrastruktūrą ir paslaugas, kurios padėtų greičiau aptikti kibernetinio saugumo grėsmes bei incidentus ir į juos reaguoti, o valstybėms narėms reikia pagalbos geriau pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir į juos reaguoti. ***Šiose srityse*** Sąjunga taip pat turėtų didinti savo pajėgumus, visų pirma susijusius su duomenų apie kibernetinio saugumo grėsmes ir incidentus rinkimu ir analize ***bei gebėjimu reaguoti į kibernetinio saugumo grėsmes ir incidentus, taip pat savo gebėjimą aktyviai veikti ir ryžtingai reaguoti į kibernetinio saugumo grėsmes ir incidentus***;
[16] https://futureu.europa.eu/lt/	[16] https://futureu.europa.eu/lt/

Pakeitimas 5

Pasiūlymas dėl reglamento
4 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(4) Sąjunga jau ėmėsi tam tikrų priemonių, kuriomis siekiama sumažinti ypatingos svarbos infrastruktūros objektų ir subjektų pažeidžiamumą ir padidinti jų atsparumą kibernetinio saugumo rizikai, visų pirma priėmė Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[17], Komisijos rekomendaciją (ES) 2017/1584[18], Europos Parlamento ir Tarybos direktyvą 2013/40/ES[19] ir Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[20]. Be to, Tarybos rekomendacijoje dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, veiksmingai, solidariai bei koordinuotai bendradarbiauti tarpusavyje, su Komisija ir kitomis atitinkamomis valdžios institucijomis bei atitinkamais subjektais, siekiant padidinti ypatingos svarbos infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą;	(4) Sąjunga jau ėmėsi tam tikrų priemonių, kuriomis siekiama sumažinti ypatingos svarbos infrastruktūros objektų ir subjektų pažeidžiamumą ir padidinti jų atsparumą kibernetinio saugumo rizikai, visų pirma priėmė Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555[17], Komisijos rekomendaciją (ES) 2017/1584[18], Europos Parlamento ir Tarybos direktyvą 2013/40/ES[19] ir Europos Parlamento ir Tarybos reglamentą (ES) 2019/881[20]. Be to, Tarybos rekomendacijoje dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą valstybės narės raginamos imtis skubių ir veiksmingų priemonių ir lojaliai, veiksmingai ***ir iniciatyviai***, solidariai bei koordinuotai bendradarbiauti tarpusavyje, su Komisija ir kitomis atitinkamomis valdžios institucijomis bei atitinkamais subjektais, siekiant padidinti ypatingos svarbos infrastruktūros objektų, naudojamų esminėms paslaugoms vidaus rinkoje teikti, atsparumą***. Be to, 2022 m. kovo mėn. Sąjunga patvirtino ir paskelbė savo saugumo ir gynybos strateginį kelrodį, kuriame daugiausia dėmesio skiriama, inter alia, kibernetinio saugumo stiprinimui ir tarptautinio bendradarbiavimo su panašiai mąstančiais sąjungininkais ir demokratiniais partneriais stiprinimui, ypač šiuo klausimu. Kibernetinis saugumas taip pat buvo neseniai paskelbtos 2023 m. sausio mėn. trečiosios bendrosios deklaracijos dėl ES ir NATO bendradarbiavimo esminis aspektas. ES ir NATO darbo grupės galutinėje vertinimo ataskaitoje rekomenduojama visapusiškai išnaudoti ES ir NATO veiksmų sąveiką[1], įskaitant civilinių ir karinių subjektų keitimąsi geriausios praktikos pavyzdžiais, susijusiais su atitinkamos kibernetinio saugumo politikos ir teisės**

	aktų įgyvendinimu*;*
	[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en
[17] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (OL L 333, 2022 12 27).	[17] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (OL L 333, 2022 12 27).
[18] 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).	[18] 2017 m. rugsėjo 13 d. Komisijos rekomendacija (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes (OL L 239, 2017 9 19, p. 36).
[19] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).	[19] 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR (OL L 218, 2013 8 14, p. 8).
[20] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).	[20] 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15).

Pakeitimas 6

Pasiūlymas dėl reglamento
6 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(6) 2022 m. lapkričio 10 d. priimtame bendrame komunikate dėl ES kibernetinės	(6) 2022 m. lapkričio 10 d. priimtame bendrame komunikate dėl ES kibernetinės

gynybos politikos[22] paskelbta ES kibernetinio solidarumo iniciatyva, kuria siekiama šių tikslų: stiprinti bendrus ES aptikimo, informuotumo apie padėtį ir reagavimo pajėgumus, skatinant diegti ES saugumo operacijų centrų (toliau – SOC) infrastruktūrą, remiant laipsnišką ES lygmens kibernetinio saugumo rezervo kūrimą, pasitelkiant patikimų privačių paslaugų teikėjų paslaugas ir, remiantis ES rizikos vertinimais, atlikti ypatingos svarbos subjektų galimų pažeidžiamumų testavimą;	gynybos politikos[22] paskelbta ES kibernetinio solidarumo iniciatyva, kuria siekiama šių tikslų: stiprinti bendrus ES aptikimo, informuotumo apie padėtį ir reagavimo pajėgumus, skatinant diegti ES saugumo operacijų centrų (toliau – SOC) infrastruktūrą, remiant laipsnišką ES lygmens kibernetinio saugumo rezervo kūrimą, pasitelkiant patikimų privačių paslaugų teikėjų paslaugas ir, remiantis ES rizikos vertinimais, atlikti ypatingos svarbos subjektų galimų pažeidžiamumų testavimą; ***Be to, kaip pabrėžiama Tarybos išvadose dėl ES kibernetinės gynybos politikos[1], greitai kintant kibernetinių grėsmių aplinkai ir sparčiai vystantis technologijoms taip pat matyti, kad reikia stiprinti civilinį ir karinį koordinavimą ir bendradarbiavimą;***
	[1] Tarybos išvados dėl ES kibernetinės gynybos politikos, kurias Taryba patvirtino savo 2023 m. gegužės 22 d. posėdyje (dok. 9618/23).
[22] Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022) 49 final.	[22] Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022) 49 final.

Pakeitimas 7

Pasiūlymas dėl reglamento
6 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(6a) atsižvelgiant į nykstančias ribas tarp civilinių ir karinių sričių, taip pat dvejopą kibernetinių priemonių ir technologijų naudojimą, būtina laikytis visapusiško ir holistinio požiūrio į skaitmeninę sritį. Įvykus didelio masto kibernetinio saugumo incidentui ir krizei, apimantiems daugiau kaip vieną valstybę narę, turėtų būti nustatytas tinkamas krizių valdymo mechanizmas. Tokios struktūros turėtų organizuoti keitimąsi

	informacija, veiksmų koordinavimą ir bendradarbiavimą su Sąjungos išorės saugumo ir karinių krizių valdymo struktūromis bei valstybių narių įstaigomis, atsakingomis už saugumą ir gynybą (kibernetinės gynybos bendruomene). Tai taip pat turėtų būti taikoma bendros saugumo ir gynybos politikos operacijoms ir misijoms, kurias Sąjunga vykdo siekdama užtikrinti taiką ir stabilumą kaimyninėse šalyse ir už jų ribų;

Pakeitimas 8

Pasiūlymas dėl reglamento
7 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(7) būtina stiprinti kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį visoje Sąjungoje, taip pat stiprinti solidarumą didinant valstybių narių ir Sąjungos parengtį bei pajėgumus reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus. Taigi turėtų būti įdiegta Europos masto SOC infrastruktūra (Europos kibernetinio saugumo skydas) siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį gebėjimus, reikėtų sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą siekiant padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, į juos reaguoti ir nedelsiant po jų atkurti veiklą, turėtų būti sukurtas Kibernetinio saugumo incidentų peržiūros mechanizmas, kad būtų galima peržiūrėti ir įvertinti konkrečius reikšmingus arba didelio masto incidentus. Šie veiksmai nedaro poveikio Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 107 ir 108 straipsniams;	(7) būtina stiprinti kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį visoje Sąjungoje, taip pat stiprinti solidarumą didinant valstybių narių ir Sąjungos parengtį bei pajėgumus reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus. Taigi turėtų būti įdiegta Europos masto SOC infrastruktūra (Europos kibernetinio saugumo skydas) siekiant sukurti ir sustiprinti bendrus aptikimo ir informuotumo apie padėtį gebėjimus, reikėtų sukurti Reagavimo į kibernetinio saugumo krizes mechanizmą siekiant padėti valstybėms narėms pasirengti reikšmingiems ir didelio masto kibernetinio saugumo incidentams, ***įskaitant incidentus, kurie yra susiję su daugiau nei viena valstybe nare,*** į juos reaguoti ir nedelsiant po jų atkurti veiklą***. Kai įmanoma ir reikalinga***, ***Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų rengti keitimosi informacija bendradarbiavimo su valstybių narių gynybos institucijomis renginius ir jį turėtų remti ES institucijos, įstaigos ir agentūros (ES kibernetinės gynybos bendruomenė);*** turėtų būti sukurtas Kibernetinio saugumo incidentų

	peržiūros mechanizmas, kad būtų galima peržiūrėti ir įvertinti konkrečius reikšmingus arba didelio masto incidentus***.*** ***Tokiomis naujomis struktūromis taip pat turėtų būti remiamos ES BSGP operacijos ir misijos***. Šie veiksmai nedaro poveikio Sutarties dėl Europos Sąjungos veikimo (toliau – SESV) 107 ir 108 straipsniams;

Pakeitimas 9

Pasiūlymas dėl reglamento
11 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(11) siekiant patikimo finansų valdymo, reikėtų nustatyti konkrečias taisykles dėl nepanaudotų įsipareigojimų ir mokėjimų asignavimų perkėlimo. Laikantis principo, kad Sąjungos biudžetas nustatomas kasmet, šiame reglamente, atsižvelgiant į nenuspėjamą, išskirtinį ir specifinį kibernetinio saugumo aplinkos pobūdį, turėtų būti numatyta galimybė nepanaudotas lėšas, be nustatytųjų Finansiniame reglamente, perkelti į kitą laikotarpį, taip kuo labiau padidinant Reagavimo į kibernetinio saugumo krizes mechanizmo pajėgumą padėti valstybėms narėms veiksmingai kovoti su kibernetinėmis grėsmėmis;	(11) siekiant patikimo finansų valdymo, reikėtų nustatyti konkrečias taisykles dėl nepanaudotų įsipareigojimų ir mokėjimų asignavimų perkėlimo. Laikantis principo, kad Sąjungos biudžetas nustatomas kasmet, šiame reglamente, atsižvelgiant į nenuspėjamą, išskirtinį ir specifinį kibernetinio saugumo aplinkos pobūdį, turėtų būti numatyta galimybė nepanaudotas lėšas, be nustatytųjų Finansiniame reglamente, perkelti į kitą laikotarpį, taip kuo labiau padidinant Reagavimo į kibernetinio saugumo krizes mechanizmo pajėgumą padėti valstybėms narėms veiksmingai kovoti su kibernetinėmis grėsmėmis***. Pagal šias konkrečias taisykles taip pat būtų leidžiama finansinę paramą, skirtą naujos kartos itin saugioms priemonėms ir infrastruktūrai įsigyti vykdant bendrus viešuosius pirkimus, teikti ilgesnį laikotarpį, siekiant gerinti kolektyvinio nustatymo pajėgumus naudojant naujausias dirbtinio intelekto (DI) ir duomenų analizės technologijas;***

