Европейски парламент
2019 – 2024

Комисия по външни работи

2023/0109(COD)

27.10.2023

СТАНОВИЩЕ

на комисията по външни работи

на вниманието на комисията по промишленост, изследвания и енергетика

относно предложението за регламент на Европейския парламент и на Съвета за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

Докладчик по становище: Драгош Тудораке

PA_Legam

Изменение 1

Предложение за регламент
Съображение 1

Текст, предложен от Комисията	*Изменение*
(1) Всички сектори на икономиката използват и се осланят на информационните и комуникационните технологии като съществен компонент на дейността си, тъй като нашите публични администрации, предприятия и граждани са повече от всякога тясно свързани и взаимозависими отвъд секторните и териториалните граници.	(1) Всички сектори на икономиката ***и военната област*** използват и се осланят на информационните и комуникационните технологии като съществен компонент на дейността си, тъй като нашите публични администрации, предприятия и граждани***, а също така и участниците от военната сфера и от сферата на отбраната,*** са повече от всякога тясно свързани и взаимозависими отвъд секторните и териториалните граници.

Изменение 2

Предложение за регламент
Съображение 2

Текст, предложен от Комисията	*Изменение*
(2) Мащабът, честотата и въздействието на киберинцидентите се увеличават, включително атаките по веригата на доставки, целящи кибершпионаж, софтуер за изнудване или смущения. Те представляват съществена заплаха за функционирането на мрежовите и информационните системи. С оглед на бързо променящата се картина на заплахите, заплахата от възможни мащабни инциденти, причиняващи значителни смущения или вреди на критичните инфраструктури, изисква повишена готовност на всички нива на рамката за киберсигурност на Съюза. ***Тази заплаха надхвърля*** рамките на военната агресия на Русия в Украйна и е вероятно да ***продължи*** да ***съществува***, като се има предвид многообразието от свързани с държави участници, престъпни участници и	(2) Мащабът, честотата и въздействието на киберинцидентите се увеличават, включително атаките по веригата на доставки, целящи кибершпионаж, софтуер за изнудване или смущения. Те представляват съществена заплаха за функционирането на мрежовите и информационните системи. С оглед на бързо променящата се картина на заплахите, заплахата от възможни мащабни инциденти, причиняващи значителни смущения или вреди на критичните инфраструктури, изисква повишена готовност на всички нива на рамката за киберсигурност на Съюза. ***Сериозността на тези заплахи придоби още по-голямо значение поради завръщането на войната на нашия континент. Тези заплахи надхвърлят*** рамките на военната агресия на Русия в Украйна и е вероятно

хактивисти, замесени в настоящото геополитическо напрежение. Такива инциденти могат да възпрепятстват предоставянето на обществени услуги и осъществяването на икономически дейности, включително в критични или висококритични сектори, да доведат до значителни финансови загуби, да нарушат доверието на потребителите, да нанесат големи вреди на икономиката на Съюза и дори да имат застрашаващи здравето или живота последици. Освен това киберинцидентите са непредвидими, тъй като често възникват и се развиват за много кратък период от време, не се ограничават в рамките на определен географски район и се случват едновременно или се разпространяват мигновено в много държави.	да ***продължат*** да ***съществуват***, като се има предвид многообразието от свързани с държави участници, престъпни участници и хактивисти, замесени в настоящото геополитическо напрежение. Такива инциденти могат да възпрепятстват предоставянето на обществени услуги и осъществяването на икономически дейности, включително в критични или висококритични сектори, да доведат до значителни финансови загуби, да нарушат доверието на потребителите, да нанесат големи вреди на икономиката ***и сигурността*** на Съюза и дори да имат застрашаващи здравето или живота последици***, като евентуално накърняват местните или националните съоръжения, свързани със сигурността***. Освен това киберинцидентите са непредвидими, тъй като често възникват и се развиват за много кратък период от време, не се ограничават в рамките на определен географски район и се случват едновременно или се разпространяват мигновено в много държави. ***Киберсигурността е важна за защитата на нашите европейски ценности и гарантира функционирането на нашите демокрации, като предпазва избирателната ни инфраструктура и демократичните процедури от всякаква външна намеса.***

Изменение 3

Предложение за регламент
Съображение 2а (ново)

Текст, предложен от Комисията	*Изменение*
	(2а) Киберсигурността е от решаващо значение за безопасността на нашия Съюз и за предотвратяване на подкопаването на нашата демокрация, икономика и сигурност

от страна на злонамерени участници, държавни и недържавни. Необходимо е да се предотврати създаването на разпокъсана картина, тъй като подобна ситуация не би представлявала подходящ подход, по-специално когато сме изправени пред предизвикателството на бъдеща широкомащабна кибератака, насочена едновременно към няколко държави членки или транснационална критична инфраструктура. Ето защо е необходим орган на Съюза, който да действа като координационна платформа за всички съществуващи и бъдещи инструменти, фондове и механизми за киберсигурност.

Изменение 4

Предложение за регламент
Съображение 3

Текст, предложен от Комисията	*Изменение*
(3) Необходимо е да се укрепи конкурентната позиция на промишлеността и сектора на услугите в Съюза в рамките на цифровизираната икономика, както и да се подкрепи тяхната цифрова трансформация, като се повиши нивото на киберсигурност на цифровия единен пазар. Както се препоръчва в три различни предложения на Конференцията за бъдещето на Европа[16], необходимо е да се повиши устойчивостта на гражданите, предприятията и субектите, извършващи дейност в критични инфраструктури, срещу нарастващите киберзаплахи, които могат да имат опустошителни последици за обществото и икономиката. Ето защо са необходими инвестиции в инфраструктури и услуги, които ще подпомогнат по-бързото откриване и реагиране при киберзаплахи и	(3) Необходимо е да се укрепи конкурентната позиция на промишлеността и сектора на услугите в Съюза в рамките на цифровизираната икономика, както и да се подкрепи тяхната цифрова трансформация, като се повиши нивото на киберсигурност на цифровия единен пазар. Както се препоръчва в три различни предложения на Конференцията за бъдещето на Европа[16], необходимо е да се повиши устойчивостта на гражданите, предприятията и субектите, извършващи дейност в критични инфраструктури, срещу нарастващите киберзаплахи, които могат да имат опустошителни последици за обществото и икономиката. Ето защо са необходими инвестиции в инфраструктури и услуги, които ще подпомогнат по-бързото откриване и реагиране при киберзаплахи и

инциденти, а държавите членки се нуждаят от помощ, за да се подготвят, както и да реагират по-добре в случай на значителни и мащабни киберинциденти. Съюзът следва също така да увеличи способностите си в тези области, особено по отношение на събирането и анализирането на данни за киберзаплахите и инцидентите.