Pakeitimas 10

Pasiūlymas dėl reglamento
13 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(13) kiekviena valstybė narė nacionaliniu lygmeniu turėtų paskirti viešąją įstaigą, kuriai būtų pavesta koordinuoti kibernetinių grėsmių aptikimo veiklą toje valstybėje narėje. Šie nacionaliniai SOC turėtų veikti kaip nacionalinis atskaitos taškas, nuo kurio nacionaliniu lygmeniu atsiveria galimybė dalyvauti Europos kibernetinio saugumo skydo veikloje, ir jie turėtų užtikrinti, kad iš viešųjų ir privačių subjektų gauta informacija apie kibernetines grėsmes būtų veiksmingai ir racionaliai dalijamasi ir ji būtų renkama nacionaliniu lygmeniu;	(13) kiekviena valstybė narė nacionaliniu lygmeniu turėtų paskirti viešąją įstaigą, kuriai būtų pavesta koordinuoti kibernetinių grėsmių aptikimo veiklą toje valstybėje narėje. Šie nacionaliniai SOC turėtų veikti kaip nacionalinis atskaitos taškas, nuo kurio nacionaliniu lygmeniu atsiveria galimybė dalyvauti Europos kibernetinio saugumo skydo veikloje, ir jie turėtų užtikrinti, kad iš viešųjų ir privačių subjektų gauta informacija apie kibernetines grėsmes būtų veiksmingai ir racionaliai dalijamasi ir ji būtų renkama nacionaliniu lygmeniu***. Kai įmanoma ir reikalinga, taip pat turėtų būti sudarytos sąlygos SOC veikloje dalyvauti gynybos subjektams, taip sukuriant gynybos ramstį, susijusį su valdymu ir informacijos, kuria keičiamasi, rūšimi, kaip nustatyta bendrame komunikate dėl ES kibernetinės gynybos politikos[1]. Tokį pasiūlymą palaiko ir vyriausiasis įgaliotinis***; ***[1] Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022)49 final.***

Pakeitimas 11

Pasiūlymas dėl reglamento
14 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(14) kaip Europos kibernetinio saugumo skydo dalis, turėtų būti įsteigti keli tarpvalstybiniai kibernetinio saugumo operacijų centrai (toliau – tarpvalstybiniai SOC). Jie turėtų suburti nacionalinius SOC iš bent trijų valstybių narių, kad būtų galima visapusiškai pasinaudoti tarpvalstybinio grėsmių aptikimo, dalijimosi informacija ir valdymo privalumais. Bendras tarpvalstybinių SOC	(14) kaip Europos kibernetinio saugumo skydo dalis, turėtų būti įsteigti keli tarpvalstybiniai kibernetinio saugumo operacijų centrai (toliau – tarpvalstybiniai SOC). Jie turėtų suburti nacionalinius SOC iš bent trijų valstybių narių, ***įskaitant gynybos ramstį,*** kad būtų galima visapusiškai pasinaudoti tarpvalstybinio grėsmių aptikimo, dalijimosi informacija ir valdymo privalumais. Bendras

tikslas turėtų būti stiprinti gebėjimus analizuoti kibernetinio saugumo grėsmes, užkirsti joms kelią bei jas aptikti ir remti kokybiškų žvalgybos duomenų apie kibernetinio saugumo grėsmes rengimą, visų pirma dalijantis duomenimis iš įvairių viešųjų ar privačių šaltinių, dalijantis naujausiomis priemonėmis ir jas bendrai naudojant, taip pat bendrai plėtojant aptikimo, analizės ir prevencijos pajėgumus patikimoje aplinkoje. Jie turėtų suteikti naujų papildomų pajėgumų, kurie remsis esamų SOC ir reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) bei kitų atitinkamų subjektų veikla ir ją papildys;	tarpvalstybinių SOC tikslas turėtų būti stiprinti gebėjimus analizuoti kibernetinio saugumo grėsmes, užkirsti joms kelią bei jas aptikti ir remti kokybiškų žvalgybos duomenų apie kibernetinio saugumo grėsmes rengimą, visų pirma dalijantis duomenimis iš įvairių viešųjų ar privačių šaltinių, ***o, kai įmanoma ir reikalinga, pateikiant pakankamai gairių dėl dalijimosi informacija, – ir*** dalijantis naujausiomis priemonėmis ir jas bendrai naudojant, taip pat bendrai plėtojant aptikimo, analizės ir prevencijos pajėgumus patikimoje aplinkoje. Jie turėtų suteikti naujų papildomų pajėgumų, kurie remsis esamų SOC ir reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) bei kitų atitinkamų subjektų veikla ir ją papildys;

Pakeitimas 12

Pasiūlymas dėl reglamento
15 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(15) nacionaliniu lygmeniu kibernetinių grėsmių stebėseną, aptikimą ir analizę paprastai užtikrina viešųjų ir privačių subjektų SOC kartu su CSIRT. Be to, CSIRT keičiasi informacija CSIRT tinkle pagal Direktyvą (ES) 2022/2555. Tarpvalstybiniai SOC turėtų sukurti naujus pajėgumus, kurie papildytų CSIRT tinklą, kaupiant viešųjų ir privačių subjektų duomenis apie grėsmes kibernetiniam saugumui bei jais dalijantis, didinant tokių duomenų vertę atliekant ekspertų analizę bei kartu įsigyjant infrastruktūros objektus ir taikant pažangiausias priemones, taip pat prisidedant prie Sąjungos pajėgumų ir ***technologinio suverenumo*** plėtojimo;	(15) nacionaliniu lygmeniu kibernetinių grėsmių stebėseną, aptikimą ir analizę paprastai užtikrina viešųjų ir privačių subjektų SOC kartu su CSIRT. Be to, CSIRT keičiasi informacija CSIRT tinkle pagal Direktyvą (ES) 2022/2555. Tarpvalstybiniai SOC turėtų sukurti naujus pajėgumus, kurie papildytų CSIRT tinklą, kaupiant viešųjų ir privačių subjektų duomenis apie grėsmes kibernetiniam saugumui bei jais dalijantis, didinant tokių duomenų vertę atliekant ekspertų analizę bei kartu įsigyjant infrastruktūros objektus ir taikant pažangiausias priemones, taip pat prisidedant prie Sąjungos pajėgumų ir ***atsparumo*** plėtojimo;

Pakeitimas 13

Pasiūlymas dėl reglamento
16 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(16) tarpvalstybiniai SOC turėtų veikti kaip centrinis punktas, leidžiantis sutelkti daug svarbių duomenų ir kibernetinių grėsmių žvalgybos informaciją, sudaryti sąlygas skleisti informaciją apie grėsmes dideliam įvairių dalyvių ratui (pvz., kompiuterinių incidentų tyrimo tarnyboms (toliau – CERT), CSIRT, keitimosi informacija ir jos analizės centrams (toliau – ISAC), ypatingos svarbos infrastruktūros objektų operatoriams). Informacija, kuria keičiasi tarpvalstybinio SOC dalyviai, galėtų apimti tinklų ir jutiklių duomenis, grėsmių žvalgybos informacijos santraukas, užvaldymo rodiklius ir kontekstinę informaciją apie incidentus, grėsmes ir pažeidžiamumus. Be to, tarpvalstybiniai SOC taip pat turėtų sudaryti bendradarbiavimo susitarimus su kitais tarpvalstybiniais SOC;	(16) tarpvalstybiniai SOC turėtų veikti kaip centrinis punktas, leidžiantis sutelkti daug svarbių duomenų ir kibernetinių grėsmių žvalgybos informaciją, sudaryti sąlygas skleisti informaciją apie grėsmes dideliam įvairių dalyvių ratui (pvz., kompiuterinių incidentų tyrimo tarnyboms (toliau – CERT), CSIRT, keitimosi informacija ir jos analizės centrams (toliau – ISAC), ypatingos svarbos infrastruktūros objektų operatoriams***, taip pat kibernetinės gynybos bendruomenei***). Informacija, kuria keičiasi tarpvalstybinio SOC dalyviai, galėtų apimti tinklų ir jutiklių duomenis, grėsmių žvalgybos informacijos santraukas, užvaldymo rodiklius ir kontekstinę informaciją apie incidentus, grėsmes ir pažeidžiamumus. Be to, tarpvalstybiniai SOC taip pat turėtų sudaryti bendradarbiavimo susitarimus su kitais tarpvalstybiniais SOC ***ir operatyviniu karinių kompiuterinių incidentų tyrimo tarnybų (milCERT) tinklu (angl. MICNET), kai jis bus sukurtas***;

Pakeitimas 14

Pasiūlymas dėl reglamento
17 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(17) atitinkamų institucijų bendras informuotumas apie padėtį yra būtina Sąjungos masto parengties reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir koordinavimo veiksmų sąlyga. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir	(17) atitinkamų institucijų bendras informuotumas apie padėtį yra būtina Sąjungos masto parengties reikšmingiems ir didelio masto kibernetinio saugumo incidentams ir koordinavimo veiksmų sąlyga. Siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą operatyviniu lygmeniu ir

užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų ir agentūrų, Direktyva (ES) 2022/2555 įsteigiamas EU-CyCLONe. Rekomendacijoje (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes apibūdinamas visų susijusių subjektų vaidmuo. Be to, Direktyvoje (ES) 2022/2555 primenama Komisijos atsakomybė pagal Sąjungos civilinės saugos mechanizmą (toliau – SCSM), nustatytą Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES, taip pat už analitinių ataskaitų dėl integruoto politinio atsako į krizes mechanizmo (toliau – IPCR) teikimą pagal Įgyvendinimo sprendimą (ES) 2018/1993. Todėl tais atvejais, kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie turėtų teikti atitinkamą informaciją EU-CyCLONe, CSIRT tinklui ir Komisijai. Visų pirma, priklausomai nuo situacijos, informacija, kuria turi būti dalijamasi, galėtų apimti techninę informaciją, informaciją apie užpuoliko arba potencialaus užpuoliko pobūdį bei motyvus ir aukštesnio lygio netechninę informaciją apie galimą arba vykstantį didelio masto kibernetinio saugumo incidentą. Šiomis aplinkybėmis reikėtų deramai atsižvelgti į būtinybės žinoti principą ir į galimai neskelbtiną informacijos, kuria dalijamasi, pobūdį;

užtikrinti reguliarų keitimąsi svarbia informacija tarp valstybių narių ir Sąjungos institucijų, įstaigų ir agentūrų, Direktyva (ES) 2022/2555 įsteigiamas EU-CyCLONe. Rekomendacijoje (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes apibūdinamas visų susijusių subjektų vaidmuo. Be to, Direktyvoje (ES) 2022/2555 primenama Komisijos atsakomybė pagal Sąjungos civilinės saugos mechanizmą (toliau – SCSM), nustatytą Europos Parlamento ir Tarybos sprendimu Nr. 1313/2013/ES, taip pat už analitinių ataskaitų dėl integruoto politinio atsako į krizes mechanizmo (toliau – IPCR) teikimą pagal Įgyvendinimo sprendimą (ES) 2018/1993. Todėl tais atvejais, kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba vykstančiu didelio masto kibernetinio saugumo incidentu, jie turėtų teikti atitinkamą informaciją EU-CyCLONe, CSIRT tinklui***, kibernetinės gynybos bendruomenei*** ir Komisijai. Visų pirma, priklausomai nuo situacijos, informacija, kuria turi būti dalijamasi, galėtų apimti techninę informaciją, informaciją apie užpuoliko arba potencialaus užpuoliko pobūdį bei motyvus ir aukštesnio lygio netechninę informaciją apie galimą arba vykstantį didelio masto kibernetinio saugumo incidentą. Šiomis aplinkybėmis reikėtų deramai atsižvelgti į būtinybės žinoti principą ir į galimai neskelbtiną informacijos, kuria dalijamasi, pobūdį;

Pakeitimas 15

Pasiūlymas dėl reglamento
19 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(19) siekiant sudaryti sąlygas didele apimtimi ir patikimoje aplinkoje keistis duomenimis apie kibernetinio saugumo	(19) siekiant sudaryti sąlygas didele apimtimi ir patikimoje aplinkoje keistis duomenimis apie kibernetinio saugumo

grėsmes iš įvairių šaltinių, Europos kibernetinio saugumo skydo veikloje dalyvaujantys subjektai turėtų turėti naujausias ir labai saugias priemones, įrangą ir infrastruktūros objektus. Tai turėtų sudaryti sąlygas pagerinti kolektyvinius nustatymo pajėgumus ir laiku įspėti valdžios institucijas ir atitinkamus subjektus, visų pirma naudojant naujausias dirbtinio intelekto ir duomenų analizės technologijas;	grėsmes iš įvairių šaltinių, Europos kibernetinio saugumo skydo veikloje dalyvaujantys subjektai***, išskyrus didelės rizikos ypatingos svarbos produktų su skaitmeniniais elementais tiekėjus,*** turėtų turėti naujausias ir labai saugias priemones, įrangą ir infrastruktūros objektus. Tai turėtų sudaryti sąlygas pagerinti kolektyvinius nustatymo pajėgumus ir laiku įspėti valdžios institucijas ir atitinkamus subjektus, visų pirma naudojant naujausias dirbtinio intelekto ir duomenų analizės technologijas; ***naudojant dirbtinį intelektą turėtų būti numatyta žmogaus atliekama priežiūra ir turėtų būti užtikrintas pakankamas raštingumas dirbtinio intelekto srityje, būtina parama ir įgaliojimai tai funkcijai vykdyti;***

Pakeitimas 16

Pasiūlymas dėl reglamento
19 a konstatuojamoji dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	(19a) pagal Reglamentą [XX/XXXX (Kibernetinio atsparumo aktą)] Europos kibernetinio saugumo skydo veikloje dalyvaujantys subjektai taip pat turėtų laikytis šiame reglamente nustatytų reikalavimų, taikomų visiems skaitmeninių elementų turintiems produktams. Atsižvelgiant į didėjančią riziką, kylančią dėl ekonominės priklausomybės, būtina kuo labiau sumažinti priklausomybę nuo didelės rizikos ypatingos svarbos produktų tiekėjų, šiuo tikslu nustatant bendrą ES ekonominio saugumo strateginę sistemą. Dėl priklausomybės nuo didelės rizikos ypatingos svarbos produktų su skaitmeniniais elementais tiekėjų kyla strateginė rizika, kuri turėtų būti mažinama Sąjungos lygmeniu, visų pirma tais atvejais, kai šalis vykdo ekonominį šnipinėjimą ar ekonominę prievartą ir

	pagal jos teisės aktus įpareigojama savavališkai gauti prieigą prie bet kokios informacijos apie įmonės veiklą ar duomenų, ypač kai ypatingos svarbos produktai skirti naudoti Direktyvoje (ES) 2022/2555 nurodytiems esminiams subjektams;

Pakeitimas 17

Pasiūlymas dėl reglamento
20 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(20) renkant duomenis, jais dalijantis bei keičiantis, Europos kibernetinio saugumo skydas turėtų stiprinti Sąjungos technologinį suverenumą. Kokybiškų patikrintų duomenų sutelkimas taip pat turėtų padėti plėtoti pažangias dirbtinio intelekto ir duomenų analizės technologijas. Tai turėtų būti lengviau padaryti sujungiant Europos kibernetinio saugumo skydą su visos Europos našiosios kompiuterijos infrastruktūra, sukurta Tarybos reglamentu (ES) 2021/1173[25];	(20) renkant duomenis, jais dalijantis bei keičiantis, Europos kibernetinio saugumo skydas turėtų stiprinti Sąjungos technologinį suverenumą***, jos strateginį savarankiškumą, konkurencingumą ir atsparumą***. Kokybiškų patikrintų duomenų sutelkimas taip pat turėtų padėti plėtoti pažangias dirbtinio intelekto ir duomenų analizės technologijas. Tai turėtų būti lengviau padaryti sujungiant Europos kibernetinio saugumo skydą su visos Europos našiosios kompiuterijos infrastruktūra, sukurta Tarybos reglamentu (ES) 2021/1173[25];
[25] 2021 m. liepos 13 d. Tarybos reglamentas (ES) 2021/1173 dėl Europos našiosios kompiuterijos bendrosios įmonės įsteigimo ir kuriuo panaikinamas Reglamentas (ES) 2018/1488 (OL L 256, 2021 7 19, p. 3).	[25] 2021 m. liepos 13 d. Tarybos reglamentas (ES) 2021/1173 dėl Europos našiosios kompiuterijos bendrosios įmonės įsteigimo ir kuriuo panaikinamas Reglamentas (ES) 2018/1488 (OL L 256, 2021 7 19, p. 3).

Pakeitimas 18

Pasiūlymas dėl reglamento
25 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(25) Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų padėti	(25) Reagavimo į kibernetinio saugumo krizes mechanizmas turėtų padėti

valstybėms narėms papildyti jų pačių priemones bei išteklius ir kitas esamas paramos reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus ir nedelsiant po jų atkurti veiklą galimybes, pavyzdžiui, Europos Sąjungos kibernetinio saugumo agentūros (toliau – ENISA) jos kompetencijos srityje teikiamas paslaugas, koordinuotą reagavimą ir CSIRT tinklo pagalbą, EU-CyCLONe poveikio mažinimo paramą, taip pat valstybių narių savitarpio pagalbą, be kita ko, pagal ES sutarties 42 straipsnio 7 dalį, PESCO greitojo reagavimo į kibernetinius incidentus ***komandas26*** ir greitojo reagavimo į hibridines grėsmes grupes. Juo turėtų būti atsižvelgiama į poreikį užtikrinti, kad būtų specialių priemonių, kuriomis būtų remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos visoje Sąjungoje ir trečiosiose valstybėse;

[26] 2017 m. gruodžio 11 d. TARYBOS SPRENDIMAS (BUSP) 2017/2315, kuriuo nustatomas nuolatinis struktūrizuotas bendradarbiavimas (PESCO) ir nustatomas dalyvaujančių valstybių narių sąrašas.

valstybėms narėms papildyti jų pačių priemones bei išteklius ir kitas esamas paramos reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus ir nedelsiant po jų atkurti veiklą galimybes, pavyzdžiui, Europos Sąjungos kibernetinio saugumo agentūros (toliau – ENISA) jos kompetencijos srityje teikiamas paslaugas, koordinuotą reagavimą ir CSIRT tinklo pagalbą, EU-CyCLONe poveikio mažinimo paramą, taip pat valstybių narių savitarpio pagalbą, be kita ko, pagal ES sutarties 42 straipsnio 7 dalį, PESCO greitojo reagavimo į kibernetinius incidentus ***komandas[1], naująjį PESCO projekto Kibernetinės ir informacinės srities koordinavimo centrą (CIDCC) ir siūlomą sukurti ES kibernetinės gynybos koordinavimo centrą (EUCDCC), kuriuo būtų pakeistas CIDCC,*** ir greitojo reagavimo į hibridines grėsmes grupes. Juo turėtų būti atsižvelgiama į poreikį užtikrinti, kad būtų specialių priemonių, kuriomis būtų remiamas pasirengimas kibernetinio saugumo incidentams ir reagavimas į juos visoje Sąjungoje ir trečiosiose valstybėse***, visų pirma ES šalyse kandidatėse, kurios suderinusios savo politiką su ES bendra užsienio ir saugumo politika ir bendra saugumo ir gynybos politika, remiant jas stiprinant savo kibernetinius pajėgumus ir stiprinant tų šalių kandidačių tarpvalstybinį ir regioninį bendradarbiavimą kibernetinėje srityje***;

[1] 2017 m. gruodžio 11 d. TARYBOS SPRENDIMAS (BUSP) 2017/2315, kuriuo nustatomas nuolatinis struktūrizuotas bendradarbiavimas (PESCO) ir nustatomas dalyvaujančių valstybių narių sąrašas.

[26] 2017 m. gruodžio 11 d. TARYBOS SPRENDIMAS (BUSP) 2017/2315, kuriuo nustatomas nuolatinis struktūrizuotas bendradarbiavimas (PESCO) ir nustatomas dalyvaujančių valstybių narių sąrašas.

Pakeitimas 19

Pasiūlymas dėl reglamento
26 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(26) šia priemone nedaroma poveikio Sąjungos lygmens reagavimo į krizes koordinavimo procedūroms ir sistemoms, visų pirma SCSM[27], IPCR[28] ir Direktyvai (ES) 2022/2555. Ji gali padėti įgyvendinti veiksmus, įgyvendinamus pagal ES sutarties 42 straipsnio 7 dalį arba SESV 222 straipsnyje apibrėžtais atvejais, arba juos papildyti. ***Be to,*** šios priemonės naudojimas***, kai tinkama,*** turėtų būti koordinuojamas su kibernetinio saugumo diplomatijos priemonių rinkinio priemonių įgyvendinimu;	(26) šia priemone nedaroma poveikio Sąjungos lygmens reagavimo į krizes koordinavimo procedūroms ir sistemoms, visų pirma SCSM[27], IPCR[28] ir Direktyvai (ES) 2022/2555. Ji gali padėti įgyvendinti veiksmus, įgyvendinamus pagal ES sutarties 42 straipsnio 7 dalį arba SESV 222 straipsnyje apibrėžtais atvejais, arba juos papildyti. Šios priemonės naudojimas ***taip pat*** turėtų būti koordinuojamas su Kibernetinio saugumo diplomatijos priemonių rinkinio priemonių įgyvendinimu***, stiprinant kibernetinės gynybos ir kitų kibernetinių bendruomenių bendradarbiavimą strateginiu, operatyviniu ir techniniu lygmenimis, visų pirma siekiant stiprinti pajėgumus kovoti su kibernetinio saugumo grėsmėmis iš už Sąjungos ribų, įskaitant ribojamąsias priemones, kurios gali būti naudojamos kibernetinės kenkimo veiklos prevencijai ir reagavimui į ją***;
[27] 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).	[27] 2013 m. gruodžio 17 d. Europos Parlamento ir Tarybos sprendimas Nr. 1313/2013/ES dėl Sąjungos civilinės saugos mechanizmo (OL L 347, 2013 12 20, p. 924).
[28] Integruotas politinio atsako į krizes mechanizmas (IPCR) pagal 2017 m. rugsėjo 13 d. Komisijos rekomendaciją (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.	[28] Integruotas politinio atsako į krizes mechanizmas (IPCR) pagal 2017 m. rugsėjo 13 d. Komisijos rekomendaciją (ES) 2017/1584 dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes.