инциденти, а държавите членки се нуждаят от помощ, за да се подготвят, както и да реагират по-добре в случай на значителни и мащабни киберинциденти. Съюзът следва също така да увеличи способностите си в тези области, особено по отношение на събирането и анализирането на данни за киберзаплахите и инцидентите***, както и своята способност да действа проактивно и да реагира решително на киберзаплахите и инцидентите***.

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

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

Изменение 5

Предложение за регламент
Съображение 4

Текст, предложен от Комисията	*Изменение*
(4) Съюзът вече е предприел редица мерки за намаляване на уязвимостта и повишаване на устойчивостта на критичните инфраструктури и субектите срещу киберрисковете, по-специално Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[17], Препоръка (ЕС) 2017/1584 на Комисията[18], Директива 2013/40/ЕС на Европейския парламент и на Съвета[19] и Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[20]. В допълнение в препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение държавите членки се приканват да предприемат спешни и ефективни мерки и да си сътрудничат лоялно, ефикасно, солидарно и координирано помежду си, с Комисията и с други съответни публични органи, както и със съответните субекти, за да повишат устойчивостта на инфраструктурата от критично	(4) Съюзът вече е предприел редица мерки за намаляване на уязвимостта и повишаване на устойчивостта на критичните инфраструктури и субектите срещу киберрисковете, по-специално Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[17], Препоръка (ЕС) 2017/1584 на Комисията[18], Директива 2013/40/ЕС на Европейския парламент и на Съвета[19] и Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[20]. В допълнение в препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение държавите членки се приканват да предприемат спешни и ефективни мерки и да си сътрудничат лоялно, ефикасно ***и проактивно***, солидарно и координирано помежду си, с Комисията и с други съответни публични органи, както и със съответните субекти, за да повишат устойчивостта на инфраструктурата от

значение, използвана за предоставяне на основни услуги на вътрешния пазар.

критично значение, използвана за предоставяне на основни услуги на вътрешния пазар. ***Освен това през март 2022 г. Съюзът одобри и пусна в действие своя Стратегически компас, който се фокусира, наред с другото, върху укрепването на киберсигурността и засилването на международното сътрудничество с единомислещи съюзници и демократични партньори, особено в тази област. Освен това киберсигурността е централен елемент в неотдавнашната трета съвместна декларация относно сътрудничеството между ЕС и НАТО от януари 2023 г. По-специално, в окончателния доклад за оценка на работната група ЕС-НАТО се препоръчва пълноценно използване на полезните взаимодействия между ЕС и НАТО[1], включително обмен на най-добри практики между гражданските и военните действащи лица относно прилагането на съответните политики и законодателство, свързани с киберпространството.***

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

---

[17] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ L 333, 27.12.2022 г.).

[18] Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

[17] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ L 333, 27.12.2022 г.).

[18] Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

[19] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8.).

[20] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

[19] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8.).

[20] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15).

Изменение 6

Предложение за регламент
Съображение 6

Текст, предложен от Комисията	*Изменение*
(6) В съвместното съобщение „Политика на ЕС за киберотбрана“[22], прието на 10 ноември 2022 г., беше обявена инициатива на ЕС за киберсолидарност със следните цели: укрепване на общите способности на ЕС за откриване, ситуационна осведоменост и реагиране чрез насърчаване на разгръщането на инфраструктура на ЕС от центрове за операции по сигурността (ЦОС), подпомагане на постепенното изграждане на резерв за киберсигурност на равнището на ЕС от услуги от доверителни частни доставчици и изпитване на критични субекти за потенциални уязвимости въз основа на оценки на риска на ЕС.	(6) В съвместното съобщение „Политика на ЕС за киберотбрана“[22], прието на 10 ноември 2022 г., беше обявена инициатива на ЕС за киберсолидарност със следните цели: укрепване на общите способности на ЕС за откриване, ситуационна осведоменост и реагиране чрез насърчаване на разгръщането на инфраструктура на ЕС от центрове за операции по сигурността (ЦОС), подпомагане на постепенното изграждане на резерв за киберсигурност на равнището на ЕС от услуги от доверителни частни доставчици и изпитване на критични субекти за потенциални уязвимости въз основа на оценки на риска на ЕС. ***Освен това бързо променящата се картина на киберзаплахите и бързият темп на технологично развитие също показват необходимостта от засилена гражданско-военна***

	координация и сътрудничество, както се подчертава в заключенията на Съвета относно политиката на ЕС за киберотбрана[1].
	[1] Заключения на Съвета относно политиката на ЕС за киберотбрана, одобрени от Съвета на заседанието му от 22 май 2023 г. (9618/23)
_____	_____
[22] Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN/2022/49 final.	[22] Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN/2022/49 final.

Изменение 7

Предложение за регламент
Съображение 6а (ново)

Текст, предложен от Комисията	*Изменение*
	(6а) Като се има предвид размиването на границите между гражданските и военните въпроси и двойната употреба на киберинструментите и технологиите, е необходим всеобхватен и цялостен подход към областта на цифровите технологии. В случай на мащабен инцидент и криза в областта на киберсигурността, засягащи повече от една държава членка, следва да се установят подходящо управление и справяне с кризи. Тези структури следва да организират обмена на информация, координацията и сътрудничеството със структурите на Съюза за външна сигурност и управление на военни кризи и с органите на държавите членки, отговарящи за сигурността и отбраната (общността за киберотбрана). Това следва да се отнася и до операциите и мисиите по линия на общата политика за

сигурност и отбрана, провеждани от Съюза за гарантиране на мира и стабилността в съседните му държави и извън тях.