Pakeitimas 20

Pasiūlymas dėl reglamento
28 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(28) Direktyvoje (ES) 2022/2555 reikalaujama, kad valstybės narės paskirtų arba įsteigtų vieną ar daugiau kibernetinio saugumo krizių valdymo institucijų ir užtikrintų, kad jos turėtų tinkamų išteklių ir galėtų veiksmingai ir efektyviai vykdyti joms pavestas užduotis. Joje taip pat reikalaujama, kad valstybės narės nustatytų, kokius pajėgumus, objektus ir procedūras galima panaudoti krizės atveju, taip pat priimtų nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Taip pat reikalaujama, kad valstybės narės įsteigtų vieną ar daugiau CSIRT, kurioms būtų pavesta atsakomybė už incidentų valdymą pagal aiškiai apibrėžtą procesą, apimant bent sektorius, subsektorius ir subjektų rūšis, patenkančius į tos direktyvos taikymo sritį, ir užtikrintų, kad jos turėtų tinkamų išteklių savo užduotims veiksmingai vykdyti. Šiuo reglamentu nedaroma poveikio Komisijos vaidmeniui užtikrinti, kad valstybės narės laikytųsi Direktyvoje (ES) 2022/2555 nustatytų pareigų. Pagal reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama pagalba veiksmams, kuriais siekiama stiprinti parengtį, taip pat reagavimo į incidentus veiksmams, kuriais siekiama sušvelninti reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikį, remti nedelsiamą veiklos ir (arba) esminių paslaugų veikimo atkūrimą;	(28) Direktyvoje (ES) 2022/2555 reikalaujama, kad valstybės narės paskirtų arba įsteigtų vieną ar daugiau kibernetinio saugumo krizių valdymo institucijų ir užtikrintų, kad jos turėtų tinkamų išteklių ir galėtų veiksmingai ir efektyviai vykdyti joms pavestas užduotis. Joje taip pat reikalaujama, kad valstybės narės nustatytų, kokius pajėgumus, objektus ir procedūras galima panaudoti krizės atveju, taip pat priimtų nacionalinį reagavimo į didelio masto kibernetinio saugumo incidentus ir krizes planą, kuriame išdėstomi didelio masto kibernetinio saugumo incidentų ir krizių valdymo tikslai ir tvarka. Taip pat reikalaujama, kad valstybės narės įsteigtų vieną ar daugiau CSIRT, kurioms būtų pavesta atsakomybė už incidentų valdymą pagal aiškiai apibrėžtą procesą, apimant bent sektorius, subsektorius ir subjektų rūšis, patenkančius į tos direktyvos taikymo sritį, ir užtikrintų, kad jos turėtų tinkamų išteklių savo užduotims veiksmingai vykdyti. Šiuo reglamentu nedaroma poveikio Komisijos vaidmeniui užtikrinti, kad valstybės narės laikytųsi Direktyvoje (ES) 2022/2555 nustatytų pareigų. Pagal reagavimo į kibernetinio saugumo krizes mechanizmą turėtų būti teikiama pagalba veiksmams, kuriais siekiama stiprinti parengtį, taip pat reagavimo į incidentus veiksmams, kuriais siekiama sušvelninti reikšmingų ir didelio masto kibernetinio saugumo incidentų poveikį, remti nedelsiamą veiklos ir (arba) esminių paslaugų veikimo atkūrimą***, tinkamai pasinaudojant visomis civilinėms ir karinėms bendruomenėms prieinamomis gynybos galimybėmis***;

Pakeitimas 21

Pasiūlymas dėl reglamento
29 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(29) vykdant pasirengimo veiksmus, siekiant skatinti nuoseklų požiūrį ir stiprinti saugumą visoje Sąjungoje ir jos vidaus rinkoje, turėtų būti teikiama parama Direktyvoje (ES) 2022/2555 nustatytuose itin svarbiuose sektoriuose veikiančių subjektų kibernetinio saugumo koordinuotam testavimui ir vertinimui. Šiuo tikslu Komisija, padedama ENISA ir bendradarbiaudama su Direktyva (ES) 2022/2555 įsteigta TIS bendradarbiavimo grupe, turėtų reguliariai nustatyti, kurie atitinkami sektoriai ar subsektoriai turėtų būti tinkami gauti finansinę paramą koordinuotam Sąjungos lygmens testavimui. ***Sektoriai*** arba ***subsektoriai*** turėtų būti atrinkti iš Direktyvos (ES) 2022/2555 I priedo („Ypatingos svarbos sektoriai“). Koordinuotas testavimas turėtų būti grindžiamas bendrais rizikos scenarijais ir metodikomis. Atrenkant sektorius ir rengiant rizikos scenarijus turėtų būti atsižvelgiama į atitinkamus Sąjungos masto rizikos vertinimus ir rizikos scenarijus, įskaitant poreikį vengti dubliavimosi, kaip antai rizikos vertinimą ir rizikos scenarijus, kuriuos Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė raginami parengti, derindami veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir sukurtais tinklais, įskaitant EU-CyCLONe, taip pat ryšių tinklų ir infrastruktūrų rizikos vertinimą, kurio buvo paprašyta Nevere paskelbtame bendrame ministrų raginime ir kurį atlieka TIS bendradarbiavimo grupė, padedant Komisijai bei ENISA ir bendradarbiaujant su Europos elektroninių ryšių reguliuotojų	(29) vykdant pasirengimo veiksmus, siekiant skatinti nuoseklų požiūrį ir stiprinti saugumą visoje Sąjungoje ir jos vidaus rinkoje, turėtų būti teikiama parama Direktyvoje (ES) 2022/2555 nustatytuose itin svarbiuose sektoriuose veikiančių subjektų kibernetinio saugumo koordinuotam testavimui ir vertinimui. Šiuo tikslu Komisija, padedama ENISA ir bendradarbiaudama su Direktyva (ES) 2022/2555 įsteigta TIS bendradarbiavimo grupe, turėtų reguliariai nustatyti, kurie atitinkami sektoriai ar subsektoriai turėtų būti tinkami gauti finansinę paramą koordinuotam Sąjungos lygmens testavimui. ***Atitinkamais atvejais taip pat turėtų būti įtraukta Europos išorės veiksmų tarnyba (EIVT), visų pirma per ES žvalgybos centrą (INTCEN) ir jo hibridinių grėsmių analizės ir informavimo centrą, padedant Europos Sąjungos karinio štabo (EUMS) Žvalgybos direktoratui prie Bendro žvalgybinės informacijos analizės centro (SIAC), ir teikti naujausius vertinimus bei padėti nustatyti sektorius*** arba ***subsektorius, kurie*** turėtų būti atrinkti iš Direktyvos (ES) 2022/2555 I priedo („Ypatingos svarbos sektoriai“). Koordinuotas testavimas turėtų būti grindžiamas bendrais rizikos scenarijais ir metodikomis***. Šis testavimas taip pat turėtų atlikti svarbų vaidmenį gerinant civilinių ir karinių subjektų bendradarbiavimą. Todėl, atlikdamos testavimus, Komisija, EIVT ir ENISA turėtų sistemingai apsvarstyti galimybę įtraukti dalyvius iš kitų kibernetinių bendruomenių, pavyzdžiui, Europos gynybos agentūros (EGA) ir kitų susijusių subjektų.*** Atrenkant sektorius ir rengiant rizikos scenarijus turėtų būti atsižvelgiama

institucija (BEREC), koordinuotus rizikos vertinimus, kurie turi būti atliekami pagal Direktyvos (ES) 2022/2555 22 straipsnį, ir skaitmeninės veiklos atsparumo testavimą, kaip numatyta Europos Parlamento ir Tarybos reglamente (ES) 2022/***255429***. Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;

[29] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011.

į atitinkamus Sąjungos masto rizikos vertinimus ir rizikos scenarijus, įskaitant poreikį vengti dubliavimosi, kaip antai rizikos vertinimą ir rizikos scenarijus, kuriuos Tarybos išvadose dėl Europos Sąjungos kibernetinio saugumo būklės raidos Komisija, vyriausiasis įgaliotinis ir TIS bendradarbiavimo grupė raginami parengti, derindami veiksmus su atitinkamomis civilinėmis ir karinėmis įstaigomis bei agentūromis ir sukurtais tinklais, įskaitant EU-CyCLONe, taip pat ryšių tinklų ir infrastruktūrų rizikos vertinimą, kurio buvo paprašyta Nevere paskelbtame bendrame ministrų raginime ir kurį atlieka TIS bendradarbiavimo grupė, padedant Komisijai bei ENISA ir bendradarbiaujant su Europos elektroninių ryšių reguliuotojų institucija (BEREC), koordinuotus rizikos vertinimus, kurie turi būti atliekami pagal Direktyvos (ES) 2022/2555 22 straipsnį, ir skaitmeninės veiklos atsparumo testavimą, kaip numatyta Europos Parlamento ir Tarybos reglamente (ES) 2022/***2554[1]***. Atrenkant sektorius taip pat reikėtų atsižvelgti į Tarybos rekomendaciją dėl Sąjungos suderinto požiūrio į ypatingos svarbos infrastruktūros atsparumo didinimą;

[1] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011.

[29] 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011.

Pakeitimas 22

Pasiūlymas dėl reglamento
32 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(32) Reagavimo į kibernetinio saugumo krizes mechanizmu turėtų būti remiama valstybių narių teikiama pagalba valstybei narei, nukentėjusiai nuo reikšmingo ar didelio masto kibernetinio saugumo incidento, be kita ko, teikiama per CSIRT tinklą, įsteigtą pagal Direktyvos (ES) 2022/2555 15 straipsnį. Pagalbą teikiančioms valstybėms narėms turėtų būti leidžiama teikti prašymus padengti išlaidas, susijusias su ekspertų grupių siuntimu teikiant savitarpio pagalbą. Tinkamos finansuoti išlaidos galėtų apimti kibernetinio saugumo ekspertų kelionės, apgyvendinimo ir dienpinigių išlaidas;	(32) Reagavimo į kibernetinio saugumo krizes mechanizmu turėtų būti remiama valstybių narių teikiama pagalba valstybei narei, nukentėjusiai nuo reikšmingo ar didelio masto kibernetinio saugumo incidento, be kita ko, teikiama per CSIRT tinklą, įsteigtą pagal Direktyvos (ES) 2022/2555 15 straipsnį. Pagalbą teikiančioms valstybėms narėms turėtų būti leidžiama teikti prašymus padengti išlaidas, susijusias su ekspertų grupių siuntimu teikiant savitarpio pagalbą***, užtikrinant, kad teikiant pagalbą trečiosioms valstybėms, visų pirma, Ukrainai ir Moldovai, būtų veiksmingai koordinuojamos atitinkamos ES programos ir priemonės, įskaitant Europos taikos priemonę (ETP), BUSP ir KVTBP***. Tinkamos finansuoti išlaidos galėtų apimti kibernetinio saugumo ekspertų kelionės, apgyvendinimo ir dienpinigių išlaidas;

Pakeitimas 23

Pasiūlymas dėl reglamento
33 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(33) turėtų būti palaipsniui sukurtas Sąjungos lygmens kibernetinio saugumo rezervas, kurį sudarytų privačių valdomų saugumo paslaugų teikėjų paslaugos, kuriomis būtų remiami reagavimo ir nedelsiamo veiklos atkūrimo veiksmai reikšmingų arba didelio masto kibernetinio saugumo incidentų atvejais. ES kibernetinio saugumo rezervas turėtų	(33) turėtų būti palaipsniui sukurtas Sąjungos lygmens kibernetinio saugumo rezervas, kurį sudarytų privačių valdomų saugumo paslaugų teikėjų paslaugos, kuriomis būtų remiami reagavimo ir nedelsiamo veiklos atkūrimo veiksmai reikšmingų arba didelio masto kibernetinio saugumo incidentų atvejais. ES kibernetinio saugumo rezervas turėtų

užtikrinti paslaugų prieinamumą ir parengtį. ES kibernetinio saugumo rezervo paslaugos turėtų padėti nacionalinėms institucijoms teikti pagalbą paveiktiems subjektams, veikiantiems ypatingos svarbos ar itin svarbiuose sektoriuose, papildant jų pačių veiksmus nacionaliniu lygmeniu. Prašydamos paramos iš ES kibernetinio saugumo rezervo, valstybės narės turėtų nurodyti, kokia parama atitinkamam subjektui teikiama nacionaliniu lygmeniu, ir į tai turėtų būti atsižvelgta vertinant valstybės narės prašymą. ES kibernetinio saugumo rezervo paslaugos taip pat gali būti naudingos panašiomis sąlygomis teikiant paramą Sąjungos institucijoms, įstaigoms ir agentūroms;	užtikrinti paslaugų prieinamumą ir parengtį. ES kibernetinio saugumo rezervo paslaugos turėtų padėti nacionalinėms institucijoms teikti pagalbą paveiktiems subjektams, veikiantiems ypatingos svarbos ar itin svarbiuose sektoriuose, papildant jų pačių veiksmus nacionaliniu lygmeniu. Prašydamos paramos iš ES kibernetinio saugumo rezervo, valstybės narės turėtų nurodyti, kokia parama atitinkamam subjektui teikiama nacionaliniu lygmeniu, ir į tai turėtų būti atsižvelgta vertinant valstybės narės prašymą. ES kibernetinio saugumo rezervo paslaugos taip pat gali būti naudingos panašiomis sąlygomis teikiant paramą Sąjungos institucijoms, įstaigoms ir agentūroms***, įskaitant BSGP misijas***;

Pakeitimas 24

Pasiūlymas dėl reglamento
34 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(34) siekiant atrinkti privačius paslaugų teikėjus, kurie teiktų paslaugas pagal ES kibernetinio saugumo rezervą, būtina nustatyti minimaliuosius kriterijus, kurie turėtų būti įtraukti į kvietimą teikti pasiūlymus tiems paslaugų teikėjams atrinkti, siekiant užtikrinti, kad būtų tenkinami valstybių narių institucijų ir subjektų, veikiančių ypatingos svarbos ar itin svarbiuose sektoriuose, poreikiai;	(34) siekiant atrinkti privačius paslaugų teikėjus, kurie teiktų paslaugas pagal ES kibernetinio saugumo rezervą, būtina nustatyti minimaliuosius kriterijus, kurie turėtų būti įtraukti į kvietimą teikti pasiūlymus tiems paslaugų teikėjams atrinkti, siekiant užtikrinti, kad būtų tenkinami valstybių narių institucijų ir subjektų, veikiančių ypatingos svarbos ar itin svarbiuose sektoriuose, poreikiai***, taip pat atsižvelgiant į riziką, susijusią su tiekėjų iš šalių, kurios laikomos strateginėmis konkurentėmis, dalyvavimu, dėl kurio gali kilti rizika ekonominiam saugumui, bei į poveikį strateginiam Sąjungos saugumui***;

Pakeitimas 25

Pasiūlymas dėl reglamento
36 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(36) siekiant remti šio reglamento tikslus skatinti bendrą informuotumą apie padėtį, didinti Sąjungos atsparumą ir sudaryti sąlygas veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus, EU-CyCLONe, CSIRT tinklas arba Komisija turėtų turėti galimybę prašyti ENISA peržiūrėti ir įvertinti grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus, susijusius su konkrečiu reikšmingu ar didelio masto kibernetinio saugumo incidentu. Užbaigusi incidento peržiūrą ir vertinimą, ENISA, bendradarbiaudama su atitinkamais suinteresuotaisiais subjektais, įskaitant privačiojo sektoriaus, valstybių narių, Komisijos ir kitų atitinkamų ES institucijų, įstaigų ir agentūrų atstovus, turėtų parengti incidento peržiūros ataskaitą. Kalbant apie privatųjį sektorių, ENISA kuria informacijos mainų su specializuotais paslaugų teikėjais, įskaitant valdomų saugumo sprendinių teikėjus ir pardavėjus, kanalus, siekdama prisidėti prie ENISA misijos pasiekti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje. Remiantis bendradarbiavimu su suinteresuotaisiais subjektais, įskaitant privatųjį sektorių, konkrečių incidentų peržiūros ataskaitoje turėtų būti siekiama įvertinti incidento priežastis, poveikį ir padarinių švelninimą po incidento. Ypač daug dėmesio turėtų būti skiriama informacijai ir patirčiai, kuria dalijasi valdomų saugumo paslaugų teikėjai, atitinkantys aukščiausio profesinio sąžiningumo, nešališkumo ir reikiamos techninės kompetencijos sąlygas, kaip reikalaujama šiame reglamente. Ataskaita turėtų būti pateikta EU-CyCLONe, CSIRT tinklui ir Komisijai ir ja turėtų būti remiamasi jų darbe. Kai incidentas susijęs su trečiąja valstybe, Komisija turėtų ja	(36) siekiant remti šio reglamento tikslus skatinti bendrą informuotumą apie padėtį, didinti Sąjungos atsparumą ir sudaryti sąlygas veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus, EU-CyCLONe, CSIRT tinklas arba Komisija turėtų turėti galimybę prašyti ENISA peržiūrėti ir įvertinti grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus, susijusius su konkrečiu reikšmingu ar didelio masto kibernetinio saugumo incidentu. ***Atsižvelgiant į saugaus junglumo sistemos, grindžiamos Europos kvantinės komunikacijos infrastruktūra (EuroQCI) ir Europos Sąjungos vyriausybiniu palydoviniu ryšiu (GOVSATCOM), kūrimą, visų pirma GALILEO GNSS diegimą gynybos naudotojams, bet kokioje būsimoje perspektyvoje turėtų būti atsižvelgiama į tai, kad kvantinės kompiuterijos sparta ir sudėtingumas sujungiamas su labai autonominėmis karinėmis sistemomis.*** Užbaigusi incidento peržiūrą ir vertinimą, ENISA, bendradarbiaudama su atitinkamais suinteresuotaisiais subjektais, įskaitant privačiojo sektoriaus, valstybių narių, Komisijos ir kitų atitinkamų ES institucijų, įstaigų ir agentūrų atstovus, turėtų parengti incidento peržiūros ataskaitą. Kalbant apie privatųjį sektorių, ENISA kuria informacijos mainų su specializuotais paslaugų teikėjais, įskaitant valdomų saugumo sprendinių teikėjus ir pardavėjus, kanalus, siekdama prisidėti prie ENISA misijos pasiekti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje. Remiantis bendradarbiavimu su suinteresuotaisiais subjektais, įskaitant privatųjį sektorių, konkrečių incidentų peržiūros ataskaitoje turėtų būti siekiama įvertinti incidento

pasidalyti ir su vyriausiuoju įgaliotiniu;	priežastis, poveikį ir padarinių švelninimą po incidento. Ypač daug dėmesio turėtų būti skiriama informacijai ir patirčiai, kuria dalijasi valdomų saugumo paslaugų teikėjai, atitinkantys aukščiausio profesinio sąžiningumo, nešališkumo ir reikiamos techninės kompetencijos sąlygas, kaip reikalaujama šiame reglamente. Ataskaita turėtų būti pateikta EU-CyCLONe, CSIRT tinklui ir Komisijai ir ja turėtų būti remiamasi jų darbe. Kai incidentas susijęs su trečiąja valstybe, Komisija turėtų ja pasidalyti ir su vyriausiuoju įgaliotiniu***, EIVT ir per misijos štabą su bet kuria BSGP misija incidento paveiktoje valstybėje***;

Pakeitimas 26

Pasiūlymas dėl reglamento
37 konstatuojamoji dalis

Komisijos siūlomas tekstas	*Pakeitimas*
(37) atsižvelgiant į nenuspėjamą kibernetinio saugumo išpuolių pobūdį ir į tai, kad jie neretai nėra susiję su konkrečia geografine vietove ir kelia didelę šalutinio poveikio riziką, didinant kaimyninių šalių atsparumą ir stiprinant gebėjimą veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus prisidedama prie visos Sąjungos apsaugos. Todėl su Skaitmeninės Europos programa asocijuotos trečiosios valstybės ***gali*** būti remiamos ES kibernetinio saugumo rezervo lėšomis, ***jei tai numatyta atitinkamame Skaitmeninės Europos programos asociacijos susitarime***. Sąjunga turėtų remti asocijuotųjų trečiųjų valstybių finansavimą pagal toms valstybėms skirtas atitinkamas partnerystes ir finansavimo priemones. Parama turėtų būti skiriama paslaugoms, susijusioms su reagavimu į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiamu veiklos atkūrimu po jų. Šiame reglamente ES kibernetinio saugumo	(37) atsižvelgiant į nenuspėjamą kibernetinio saugumo išpuolių pobūdį ir į tai, kad jie neretai nėra susiję su konkrečia geografine vietove ir kelia didelę šalutinio poveikio riziką, didinant kaimyninių šalių***, visų pirma Ukrainos ir Moldovos,*** atsparumą ir stiprinant gebėjimą veiksmingai reaguoti į reikšmingus ir didelio masto kibernetinio saugumo incidentus prisidedama prie visos Sąjungos apsaugos. Todėl su Skaitmeninės Europos programa asocijuotos trečiosios valstybės ***turėtų*** būti remiamos ES kibernetinio saugumo rezervo lėšomis***. Parama taip pat turėtų būti teikiama toms trečiosioms valstybėms***, ***kuriose vykdoma BSGP misija, kuriai suteikti specialūs įgaliojimai stiprinti atsparumą hibridinėms grėsmėms, įskaitant kibernetines grėsmes, arba taikoma ETP pagalbos priemonė, skirta tos valstybės kibernetiniam atsparumui stiprinti***. Sąjunga turėtų remti asocijuotųjų trečiųjų valstybių finansavimą pagal toms valstybėms skirtas atitinkamas

rezervui ir patikimiems paslaugų teikėjams nustatytos sąlygos turėtų būti taikomos teikiant paramą Skaitmeninės Europos programos asocijuotosioms trečiosioms valstybėms;	partnerystes ir finansavimo priemones. Parama turėtų būti skiriama paslaugoms, susijusioms su reagavimu į reikšmingus arba didelio masto kibernetinio saugumo incidentus ir nedelsiamu veiklos atkūrimu po jų. Šiame reglamente ES kibernetinio saugumo rezervui ir patikimiems paslaugų teikėjams nustatytos sąlygos turėtų būti taikomos teikiant paramą Skaitmeninės Europos programos asocijuotosioms trečiosioms valstybėms;

Pakeitimas 27

Pasiūlymas dėl reglamento
1 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) sukurti Europos kibernetinio saugumo incidentų peržiūros mechanizmą reikšmingiems arba didelio masto incidentams peržiūrėti ir įvertinti.	c) sukurti Europos kibernetinio saugumo incidentų peržiūros mechanizmą reikšmingiems arba didelio masto incidentams ***arba grėsmėms*** peržiūrėti ir įvertinti.