Изменение 8

Предложение за регламент
Съображение 7

Текст, предложен от Комисията	*Изменение*
(7) Необходимо е да се подобрят откриването и ситуационната осведоменост по отношение на киберзаплахите и инцидентите в целия Съюз, както и да се укрепи солидарността чрез повишаване на готовността и способностите на държавите членки и на Съюза за реагиране при значителни и мащабни киберинциденти. Поради това следва да бъде разгърната общоевропейска инфраструктура от ЦОС (европейски киберщит) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост; следва да бъде създаден Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти; следва да бъде създаден европейски Механизъм за преглед на киберинциденти, чрез който да се разглеждат и оценяват конкретни значителни или мащабни киберинциденти. Тези действия не засягат членове 107 и 108 от Договора за функционирането на Европейския съюз („ДФЕС“).	(7) Необходимо е да се подобрят откриването и ситуационната осведоменост по отношение на киберзаплахите и инцидентите в целия Съюз, както и да се укрепи солидарността чрез повишаване на готовността и способностите на държавите членки и на Съюза за реагиране при значителни и мащабни киберинциденти. Поради това следва да бъде разгърната общоевропейска инфраструктура от ЦОС (европейски киберщит) за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост; следва да бъде създаден Механизъм за действие при извънредни ситуации в областта на киберсигурността, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни киберинциденти***, включително инцидентите, в които са въвлечени повече от една държава членка. Когато е възможно и необходимо, Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да организира споделяне на информация и сътрудничество с органите за отбрана на държавите членки и да се подпомага от институциите, органите и агенциите на ЕС (общността на ЕС за киберотбрана)***; следва да бъде създаден европейски Механизъм за преглед на

киберинциденти, чрез който да се разглеждат и оценяват конкретни значителни или мащабни киберинциденти. ***Тези нови структури следва също така да подкрепят операциите и мисиите на ЕС по линия на ОПСО.*** Тези действия не засягат членове 107 и 108 от Договора за функционирането на Европейския съюз („ДФЕС“).

Изменение 9

Предложение за регламент
Съображение 11

Текст, предложен от Комисията	*Изменение*
(11) За целите на доброто финансово управление следва да се определят специални правила за пренасяне на неизползваните бюджетни кредити за поети задължения и за плащания. При спазване на принципа, че бюджетът на Съюза се определя ежегодно, в настоящия регламент следва, предвид непредвидимия, извънреден и специфичен характер на положението в областта на киберсигурността, да се предвидят възможности за пренасяне на неизползвани средства извън определените във Финансовия регламент, като по този начин се увеличи максимално капацитетът на Механизма за действие при извънредни ситуации в областта на киберсигурността за подпомагане на държавите членки в ефективното противодействие на киберзаплахите.	(11) За целите на доброто финансово управление следва да се определят специални правила за пренасяне на неизползваните бюджетни кредити за поети задължения и за плащания. При спазване на принципа, че бюджетът на Съюза се определя ежегодно, в настоящия регламент следва, предвид непредвидимия, извънреден и специфичен характер на положението в областта на киберсигурността, да се предвидят възможности за пренасяне на неизползвани средства извън определените във Финансовия регламент, като по този начин се увеличи максимално капацитетът на Механизма за действие при извънредни ситуации в областта на киберсигурността за подпомагане на държавите членки в ефективното противодействие на киберзаплахите. ***Тези специфични правила ще позволят също така по-дългосрочна финансова подкрепа за съвместно възлагане на обществени поръчки за свръхсигурни инструменти и инфраструктура от следващо поколение с цел подобряване на капацитета за колективно разкриване чрез използване на най-***

	новите постижения в областта на изкуствения интелект (ИИ) и анализа на данни.

Изменение 10

Предложение за регламент
Съображение 13

Текст, предложен от Комисията	*Изменение*
(13) Всяка държава членка следва да определи публичен орган на национално равнище, натоварен със задачата да координира дейностите по откриване на киберзаплахи в тази държава членка. Тези национални ЦОС следва да действат като отправна точка и портал на национално равнище за участие в европейския киберщит и следва да гарантират, че информацията за киберзаплахите от публични и частни субекти се споделя и събира на национално равнище по ефективен и рационализиран начин.	(13) Всяка държава членка следва да определи публичен орган на национално равнище, натоварен със задачата да координира дейностите по откриване на киберзаплахи в тази държава членка. Тези национални ЦОС следва да действат като отправна точка и портал на национално равнище за участие в европейския киберщит и следва да гарантират, че информацията за киберзаплахите от публични и частни субекти се споделя и събира на национално равнище по ефективен и рационализиран начин. ***Когато е осъществимо и необходимо, ЦОС следва също така да дават възможност за участие на структури, свързани с отбраната, като се създава „отбранителен стълб“ по отношение на управлението и вида на споделяната информация, както е посочено в съвместното съобщение относно политиката на ЕС за киберотбрана[1] и подкрепено от върховния представител.*** ***[1] Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN/2022/49 final.***

Изменение 11

Предложение за регламент
Съображение 14

Текст, предложен от Комисията	*Изменение*
(14) Като част от европейския киберщит следва да бъдат създадени редица трансгранични центрове за операции по сигурността („трансгранични ЦОС“). Те следва да обединяват национални ЦОС от поне три държави членки, за да могат да се постигнат всички ползи от трансграничното откриване на заплахи и от обмена и управлението на информация. Общата цел на трансграничните ЦОС следва да бъде укрепване на способностите за анализ, превенция и откриване на киберзаплахи и подпомагане на изготвянето на висококачествена разузнавателна информация за киберзаплахите, по-специално чрез обмен на данни от различни източници, публични или частни, както и чрез споделяне и съвместно използване на най-съвременни инструменти и съвместно развитие на способности за откриване, анализ и превенция в доверителна среда. Те следва да осигурят нов допълнителен капацитет, който да надгражда и допълва съществуващите ЦОС и екипите за реагиране при инциденти с компютърната сигурност („ЕРИКС“), както и други съответни участници.	(14) Като част от европейския киберщит следва да бъдат създадени редица трансгранични центрове за операции по сигурността („трансгранични ЦОС“). Те следва да обединяват национални ЦОС от поне три държави членки, ***включително „стълб на отбраната“,*** за да могат да се постигнат всички ползи от трансграничното откриване на заплахи и от обмена и управлението на информация. Общата цел на трансграничните ЦОС следва да бъде укрепване на способностите за анализ, превенция и откриване на киберзаплахи и подпомагане на изготвянето на висококачествена разузнавателна информация за киберзаплахите, по-специално чрез обмен на данни от различни източници, публични или частни, ***и когато е необходимо и осъществимо, военни с достатъчни насоки за обмен на информация***, както и чрез споделяне и съвместно използване на най-съвременни инструменти и съвместно развитие на способности за откриване, анализ и превенция в доверителна среда. Те следва да осигурят нов допълнителен капацитет, който да надгражда и допълва съществуващите ЦОС и екипите за реагиране при инциденти с компютърната сигурност („ЕРИКС“), както и други съответни участници.

Изменение 12

Предложение за регламент
Съображение 15

Текст, предложен от Комисията	*Изменение*
(15) На национално равнище наблюдението, откриването и анализът на киберзаплахите обикновено се	(15) На национално равнище наблюдението, откриването и анализът на киберзаплахите обикновено се

осигуряват от ЦОС от публични и частни субекти в комбинация с ЕРИКС. Освен това ЕРИКС обменят информация в контекста на мрежата на ЕРИКС в съответствие с Директива (ЕС) 2022/2555. Трансграничните ЦОС следва да представляват нов капацитет, който допълва мрежата на ЕРИКС, като обединяват и обменят данни за киберзаплахите от публични и частни субекти, повишават стойността на тези данни чрез експертен анализ и съвместно придобити инфраструктури и най-съвременни инструменти и допринасят за развитието на способностите и ***технологичния суверенитет*** на Съюза.

осигуряват от ЦОС от публични и частни субекти в комбинация с ЕРИКС. Освен това ЕРИКС обменят информация в контекста на мрежата на ЕРИКС в съответствие с Директива (ЕС) 2022/2555. Трансграничните ЦОС следва да представляват нов капацитет, който допълва мрежата на ЕРИКС, като обединяват и обменят данни за киберзаплахите от публични и частни субекти, повишават стойността на тези данни чрез експертен анализ и съвместно придобити инфраструктури и най-съвременни инструменти и допринасят за развитието на способностите и ***устойчивостта*** на Съюза.

Изменение 13

Предложение за регламент
Съображение 16

Текст, предложен от Комисията	*Изменение*
(16) Трансграничните ЦОС следва да действат като централно звено, позволяващо широко обединяване на относимите данни и разузнавателната информация за киберзаплахите, да дават възможност за разпространение на информация за заплахите сред голям и разнообразен набор от участници (напр. екипи за незабавно реагиране при компютърни инциденти („CERT“), ЕРИКС, центрове за обмен на информация и анализ („ISAC“), оператори на критични инфраструктури). Информацията, която се обменя между участниците в трансграничен ЦОС, може да включва данни от мрежи и сензори, разузнавателни сведения за заплахи, показатели за компрометиране на системите и контекстуална информация за инциденти, заплахи и уязвимости. Освен това трансграничните ЦОС	(16) Трансграничните ЦОС следва да действат като централно звено, позволяващо широко обединяване на относимите данни и разузнавателната информация за киберзаплахите, да дават възможност за разпространение на информация за заплахите сред голям и разнообразен набор от участници (напр. екипи за незабавно реагиране при компютърни инциденти („CERT“), ЕРИКС, центрове за обмен на информация и анализ („ISAC“), оператори на критични инфраструктури***, както и общността за киберотбрана***). Информацията, която се обменя между участниците в трансграничен ЦОС, може да включва данни от мрежи и сензори, разузнавателни сведения за заплахи, показатели за компрометиране на системите и контекстуална информация за инциденти, заплахи и уязвимости.

следва да сключват и споразумения за сътрудничество с други трансгранични ЦОС.	Освен това трансграничните ЦОС следва да сключват и споразумения за сътрудничество с други трансгранични ЦОС ***и с оперативната мрежа за milCERT (MICNET), след като бъде създадена***.

Изменение 14

Предложение за регламент
Съображение 17

Текст, предложен от Комисията	*Изменение*
(17) Споделената ситуационна осведоменост между съответните органи е необходима предпоставка за готовността и координацията в целия Съюз по отношение на значителни и мащабни киберинциденти. С Директива (ЕС) 2022/2555 се създава EU-CyCLONe с цел подпомагане на координираното управление на мащабни киберинциденти и кризи на оперативно равнище и осигуряване на редовния обмен на относимата информация сред държавите членки и институциите, органите, службите и агенциите на Съюза. В Препоръка (ЕС) 2017/1584 относно координирана реакция на мащабни киберинциденти и кризи се разглежда ролята на всички съответни участници. В Директива (ЕС) 2022/2555 се припомнят и отговорностите на Комисията в рамките на Механизма за гражданска защита на Съюза („МГЗС“), създаден с Решение 1313/2013/ЕС на Европейския парламент и на Съвета, както и тези за предоставянето на аналитични доклади за механизма за интегрирана реакция при политическа криза („ИРПК“) съгласно Решение за изпълнение (ЕС) 2018/1993. Следователно в ситуации, когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те	(17) Споделената ситуационна осведоменост между съответните органи е необходима предпоставка за готовността и координацията в целия Съюз по отношение на значителни и мащабни киберинциденти. С Директива (ЕС) 2022/2555 се създава EU-CyCLONe с цел подпомагане на координираното управление на мащабни киберинциденти и кризи на оперативно равнище и осигуряване на редовния обмен на относимата информация сред държавите членки и институциите, органите, службите и агенциите на Съюза. В Препоръка (ЕС) 2017/1584 относно координирана реакция на мащабни киберинциденти и кризи се разглежда ролята на всички съответни участници. В Директива (ЕС) 2022/2555 се припомнят и отговорностите на Комисията в рамките на Механизма за гражданска защита на Съюза („МГЗС“), създаден с Решение 1313/2013/ЕС на Европейския парламент и на Съвета, както и тези за предоставянето на аналитични доклади за механизма за интегрирана реакция при политическа криза („ИРПК“) съгласно Решение за изпълнение (ЕС) 2018/1993. Следователно в ситуации, когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те

следва да предоставят относимата информация на EU-CyCLONe, мрежата на ЕРИКС и Комисията. По-специално в зависимост от ситуацията, информацията, която трябва да бъде споделена, може да включва техническа информация, информация за естеството и мотивите на нападателя или потенциалния нападател, както и нетехническа информация от по-високо ниво за потенциален или текущ мащабен киберинцидент. В този контекст следва да се обърне надлежно внимание на принципа „необходимост да се знае“ и на потенциално чувствителния характер на споделяната информация.	следва да предоставят относимата информация на EU-CyCLONe, мрежата на ЕРИКС***, общността за киберотбрана*** и Комисията. По-специално в зависимост от ситуацията, информацията, която трябва да бъде споделена, може да включва техническа информация, информация за естеството и мотивите на нападателя или потенциалния нападател, както и нетехническа информация от по-високо ниво за потенциален или текущ мащабен киберинцидент. В този контекст следва да се обърне надлежно внимание на принципа „необходимост да се знае“ и на потенциално чувствителния характер на споделяната информация.