Pakeitimas 28

Pasiūlymas dėl reglamento
1 straipsnio 2 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip sudarant sąlygas stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio ***suverenumo*** kibernetinio saugumo srityje;	a) stiprinti bendrą Sąjungos kibernetinių grėsmių ir incidentų aptikimą ir informuotumą apie padėtį, taip sudarant sąlygas stiprinti Sąjungos pramonės ir paslaugų sektorių konkurencinę padėtį visoje skaitmeninėje ekonomikoje ir prisidėti prie Sąjungos technologinio ***atsparumo*** kibernetinio saugumo srityje;

Pakeitimas 29

Pasiūlymas dėl reglamento
1 straipsnio 2 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) stiprinti subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, be kita ko, teikiant Sąjungos paramą reaguojant į kibernetinio saugumo incidentus Skaitmeninės Europos programos (SEP) asocijuotosioms trečiosioms valstybėms;	b) stiprinti subjektų, veikiančių ypatingos svarbos ir itin svarbiuose sektoriuose visoje Sąjungoje, parengtį ir solidarumą plėtojant bendrus reagavimo į reikšmingus arba didelio masto kibernetinio saugumo incidentus pajėgumus, be kita ko, teikiant Sąjungos paramą reaguojant į kibernetinio saugumo incidentus Skaitmeninės Europos programos (SEP) asocijuotosioms trečiosioms valstybėms ***arba toms trečiosioms valstybėms, kurios yra kandidatės įstoti į Sąjungą ir kurios neprieštarauja Sąjungos ir jos valstybių narių saugumo ir gynybos interesams, kaip nustatyta BUSP sistemoje pagal Europos Sąjungos sutarties V antraštinę dalį***; ***valstybės narės turėtų apsvarstyti galimybę aktyvią kibernetinės gynybos programą įtraukti į jų nacionalinę kibernetinio saugumo strategiją, kuri apima reguliarias bendras valstybių narių ir tarptautinių organizacijų mokymo pratybas. Tokia programa turėtų užtikrinti sinchronizuotą galimybę realiu laiku aptikti, nustatyti, išanalizuoti ir sušvelninti grėsmes;***

Pakeitimas 30

Pasiūlymas dėl reglamento
1 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. mažinti sisteminę kibernetinio saugumo riziką, kurią kelia priklausomybė nuo ypatingos svarbos įrangos iš šalių, kurios prieštarautų Sąjungos ir jos valstybių narių saugumo ir gynybos interesams, kaip nustatyta BUSP sistemoje pagal Europos Sąjungos sutarties V antraštinę dalį;

Pakeitimas 31

Pasiūlymas dėl reglamento
2 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	kibernetinės gynybos bendruomenė – valstybių narių gynybos institucijos, remiamos ES institucijų, įstaigų ir agentūrų, kaip nurodyta bendrame komunikate dėl ES kibernetinės gynybos politikos[1];
	[1] Bendras komunikatas Europos Parlamentui ir Tarybai „ES kibernetinės gynybos politika“, JOIN(2022)49 final.

Pakeitimas 32

Pasiūlymas dėl reglamento
3 straipsnio 2 dalies 1 pastraipos b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) padėti modernizuoti visas kibernetinės gynybos sistemas, didinti kibernetinės gynybos pajėgumų kokybę diegiant DI sistemas ir paspartinti nacionalinių SOC ir tarpvalstybinių SOC keitimąsi informacija;

Pakeitimas 33

Pasiūlymas dėl reglamento
3 straipsnio 2 dalies 1 pastraipos d a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	da) peržiūri ir įvertina ypatingos svarbos kibernetinio saugumo technologijas ir įrangą, kurias SOC naudoja reaguodami į kibernetinio saugumo incidentus dėl sisteminės rizikos, kylančios dėl didelės rizikos teikėjų kontrolės šalyse, kurios prieštarautų Sąjungos ir jos valstybių narių saugumo

	ir gynybos interesams, kaip nustatyta BUSP srityje pagal ES sutarties V antraštinę dalį;

Pakeitimas 34

Pasiūlymas dėl reglamento
4 straipsnio 1 dalies 2 pastraipa

Komisijos siūlomas tekstas	*Pakeitimas*
Jis yra pajėgus veikti kaip atskaitos taškas ir kreiptis į kitas viešąsias ir privačias nacionalinio lygmens organizacijas, kad rinktų ir analizuotų informaciją apie kibernetinio saugumo grėsmes ir incidentus ir prisidėtų prie tarpvalstybinio SOC veiklos. Jis aprūpinamas naujausiomis technologijomis, kuriomis galima aptikti, kaupti ir analizuoti su kibernetinio saugumo grėsmėmis ir incidentais susijusius duomenis.	Jis yra pajėgus veikti kaip atskaitos taškas ir kreiptis į kitas viešąsias ir privačias***, o prireikus ir karines*** nacionalinio lygmens organizacijas, kad rinktų ir analizuotų informaciją apie kibernetinio saugumo grėsmes ir incidentus ir prisidėtų prie tarpvalstybinio SOC veiklos. Jis aprūpinamas naujausiomis technologijomis, kuriomis galima aptikti, kaupti ir analizuoti su kibernetinio saugumo grėsmėmis ir incidentais susijusius duomenis.

Pakeitimas 35

Pasiūlymas dėl reglamento
4 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Paskelbus kvietimą pareikšti susidomėjimą, Europos kibernetinio saugumo kompetencijos centras (ECCC) atrenka nacionalinius SOC dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktiems nacionaliniams SOC gali skirti dotacijas šių priemonių ir infrastruktūros veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 50 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas padengia valstybė narė. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir nacionalinis SOC sudaro	2. Paskelbus kvietimą pareikšti susidomėjimą, Europos kibernetinio saugumo kompetencijos centras (ECCC) atrenka nacionalinius SOC dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktiems nacionaliniams SOC gali skirti dotacijas šių priemonių ir infrastruktūros veikimui finansuoti***, laikantis griežtos sąlygos, kad tokiomis priemonėmis ir infrastruktūra aprūpina patikimi paslaugų teikėjai, kaip nurodyta 16 straipsnyje***. Sąjungos finansiniu įnašu padengiama iki 50 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas

prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.	padengia valstybė narė. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir nacionalinis SOC sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.

Pakeitimas 36

Pasiūlymas dėl reglamento
5 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Paskelbus kvietimą pareikšti susidomėjimą, ECCC atrenka prieglobos konsorciumą dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktam prieglobos konsorciumui gali skirti dotaciją priemonių ir infrastruktūros veikimui finansuoti. Sąjungos finansiniu įnašu padengiama iki 75 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas padengia prieglobos konsorciumas. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir prieglobos konsorciumas sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.	2. Paskelbus kvietimą pareikšti susidomėjimą, ECCC atrenka prieglobos konsorciumą dalyvauti bendruose viešuosiuose priemonių ir infrastruktūros pirkimuose su ECCC. ECCC atrinktam prieglobos konsorciumui gali skirti dotaciją priemonių ir infrastruktūros veikimui finansuoti***, laikantis griežtos sąlygos, kad tokiomis priemonėmis ir infrastruktūra aprūpina patikimi paslaugų teikėjai, kaip nurodyta 16 straipsnyje***. Sąjungos finansiniu įnašu padengiama iki 75 proc. priemonių ir infrastruktūros įsigijimo išlaidų ir iki 50 proc. veiklos išlaidų, o likusias išlaidas padengia prieglobos konsorciumas. Prieš pradėdami priemonių ir infrastruktūros įsigijimo procedūrą, ECCC ir prieglobos konsorciumas sudaro prieglobos ir naudojimo susitarimą, kuriuo reglamentuojamas priemonių ir infrastruktūros naudojimas.

Pakeitimas 37

Pasiūlymas dėl reglamento
5 straipsnio 2 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	2a. bet kokia infrastruktūra arba paslaugų teikėjas, kurio kilmės šalis yra didelės rizikos trečioji valstybė,

automatiškai neįtraukiamas.

Pakeitimas 38

Pasiūlymas dėl reglamento
6 straipsnio 1 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ba) tiesiogiai padedama stiprinti dalyvaujančių narių karinius ir gynybos pajėgumus arba užkertamas kelias tiesioginei ir neišvengiamai grėsmei jų saugumui. Kadangi pažeidžiamų gynybos sektoriaus elementų išnaudojimas gali sukelti didelių trikdžių ir padaryti didelės žalos, gynybos pramonės kibernetiniam saugumui reikia specialių priemonių tiekimo grandinių, visų pirma žemesnių tiekimo grandinių subjektų, kuriems nereikia prieigos prie įslaptintos informacijos, tačiau kurie galėtų kelti didelę riziką visam sektoriui, saugumui užtikrinti. Ypač daug dėmesio turėtų būti skiriama poveikiui, kurį pažeidimas galėtų turėti, ir grėsmei manipuliuoti tinklo duomenimis, dėl ko ypatingos svarbos gynybos ištekliai gali tapti nenaudingais ar net jų operacinės sistemos nustatomos valdyti rankiniu būdu, dėl ko jos tampa neapsaugotos nuo užgrobimo.