Изменение 15

Предложение за регламент
Съображение 19

Текст, предложен от Комисията	*Изменение*
(19) За да се даде възможност за широкомащабен обмен на данни за киберзаплахите от различни източници в доверителна среда, субектите, участващи в европейския киберщит, следва да разполагат с най-съвременни инструменти, оборудване и инфраструктури с високо ниво на сигурност. Това следва да даде възможност за подобряване на колективните способности за откриване и за своевременно предупреждение на органите и съответните субекти, по-специално чрез използване на най-новите технологии за изкуствен интелект и анализ на данни.	(19) За да се даде възможност за широкомащабен обмен на данни за киберзаплахите от различни източници в доверителна среда, субектите, участващи в европейския киберщит, следва да разполагат с най-съвременни инструменти, оборудване и инфраструктури с високо ниво на сигурност***, като се изключват високорисковите доставчици на продукти от критично значение с цифрови елементи***. Това следва да даде възможност за подобряване на колективните способности за откриване и за своевременно предупреждение на органите и съответните субекти, по-специално чрез използване на най-новите технологии за изкуствен интелект и анализ на данни. ***При използването на ИИ следва да се осигури човешки надзор, като следва да се гарантира достатъчно ниво на***

	грамотност в областта на ИИ, както и необходимата подкрепа и правомощия за упражняване на тази функция.

Изменение 16

Предложение за регламент
Съображение 19а (ново)

Текст, предложен от Комисията	*Изменение*
	(19а) В съответствие с Регламент [XX/XXXX (Законодателен акт за киберустойчивост)] субектите, участващи в европейския киберщит, следва да обхващат и изискванията, определени в настоящия регламент за всички продукти с цифрови елементи. С оглед на нарастващите рискове, произтичащи от икономическите зависимости, е необходимо да се сведе до минимум излагането на високорискови доставчици на продукти от критично значение чрез обща стратегическа рамка за икономическата сигурност на ЕС. Зависимостта от високорискови доставчици на продукти от критично значение с цифрови елементи представлява стратегически риск, който следва да бъде разглеждан на равнището на Съюза, по-специално дали дадена държава се ангажира с икономически шпионаж или икономическа принуда и нейното законодателство налага произволен достъп до всякакъв вид операции или данни на дружеството, особено когато продуктите от критично значение са предназначени за използване от съществените субекти, посочени в Директива (ЕС) 2022/2555.

Изменение 17

Предложение за регламент
Съображение 20

Текст, предложен от Комисията	*Изменение*
(20) Чрез събирането, споделянето и обмена на данни европейският киберщит следва да повиши технологичния суверенитет на Съюза. Обединяването на висококачествени подбрани данни следва да допринесе и за разработването на авангардни технологии за изкуствен интелект и анализ на данни. Това следва да бъде улеснено чрез свързването на европейския киберщит с общоевропейската инфраструктура за високопроизводителни изчислителни технологии, създадена с Регламент (ЕС) 2021/1173***25*** на Съвета.	(20) Чрез събирането, споделянето и обмена на данни европейският киберщит следва да повиши технологичния суверенитет***, стратегическата автономност, конкурентоспособността и издръжливостта*** на Съюза. Обединяването на висококачествени подбрани данни следва да допринесе и за разработването на авангардни технологии за изкуствен интелект и анализ на данни. Това следва да бъде улеснено чрез свързването на европейския киберщит с общоевропейската инфраструктура за високопроизводителни изчислителни технологии, създадена с Регламент (ЕС) 2021/1173 на Съвета***25***.
[25] Регламент (ЕС) 2021/1173 на Съвета от 13 юли 2021 г. за създаване на Съвместно предприятие за европейски високопроизводителни изчислителни технологии и за отмяна на Регламент (ЕС) 2018/1488, (ОВ L 256, 19.7.2021 г., стр. 3).	[25] Регламент (ЕС) 2021/1173 на Съвета от 13 юли 2021 г. за създаване на Съвместно предприятие за европейски високопроизводителни изчислителни технологии и за отмяна на Регламент (ЕС) 2018/1488, (ОВ L 256, 19.7.2021 г., стр. 3).

Изменение 18

Предложение за регламент
Съображение 25

Текст, предложен от Комисията	*Изменение*
(25) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя подкрепа на държавите членки в допълнение към техните собствени мерки и ресурси, както и към други	(25) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя подкрепа на държавите членки в допълнение към техните собствени мерки и ресурси, както и към други

съществуващи възможности за подкрепа в случай на реагиране и незабавно възстановяване след значителни и мащабни киберинциденти, като например услугите, предоставяни от Агенцията на Европейския съюз за киберсигурност („ENISA“) в съответствие с нейния мандат, координираното реагиране и помощта от мрежата на ЕРИКС, подкрепата за смекчаване на последиците от EU-CyCLONe, както и взаимната помощ между държавите членки, включително в контекста на член 42, параграф 7 от ДЕС, екипите за бързо реагиране в областта на киберсигурността на ПСС***[26]*** и хибридните екипи за бързо реагиране. Следва да се разгледа необходимостта да се гарантира наличието на специализирани средства за подпомагане на готовността и реагирането при киберинциденти в целия Съюз и в трети държави.

съществуващи възможности за подкрепа в случай на реагиране и незабавно възстановяване след значителни и мащабни киберинциденти, като например услугите, предоставяни от Агенцията на Европейския съюз за киберсигурност („ENISA“) в съответствие с нейния мандат, координираното реагиране и помощта от мрежата на ЕРИКС, подкрепата за смекчаване на последиците от EU-CyCLONe, както и взаимната помощ между държавите членки, включително в контекста на член 42, параграф 7 от ДЕС, екипите за бързо реагиране в областта на киберсигурността на ПСС***[1], новия „Координационен център в областта на киберсигурността и информацията (CIDCC)“ по линия на ПСС и неговия предложен „наследник“, а именно Координационния център на ЕС за киберотбрана (КЦК на ЕС), както*** и хибридните екипи за бързо реагиране. Следва да се разгледа необходимостта да се гарантира наличието на специализирани средства за подпомагане на готовността и реагирането при киберинциденти в целия Съюз и в трети държави***, особено в тези страни кандидатки за членство в ЕС, които са в съответствие с общата външна политика и политика за сигурност и общата политика за сигурност и отбрана на ЕС, като им се оказва подкрепа при изграждането на техните киберспособности и засилването на трансграничното и регионалното сътрудничество между тези страни кандидатки в областта на киберпространството.***

[1] Решение (ОВППС) 2017/2315 на Съвета от 11 декември 2017 година за установяване на постоянно структурирано сътрудничество (ПСС) и определяне на списъка на участващите държави членки.