Pakeitimas 39

Pasiūlymas dėl reglamento
6 straipsnio 1 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	bb) padedama stiprinti dalyvaujančių narių gynybos pajėgumus arba užkertamas kelias tiesioginei ir neišvengiamai jų saugumui kylančiai grėsmei užtikrinant tiekimo grandinių, visų pirma žemesnių tiekimo grandinių subjektų, kuriems nereikia prieigos prie įslaptintos informacijos, tačiau kurie

	galėtų kelti didelę riziką visam sektoriui, saugumą;

Pakeitimas 40

Pasiūlymas dėl reglamento
7 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba tebesitęsiančiu didelio masto kibernetinio saugumo incidentu, jie nepagrįstai nedelsdami pateikia atitinkamą informaciją Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (EU-CyCLONe), reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklui ir Komisijai, atsižvelgiant į jų atitinkamus krizių valdymo vaidmenis pagal Direktyvą (ES) 2022/2555.	1. Kai tarpvalstybiniai SOC gauna informacijos, susijusios su galimu arba tebesitęsiančiu didelio masto kibernetinio saugumo incidentu, jie nepagrįstai nedelsdami pateikia atitinkamą informaciją Europos ryšių palaikymo dėl kibernetinių krizių organizaciniam tinklui (EU-CyCLONe), reagavimo į kompiuterių saugumo incidentus tarnybų (CSIRT) tinklui ir Komisijai, ***įskaitant vyriausiąjį įgaliotinį ir EIVT, kai incidentas susijęs su trečiąja valstybe,*** atsižvelgiant į jų atitinkamus krizių valdymo vaidmenis pagal Direktyvą (ES) 2022/2555.

Pakeitimas 41

Pasiūlymas dėl reglamento
8 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina aukštą Europos kibernetinio saugumo skydo infrastruktūros duomenų saugumo ir fizinio saugumo lygį ir užtikrina, kad infrastruktūra būtų tinkamai valdoma ir kontroliuojama taip, kad būtų apsaugota nuo grėsmių ir būtų užtikrintas jos ir sistemų, įskaitant ***duomenis***, kuriais keičiamasi per infrastruktūrą, saugumas.	1. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina aukštą Europos kibernetinio saugumo skydo infrastruktūros duomenų saugumo ir fizinio saugumo lygį ir užtikrina, kad infrastruktūra būtų tinkamai valdoma ir kontroliuojama taip, kad būtų apsaugota nuo grėsmių ir būtų užtikrintas jos ir sistemų ***saugumas, mažinant riziką ir skatinant ES technologinį pranašumą ypatingos svarbos sektoriuose***, įskaitant ***priemones, kuriomis apribojamas didelės rizikos tiekėjų dalyvavimas arba jie pašalinami, taip pat apsaugotas duomenų***, kuriais keičiamasi per infrastruktūrą,

saugumas.

Pakeitimas 42

Pasiūlymas dėl reglamento
8 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina, kad dalijimasis informacija Europos kibernetinio saugumo skydo sistemoje su subjektais, kurie nėra valstybių narių viešosios įstaigos, nedarytų neigiamo poveikio Sąjungos saugumo interesams.	2. Europos kibernetinio saugumo skydo veikloje dalyvaujančios valstybės narės užtikrina, kad dalijimasis informacija Europos kibernetinio saugumo skydo sistemoje su subjektais, kurie nėra valstybių narių viešosios įstaigos, nedarytų neigiamo poveikio Sąjungos saugumo interesams ***ir kad bet koks dalijimasis informacija su didelės rizikos tiekėjais būtų ribotos apimties ir nedarytų žalos Sąjungos saugumui ir strateginiams interesams***.

Pakeitimas 43

Pasiūlymas dėl reglamento
8 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi techniniai reikalavimai, kurių laikydamosi valstybės narės vykdo 1 ir 2 dalyse nustatytą pareigą. Tie įgyvendinimo aktai priimami laikantis šio reglamento 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Tai darydama Komisija, padedama vyriausiojo įgaliotinio, atsižvelgia į atitinkamus gynybos lygio saugumo standartus, kad palengvintų bendradarbiavimą su kariniais subjektais.	3. Komisija gali priimti įgyvendinimo aktus, kuriais nustatomi techniniai reikalavimai, kurių laikydamosi valstybės narės vykdo 1 ir 2 dalyse nustatytą pareigą. Tie įgyvendinimo aktai priimami laikantis šio reglamento 21 straipsnio 2 dalyje nurodytos nagrinėjimo procedūros. Tai darydama Komisija, padedama vyriausiojo įgaliotinio, atsižvelgia į atitinkamus gynybos lygio saugumo standartus, kad palengvintų bendradarbiavimą su kariniais subjektais***, tinkamai pasinaudodama visomis civilinėms ir karinėms bendruomenėms prieinamomis gynybos galimybėmis platesnio masto ES saugumui ir gynybai užtikrinti, ir apie tai informuoja Europos Parlamentą***.

Pakeitimas 44

Pasiūlymas dėl reglamento
9 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Veiksmai, kuriais įgyvendinamas Reagavimo į kibernetinio saugumo krizes mechanizmas, remiami Skaitmeninės Europos programos lėšomis ir įgyvendinami pagal Reglamentą (ES) 2021/694, visų pirma jo 3 konkretų tikslą.	2. Veiksmai, kuriais įgyvendinamas Reagavimo į kibernetinio saugumo krizes mechanizmas, remiami Skaitmeninės Europos programos lėšomis ir įgyvendinami pagal Reglamentą (ES) 2021/694, visų pirma jo 3 konkretų tikslą***, o įgyvendinant pagalbos priemones trečiosiose valstybėse, visų pirma Ukrainoje ir Moldovoje, – pagal Europos taikos priemonę (ETP)***.

Pakeitimas 45

Pasiūlymas dėl reglamento
10 straipsnio 1 dalies a punktas

Komisijos siūlomas tekstas	*Pakeitimas*
a) pasirengimo veiksmai, įskaitant koordinuotą subjektų, veikiančių itin svarbiuose sektoriuose visoje Sąjungoje, parengties testavimą;	a) pasirengimo veiksmai, įskaitant koordinuotą subjektų, veikiančių itin svarbiuose sektoriuose***, pavyzdžiui, viešosios infrastruktūros, rinkimų infrastruktūros, transporto, sveikatos priežiūros, finansų, telekomunikacijų, maisto tiekimo ir saugumo sektoriuose*** visoje Sąjungoje, parengties testavimą;

Pakeitimas 46

Pasiūlymas dėl reglamento
10 straipsnio 1 dalies c punktas

Komisijos siūlomas tekstas	*Pakeitimas*
c) savitarpio pagalbos veiksmai, t. y. pagalba, kurią vienos valstybės narės nacionalinės institucijos teikia kitai valstybei narei, visų pirma kaip nustatyta	c) savitarpio pagalbos veiksmai, t. y. pagalba, kurią vienos valstybės narės nacionalinės institucijos teikia kitai valstybei narei, visų pirma kaip nustatyta

Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies f punkte**.**	Direktyvos (ES) 2022/2555 11 straipsnio 3 dalies f punkte***, taip pat pagal ES sutarties 42 straipsnio 7 dalį ir SESV 222 straipsnį;***

Pakeitimas 47

Pasiūlymas dėl reglamento
10 straipsnio 1 dalies c a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ca) aukštos rizikos tiekėjų, kurie prieštarautų Sąjungos ir jos valstybių narių saugumo ir gynybos interesams, kaip nustatyta BUSP sistemoje pagal Europos Sąjungos sutarties V antraštinę dalį, ypatingos svarbos įrangos pakeitimas ir veiklos nutraukimas.

Pakeitimas 48

Pasiūlymas dėl reglamento
11 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. TIS bendradarbiavimo grupė, bendradarbiaudama su Komisija, ENISA ir ***vyriausiuoju įgaliotiniu***, parengia bendrus rizikos scenarijus ir koordinuoto testavimo metodikas.	2. TIS bendradarbiavimo grupė, bendradarbiaudama su Komisija, ENISA***, vyriausiuoju įgaliotiniu, EIVT*** ir***, kai tikslinga, su EGA***, parengia bendrus rizikos scenarijus ir koordinuoto testavimo metodikas.

Pakeitimas 49

Pasiūlymas dėl reglamento
12 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. ES kibernetinio saugumo rezervą sudaro reagavimo į incidentus paslaugos, kurias teikia patikimi paslaugų teikėjai, atrinkti pagal 16 straipsnyje nustatytus kriterijus. Į rezervą įtraukiamos iš anksto įsipareigotos teikti paslaugos. Paslaugos	2. ES kibernetinio saugumo rezervą sudaro reagavimo į incidentus paslaugos, kurias teikia patikimi paslaugų teikėjai, atrinkti pagal 16 straipsnyje nustatytus kriterijus. Į rezervą įtraukiamos iš anksto įsipareigotos teikti paslaugos. Paslaugos

diegiamos visose valstybėse narėse.	diegiamos visose valstybėse narėse ***ir trečiosiose valstybėse, kurios atitinka taikomus šio reglamento reikalavimus***.

Pakeitimas 50

Pasiūlymas dėl reglamento
12 straipsnio 3 dalies b punktas

Komisijos siūlomas tekstas	*Pakeitimas*
b) Sąjungos institucijos, įstaigos ir agentūros.	b) Sąjungos institucijos, įstaigos ir agentūros***, įskaitant BSGP misijas***.

Pakeitimas 51

Pasiūlymas dėl reglamento
12 straipsnio 4 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
4. 3 dalies a punkte nurodyti naudotojai naudojasi ES kibernetinio saugumo rezervo paslaugomis, kad reaguotų į reikšmingus arba didelio masto incidentus, darančius poveikį ypatingos svarbos ar itin svarbiuose sektoriuose veikiantiems subjektams, arba padėtų į juos reaguoti ir nedelsiant po jų atkurti veiklą.	4. 3 dalies a punkte nurodyti naudotojai naudojasi ES kibernetinio saugumo rezervo paslaugomis, kad reaguotų į reikšmingus arba didelio masto incidentus, darančius poveikį ypatingos svarbos ar itin svarbiuose sektoriuose***, pavyzdžiui, viešosios infrastruktūros, rinkimų infrastruktūros, transporto, sveikatos priežiūros, finansų, telekomunikacijų, maisto tiekimo ir saugumo sektoriuose*** veikiantiems subjektams, arba padėtų į juos reaguoti ir nedelsiant po jų atkurti veiklą.

Pakeitimas 52

Pasiūlymas dėl reglamento
12 straipsnio 5 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
5. Komisijai tenka bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Komisija, atsižvelgdama į 3 dalyje nurodytų naudotojų poreikius,	5. Komisijai tenka bendra atsakomybė už ES kibernetinio saugumo rezervo įgyvendinimą. Komisija, atsižvelgdama į 3 dalyje nurodytų naudotojų poreikius,

nustato ES kibernetinio saugumo rezervo prioritetus ir raidą, prižiūri jo įgyvendinimą ir užtikrina papildomumą, nuoseklumą, sinergiją ir sąsajas su kitais paramos veiksmais pagal šį reglamentą, taip pat su kitais Sąjungos veiksmais ir programomis.	nustato ES kibernetinio saugumo rezervo prioritetus ir raidą, prižiūri jo įgyvendinimą ir užtikrina papildomumą, nuoseklumą, sinergiją ir sąsajas su kitais paramos veiksmais pagal šį reglamentą, taip pat su kitais Sąjungos veiksmais ir programomis ***bei tikslais, visų pirma strateginiu tikslu mažinti priklausomybę nuo didelės rizikos tiekėjų, kurie prieštarautų Sąjungos ir jos valstybių narių saugumo ir gynybos interesams, kaip nustatyta BUSP sistemoje pagal Europos Sąjungos sutarties V antraštinę dalį***.