[26] Решение (ОВППС) 2017/2315 на Съвета от 11 декември 2017 г. за установяване на постоянно структурирано сътрудничество (ПСС) и определяне на списъка на участващите държави членки.

[26] Решение (ОВППС) 2017/2315 на Съвета от 11 декември 2017 г. за установяване на постоянно структурирано сътрудничество (ПСС) и определяне на списъка на участващите държави членки.

Изменение 19

Предложение за регламент
Съображение 26

Текст, предложен от Комисията	*Изменение*
(26) Настоящият инструмент не засяга процедурите и рамките за координиране на реагирането при кризи на равнището на Съюза, по-специално МГЗС[28], ИРПК**,,** и Директива (ЕС) 2022/2555. Той може да подкрепи или да допълни действията, осъществявани в контекста на член 42, параграф 7 от ДЕС или в ситуации, определени в член 222 от ДФЕС. Използването на този инструмент следва също така да бъде координирано с прилагането на мерките от инструментариума за кибердипломация***, когато това е уместно***.	(26) Настоящият инструмент не засяга процедурите и рамките за координиране на реагирането при кризи на равнището на Съюза, по-специално МГЗС[28], ИРПК и Директива (ЕС) 2022/2555. Той може да подкрепи или да допълни действията, осъществявани в контекста на член 42, параграф 7 от ДЕС или в ситуации, определени в член 222 от ДФЕС. Използването на този инструмент следва също така да бъде координирано с прилагането на мерките от инструментариума за кибердипломация***, като се засилва сътрудничеството на стратегическо, оперативно и техническо равнище между киберотбраната и други киберобщности, по-специално с цел укрепване на способностите за борба със заплахите за киберсигурността от държави извън Съюза, включително ограничителни мерки, които могат да се използват за предотвратяване и реагиране на злонамерени действия в киберпространството***.

[27] Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм

[27] Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм

за гражданска защита на Съюза (ОВ L 347, 20.12.2013 г., стр. 924).

[28] Договорености за интегрирана реакция на ЕС при политическа криза (ИРПК) и в съответствие с Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи.

за гражданска защита на Съюза (ОВ L 347, 20.12.2013 г., стр. 924).

[28] Договорености за интегрирана реакция на ЕС при политическа криза (ИРПК) и в съответствие с Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи.

Изменение 20

Предложение за регламент
Съображение 28

Текст, предложен от Комисията	*Изменение*
(28) Директива (ЕС) 2022/2555 изисква от държавите членки да определят или създадат един или повече органи за управление на киберкризи и да гарантират, че те разполагат с достатъчно ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин. В нея също така се изисква държавите членки да определят способностите, активите и процедурите, които могат да бъдат използвани в случай на криза, както и да приемат национален план за реагиране при мащабни киберинциденти и кризи, в който се определят целите и условията и редът за управлението на мащабни киберинциденти и кризи. От държавите членки се изисква също така да създадат един или повече ЕРИКС, натоварени с отговорности за действия при инцидент в съответствие с добре определен процес и обхващащи най-малко секторите, подсекторите и видовете субекти, попадащи в обхвата на посочената директива, както и да гарантират, че те разполагат с достатъчно ресурси за ефективно изпълнение на възложените им задачи. Настоящият регламент не засяга ролята на Комисията за осигуряване на	(28) Директива (ЕС) 2022/2555 изисква от държавите членки да определят или създадат един или повече органи за управление на киберкризи и да гарантират, че те разполагат с достатъчно ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин. В нея също така се изисква държавите членки да определят способностите, активите и процедурите, които могат да бъдат използвани в случай на криза, както и да приемат национален план за реагиране при мащабни киберинциденти и кризи, в който се определят целите и условията и редът за управлението на мащабни киберинциденти и кризи. От държавите членки се изисква също така да създадат един или повече ЕРИКС, натоварени с отговорности за действия при инцидент в съответствие с добре определен процес и обхващащи най-малко секторите, подсекторите и видовете субекти, попадащи в обхвата на посочената директива, както и да гарантират, че те разполагат с достатъчно ресурси за ефективно изпълнение на възложените им задачи. Настоящият регламент не засяга ролята на Комисията за осигуряване на

спазването от страна на държавите членки на задълженията по Директива (ЕС) 2022/2555. Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя помощ за действия, насочени към укрепване на готовността, както и за действия в отговор на инциденти с цел смекчаване на въздействието на значителни и мащабни киберинциденти, подпомагане на незабавното възстановяване и/или възстановяване на функционирането на основните услуги.

спазването от страна на държавите членки на задълженията по Директива (ЕС) 2022/2555. Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да предоставя помощ за действия, насочени към укрепване на готовността, както и за действия в отговор на инциденти с цел смекчаване на въздействието на значителни и мащабни киберинциденти, подпомагане на незабавното възстановяване и/или възстановяване на функционирането на основните услуги***, като се използва по подходящ начин целият спектър от отбранителни възможности, с които разполагат гражданските и военните общности***.

Изменение 21

Предложение за регламент
Съображение 29

Текст, предложен от Комисията	*Изменение*
(29) Като част от действията за готовност, за да се насърчи последователен подход и да се укрепи сигурността в целия Съюз и неговия вътрешен пазар, следва да се предостави подкрепа за координирано изпитване и оценка на киберсигурността на субектите, извършващи дейност във висококритични сектори, определени съгласно Директива (ЕС) 2022/2555. За тази цел Комисията, с подкрепата на ENISA и в сътрудничество с групата за сътрудничество за МИС, създадена с Директива (ЕС) 2022/2555, следва редовно да определя съответните сектори или подсектори, които следва да отговарят на условията за получаване на финансова подкрепа за координирани изпитвания на равнището на Съюза. Секторите или подсекторите следва да бъдат избрани от приложение I към Директива (ЕС) 2022/2555 („Сектори с	(29) Като част от действията за готовност, за да се насърчи последователен подход и да се укрепи сигурността в целия Съюз и неговия вътрешен пазар, следва да се предостави подкрепа за координирано изпитване и оценка на киберсигурността на субектите, извършващи дейност във висококритични сектори, определени съгласно Директива (ЕС) 2022/2555. За тази цел Комисията, с подкрепата на ENISA и в сътрудничество с групата за сътрудничество за МИС, създадена с Директива (ЕС) 2022/2555, следва редовно да определя съответните сектори или подсектори, които следва да отговарят на условията за получаване на финансова подкрепа за координирани изпитвания на равнището на Съюза. ***Когато е целесъобразно, Европейската служба за външна дейност (ЕСВД), по-специално чрез***

висока степен на критичност“). Координираните изпитвания следва да се основават на общи сценарии на риска и методологии. При подбора на секторите и разработването на сценариите на риска следва да се вземат предвид съответните оценки на риска и сценарии на риска за целия Съюз, включително необходимостта от избягване на дублиране, като например оценката на риска и сценариите на риска, за които се призовава в заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството и които трябва да бъдат извършени от Комисията, върховния представител и групата за сътрудничество за МИС, в координация със съответните граждански и военни органи и агенции и установените мрежи, включително EU-CyCLONe, както и оценката на риска на комуникационните мрежи и инфраструктури, поискана от съвместния призив на министрите от Невер и извършена от групата за сътрудничество за МИС, с подкрепата на Комисията и ENISA и в сътрудничество с Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС), координираните оценки на риска, които ще бъдат извършени съгласно член 22 от Директива (ЕС) 2022/2555, и изпитването на оперативната устойчивост на цифровите технологии, както е предвидено в Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета***[29]***. При подбора на секторите следва да се вземе предвид и препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение.

Центъра на ЕС за анализ на информация (INTCEN) и неговото звено за синтез на информацията за хибридните заплахи, с подкрепата на дирекция „Разузнаване“ на Военния секретариат на Европейския съюз (ВСЕС) в рамките на единното звено за анализ на разузнавателна информация (SIAC), също следва да бъде асоциирана към предоставянето на актуални оценки и по този начин да допринася за идентифицирането на секторите или подсекторите***, които*** следва да бъдат избрани от приложение I към Директива (ЕС) 2022/2555 („Сектори с висока степен на критичност“). Координираните изпитвания следва да се основават на общи сценарии на риска и методологии. ***Тези изпитвания могат да играят важна роля и за подобряване на сътрудничеството между гражданските и военните структури. Ето защо при организирането на изпитвания Комисията, ЕСВД и ENISA следва системно да обмислят включването на участници от други кибернетични общности, като например Европейската агенция по отбрана (EDA) и други съответни структури.*** При подбора на секторите и разработването на сценариите на риска следва да се вземат предвид съответните оценки на риска и сценарии на риска за целия Съюз, включително необходимостта от избягване на дублиране, като например оценката на риска и сценариите на риска, за които се призовава в заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството и които трябва да бъдат извършени от Комисията, върховния представител и групата за сътрудничество за МИС, в координация със съответните граждански и военни органи и агенции и установените мрежи, включително EU-CyCLONe, както и оценката на риска на комуникационните

	мрежи и инфраструктури, поискана от съвместния призив на министрите от Невер и извършена от групата за сътрудничество за МИС, с подкрепата на Комисията и ENISA и в сътрудничество с Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС), координираните оценки на риска, които ще бъдат извършени съгласно член 22 от Директива (ЕС) 2022/2555, и изпитването на оперативната устойчивост на цифровите технологии, както е предвидено в Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета***[1]***. При подбора на секторите следва да се вземе предвид и препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на инфраструктурата от критично значение.
	[1] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 година относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011.
[29] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011.	[29] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011.

Изменение 22

Предложение за регламент
Съображение 32

Текст, предложен от Комисията	*Изменение*
(32) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да подкрепя помощта, предоставяна от държавите членки на дадена държава членка, засегната от значителен или мащабен киберинцидент, включително от мрежата на ЕРИКС, посочена в член 15 от Директива (ЕС) 2022/2555. На държавите членки, които предоставят помощ, следва да бъде разрешено да подават искания за покриване на разходите, свързани с изпращането на експертни екипи в рамките на взаимопомощта. Допустимите разходи може да включват пътни разходи, разходи за настаняване и дневни надбавки на експертите по киберсигурност.	(32) Механизмът за действие при извънредни ситуации в областта на киберсигурността следва да подкрепя помощта, предоставяна от държавите членки на дадена държава членка, засегната от значителен или мащабен киберинцидент, включително от мрежата на ЕРИКС, посочена в член 15 от Директива (ЕС) 2022/2555. На държавите членки, които предоставят помощ, следва да бъде разрешено да подават искания за покриване на разходите, свързани с изпращането на експертни екипи в рамките на взаимопомощта***, като се гарантира ефективна координация между съответните програми и инструменти на ЕС, включително Европейския механизъм за подкрепа на мира (ЕМПМ), ОВППС и ИССРМС, когато предоставят помощ на трети държави, по-специално на Украйна и Молдова***. Допустимите разходи може да включват пътни разходи, разходи за настаняване и дневни надбавки на експертите по киберсигурност.

Изменение 23

Предложение за регламент
Съображение 33

Текст, предложен от Комисията	*Изменение*
(33) Постепенно следва да бъде създаден резерв за киберсигурност на равнището на Съюза, състоящ се от услуги на частни доставчици на управлявани услуги за сигурност, който да подпомага действията за реагиране и незабавно възстановяване в случаи на значителни или мащабни киберинциденти. Резервът за киберсигурност на ЕС следва да гарантира наличността и готовността на	(33) Постепенно следва да бъде създаден резерв за киберсигурност на равнището на Съюза, състоящ се от услуги на частни доставчици на управлявани услуги за сигурност, който да подпомага действията за реагиране и незабавно възстановяване в случаи на значителни или мащабни киберинциденти. Резервът за киберсигурност на ЕС следва да гарантира наличността и готовността на

услугите. Услугите от резерва за киберсигурност на ЕС следва да подпомагат националните органи при предоставянето на помощ на засегнатите субекти, извършващи дейност в критични или висококритични сектори, като допълнение към собствените им действия на национално равнище. Когато искат подкрепа от резерва за киберсигурност на ЕС, държавите членки следва да посочат подкрепата, предоставена на засегнатия субект на национално равнище, която следва да бъде взета предвид при оценката на искането на държавата членка. Услугите от резерва за киберсигурност на ЕС могат да служат и за подкрепа на институциите, органите, службите и агенциите на ЕС при сходни условия.