Pakeitimas 53

Pasiūlymas dėl reglamento
12 straipsnio 7 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
7. Siekdama padėti Komisijai sukurti ES kibernetinio saugumo rezervą, ENISA, pasikonsultavusi su valstybėmis narėmis ir Komisija, parengia reikiamų paslaugų aprašą. ENISA, pasikonsultavusi su Komisija, parengia panašų aprašą, kad nustatytų trečiųjų valstybių, galinčių gauti paramą iš ES kibernetinio saugumo rezervo pagal 17 straipsnį, poreikius. Kai tikslinga, Komisija konsultuojasi su vyriausiuoju įgaliotiniu.	7. Siekdama padėti Komisijai sukurti ES kibernetinio saugumo rezervą, ENISA, pasikonsultavusi su valstybėmis narėmis ir Komisija, parengia reikiamų paslaugų aprašą. ENISA, ***padedama EIVT ir*** pasikonsultavusi su Komisija, parengia panašų aprašą, kad nustatytų trečiųjų valstybių, galinčių gauti paramą iš ES kibernetinio saugumo rezervo pagal 17 straipsnį, poreikius. Kai tikslinga, Komisija konsultuojasi su vyriausiuoju įgaliotiniu.

Pakeitimas 54

Pasiūlymas dėl reglamento
14 straipsnio 2 dalies a a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) incidento poveikį Sąjungos saugumui ir gynybai;

Pakeitimas 55

Pasiūlymas dėl reglamento
15 straipsnio 3 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
3. Konsultuojantis su vyriausiuoju įgaliotiniu, parama pagal reagavimo į kibernetinio saugumo krizes mechanizmą gali papildyti pagal bendrą užsienio ir saugumo politiką ir bendrą saugumo ir gynybos politiką teikiamą pagalbą, be kita ko, pasitelkiant greitojo reagavimo į kibernetines grėsmes grupes. Ji taip pat gali papildyti vienos valstybės narės kitai valstybei narei teikiamą pagalbą pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį arba ja gali būti prisidedama prie tokios pagalbos.	3. Konsultuojantis su vyriausiuoju įgaliotiniu, parama pagal reagavimo į kibernetinio saugumo krizes mechanizmą gali papildyti pagal bendrą užsienio ir saugumo politiką ir bendrą saugumo ir gynybos politiką teikiamą pagalbą, be kita ko, pasitelkiant greitojo reagavimo į kibernetines grėsmes grupes***, siekiant geriau remti ES valstybes nares, BSGP misijas ir operacijas bei tas trečiąsias valstybes, visų pirma Ukrainą ir Moldovą, kurios savo pastangas stiprinti kibernetinės gynybos pajėgumus suderino su ES bendra užsienio ir saugumo politika bei bendra saugumo ir gynybos politika***. Ji taip pat gali papildyti vienos valstybės narės kitai valstybei narei teikiamą pagalbą pagal Europos Sąjungos sutarties 42 straipsnio 7 dalį arba ja gali būti prisidedama prie tokios pagalbos.

Pakeitimas 56

Pasiūlymas dėl reglamento
16 straipsnio 2 dalies b a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	aa) paslaugų teikėjas įrodo, kad jo sprendimų priėmimo ir valdymo struktūroms nedaroma jokia nederama valstybių vyriausybių įtaka, kuri prieštarautų Sąjungos ir jos valstybių narių saugumo ir gynybos interesams, kaip nustatyta BUSP sistemoje pagal Europos Sąjungos sutarties V antraštinę dalį;

Pakeitimas 57

Pasiūlymas dėl reglamento
16 straipsnio 2 dalies f punktas

Komisijos siūlomas tekstas	*Pakeitimas*
f) paslaugų teikėjas turi techninę ir programinę įrangą, kurios reikia prašomai paslaugai teikti;	f) paslaugų teikėjas turi techninę ir programinę įrangą, kurios reikia prašomai paslaugai teikti***, ir atitinka Reglamento XX/XXXX (Kibernetinio atsparumo akto) X straipsnyje nustatytus reikalavimus***;

Pakeitimas 58

Pasiūlymas dėl reglamento
16 straipsnio 2 dalies j a punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	ja) paslaugų teikėjas, kurio kilmės šalis yra didelės rizikos trečioji valstybė, nėra priimtinas.

Pakeitimas 59

Pasiūlymas dėl reglamento
16 straipsnio 2 dalies j b punktas (naujas)

Komisijos siūlomas tekstas	*Pakeitimas*
	jb) jei įmanoma, paslaugų teikėjas glaudžiai bendradarbiauja su atitinkamomis MVĮ;

Pakeitimas 60

Pasiūlymas dėl reglamento
17 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Trečiosios valstybės gali prašyti paramos iš ES kibernetinio saugumo rezervo, jei tai numatyta sudarytuose asociacijos susitarimuose dėl jų	1. Trečiosios valstybės gali prašyti paramos iš ES kibernetinio saugumo rezervo, jeigu:

dalyvavimo Skaitmeninės Europos programoje.	
	a) tai numatyta sudarytuose asociacijos susitarimuose dėl jų dalyvavimo Skaitmeninės Europos programoje;
	b) jose vykdoma BSGP misija, kuriai suteikti specialūs įgaliojimai stiprinti atsparumą hibridinėms grėsmėms, įskaitant kibernetines grėsmes, arba taikoma ETP pagalbos priemonė, skirta tos valstybės kibernetiniam atsparumui stiprinti.

Pakeitimas 61

Pasiūlymas dėl reglamento
17 straipsnio 2 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
2. Parama iš ES kibernetinio saugumo rezervo teikiama pagal šį reglamentą ir visas ***1*** dalyje nurodytuose asociacijos susitarimuose nustatytas specialiąsias sąlygas.	2. Parama iš ES kibernetinio saugumo rezervo teikiama pagal šį reglamentą ir visas dalyje nurodytuose asociacijos susitarimuose nustatytas specialiąsias sąlygas***, išskyrus tas trečiąsias valstybes, kurioms taikomos 1 dalies b punkte išdėstytos nuostatos***.

Pakeitimas 62

Pasiūlymas dėl reglamento
18 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
1. Komisijos, EU-CyCLONe arba CSIRT tinklo prašymu ENISA peržiūri ir įvertina su konkrečiu reikšmingu arba didelio masto kibernetinio saugumo incidentu susijusias grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus. Užbaigusi incidento peržiūrą ir vertinimą, ENISA pateikia incidento peržiūros ataskaitą CSIRT tinklui, EU-CyCLONe ir Komisijai, kad padėtų joms atlikti savo užduotis, visų pirma užduotis,	1. Komisijos, EU-CyCLONe arba CSIRT tinklo prašymu ENISA peržiūri ir įvertina su konkrečiu reikšmingu arba didelio masto kibernetinio saugumo incidentu susijusias grėsmes, pažeidžiamumus ir poveikio švelninimo veiksmus. Užbaigusi incidento peržiūrą ir vertinimą, ENISA pateikia incidento peržiūros ataskaitą CSIRT tinklui, EU-CyCLONe ir Komisijai, kad padėtų joms atlikti savo užduotis, visų pirma užduotis,

nustatytas Direktyvos (ES) 2022/2555 15 ir 16 straipsniuose. Kai aktualu, Komisija ataskaita dalijasi su vyriausiuoju įgaliotiniu.	nustatytas Direktyvos (ES) 2022/2555 15 ir 16 straipsniuose. Kai aktualu, ***ypač kai incidentas susijęs su trečiąja valstybe,*** Komisija ataskaita dalijasi su vyriausiuoju įgaliotiniu ***ir EIVT***.

Pakeitimas 63

Pasiūlymas dėl reglamento
18 straipsnio 3 a dalis (nauja)

Komisijos siūlomas tekstas	*Pakeitimas*
	3a. Ataskaita dalijamasi su Europos Parlamentu laikantis Sąjungos arba nacionalinės teisės dėl neskelbtinos įslaptintos informacijos apsaugos.

Pakeitimas 64

Pasiūlymas dėl reglamento
19 straipsnio 1 dalies 1 punkto a papunkčio 1 punktas
Reglamentas (ES) 2021/694
6 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
aa) remti ES kibernetinio saugumo skydo plėtojimą, įskaitant nacionalinių ir tarpvalstybinių SOC platformų, kurios padeda didinti informuotumą apie padėtį Sąjungoje ir stiprinti Sąjungos kibernetinių grėsmių žvalgybos pajėgumus, kūrimą, diegimą ir veikimą;	aa) remti ES kibernetinio saugumo skydo plėtojimą, įskaitant nacionalinių ir tarpvalstybinių SOC platformų, kurios padeda didinti informuotumą apie padėtį Sąjungoje ir stiprinti Sąjungos kibernetinių grėsmių žvalgybos pajėgumus ***bei mažinti Sąjungos priklausomybę nuo didelės rizikos ypatingos svarbos kibernetinio saugumo įrangos ar komponentų tiekėjų***, ***kurie prieštarautų Sąjungos ir jos valstybių narių saugumo ir gynybos interesams, kaip nustatyta BUSP sistemoje pagal Europos Sąjungos sutarties V antraštinę dalį,*** kūrimą, diegimą ir veikimą;

Pakeitimas 65

Pasiūlymas dėl reglamento
20 straipsnio 1 dalis

Komisijos siūlomas tekstas	*Pakeitimas*
Iki ***[ketveri*** metai nuo šio reglamento taikymo pradžios ***dienos]*** Komisija pateikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitą.	Iki ***[treji*** metai nuo šio reglamento taikymo pradžios ***dienos ir vėliau kas dvejus metus]*** Komisija pateikia Europos Parlamentui ir Tarybai šio reglamento vertinimo ir peržiūros ataskaitą.

NUOMONĘ TEIKIANČIO KOMITETO PROCEDŪRA

Pavadinimas	Solidarumo stiprinimo ir pajėgumo aptikti kibernetinio saugumo grėsmes ir incidentus Sąjungoje, jiems pasirengti ir į juos reaguoti didinimo priemonių nustatymas
Nuorodos	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Atsakingas komitetas Paskelbimo plenariniame posėdyje data	ITRE 1.6.2023
Nuomonę pateikė Paskelbimo plenariniame posėdyje data	AFET 1.6.2023
Nuomonės referentas (-ė) Paskyrimo data	Dragoş Tudorache 16.6.2023
Svarstymas komitete	18.9.2023
Priėmimo data	24.10.2023
Galutinio balsavimo rezultatai	+: 39 –: 4 0: 0
Posėdyje per galutinį balsavimą dalyvavę nariai	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
Posėdyje per galutinį balsavimą dalyvavę pavaduojantys nariai	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

GALUTINIS VARDINIS BALSAVIMAS NUOMONĘ TEIKIANČIAME KOMITETE

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

Sutartiniai ženklai:
+ : už
- : prieš
0 : susilaikė