услугите. Услугите от резерва за киберсигурност на ЕС следва да подпомагат националните органи при предоставянето на помощ на засегнатите субекти, извършващи дейност в критични или висококритични сектори, като допълнение към собствените им действия на национално равнище. Когато искат подкрепа от резерва за киберсигурност на ЕС, държавите членки следва да посочат подкрепата, предоставена на засегнатия субект на национално равнище, която следва да бъде взета предвид при оценката на искането на държавата членка. Услугите от резерва за киберсигурност на ЕС могат да служат и за подкрепа на институциите, органите, службите и агенциите на ЕС***, включително мисиите по линия на ОПСО,*** при сходни условия.

Изменение 24

Предложение за регламент
Съображение 34

Текст, предложен от Комисията	*Изменение*
(34) За целите на подбора на частни доставчици на услуги, които да предоставят услуги в контекста на резерва за киберсигурност на ЕС, е необходимо да се установи набор от минимални критерии, които следва да бъдат включени в поканата за участие в търг за подбор на тези доставчици, за да се гарантира, че са удовлетворени нуждите на органите и субектите на държавите членки, извършващи дейност в критични или висококритични сектори.	(34) За целите на подбора на частни доставчици на услуги, които да предоставят услуги в контекста на резерва за киберсигурност на ЕС, е необходимо да се установи набор от минимални критерии, които следва да бъдат включени в поканата за участие в търг за подбор на тези доставчици, за да се гарантира, че са удовлетворени нуждите на органите и субектите на държавите членки, извършващи дейност в критични или висококритични сектори***, като се вземат предвид и рисковете, свързани с участието на доставчици от стратегически конкурентни държави, които могат да породят рискове за икономическата сигурност, както и***

последиците за стратегическата сигурност на Съюза.

Изменение 25

Предложение за регламент
Съображение 36

Текст, предложен от Комисията	*Изменение*
(36) За да се подкрепят целите на настоящия регламент за насърчаване на споделената ситуационна осведоменост, повишаване на устойчивостта на Съюза и осигуряване на ефективно реагиране на значителни и мащабни киберинциденти, EU-CyCLONe, мрежата на ЕРИКС или Комисията следва да могат да поискат от ENISA да направи преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA следва да изготви доклад за преглед на инцидента в сътрудничество със съответните заинтересовани страни, включително представители на частния сектор, държавите членки, Комисията и други съответни институции, органи, служби и агенции на ЕС. Що се отнася до частния сектор, ENISA разработва канали за обмен на информация със специализирани доставчици, включително доставчици на управлявани решения за сигурност и потенциални оференти, за да допринесе за мисията на ENISA за постигане на високо общо ниво на киберсигурност в целия Съюз. Въз основа на сътрудничеството със заинтересованите страни, включително частния сектор, докладът за преглед на конкретни инциденти следва да има за цел да оцени причините, въздействията и мерките за смекчаване от даден	(36) За да се подкрепят целите на настоящия регламент за насърчаване на споделената ситуационна осведоменост, повишаване на устойчивостта на Съюза и осигуряване на ефективно реагиране на значителни и мащабни киберинциденти, EU-CyCLONe, мрежата на ЕРИКС или Комисията следва да могат да поискат от ENISA да направи преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. ***С оглед на разработването на сигурна система за свързаност, която се основава на европейската квантова комуникационна инфраструктура (EuroQCI) и на правителствените сателитни комуникации на Европейския съюз (GOVSATCOM), и по-специално въвеждането на глобалната навигационна спътникова система „Галилео“ за ползватели от сферата на отбраната, при всяко евентуално бъдещо развитие следва да се отчита възможността за избухване на „хипервойна“, при която скоростта и сложността на квантовите изчислителни технологии се съчетават с военни системи с голяма автономност***. След приключване на прегледа и оценката на даден инцидент ENISA следва да изготви доклад за преглед на инцидента в сътрудничество със съответните заинтересовани страни, включително представители на частния сектор,

инцидент след неговото възникване. Особено внимание следва да се обърне на приноса и изводите, споделени от доставчиците на управлявани услуги за сигурност, които отговарят на условията за най-висока професионална почтеност, безпристрастност и необходим технически опит, както се изисква в настоящия регламент. Докладът следва да бъде представен и използван в работата на EU-CyCLONe, мрежата на ЕРИКС и Комисията. Когато инцидентът се отнася до трета държава, Комисията споделя доклада също с върховния представител.

държавите членки, Комисията и други съответни институции, органи, служби и агенции на ЕС. Що се отнася до частния сектор, ENISA разработва канали за обмен на информация със специализирани доставчици, включително доставчици на управлявани решения за сигурност и потенциални оференти, за да допринесе за мисията на ENISA за постигане на високо общо ниво на киберсигурност в целия Съюз. Въз основа на сътрудничеството със заинтересованите страни, включително частния сектор, докладът за преглед на конкретни инциденти следва да има за цел да оцени причините, въздействията и мерките за смекчаване от даден инцидент след неговото възникване. Особено внимание следва да се обърне на приноса и изводите, споделени от доставчиците на управлявани услуги за сигурност, които отговарят на условията за най-висока професионална почтеност, безпристрастност и необходим технически опит, както се изисква в настоящия регламент. Докладът следва да бъде представен и използван в работата на EU-CyCLONe, мрежата на ЕРИКС и Комисията. Когато инцидентът се отнася до трета държава, Комисията споделя доклада също с върховния представител***, ЕСВД и всяка мисия по линия на ОПСО в държавата, засегната от инцидента, чрез техните щабове***.

Изменение 26

Предложение за регламент
Съображение 37

Текст, предложен от Комисията	*Изменение*
(37) Като се има предвид непредвидимият характер на атаките срещу киберсигурността и фактът, че те често не се ограничават в определен	(37) Като се има предвид непредвидимият характер на атаките срещу киберсигурността и фактът, че те често не се ограничават в определен

географски район и пораждат висок риск от разпространение, укрепването на устойчивостта на съседните държави и способностите им да реагират ефективно на значителни и мащабни киберинциденти допринася за защитата на Съюза като цяло. Поради това трети държави, асоциирани към програмата „Цифрова Европа“, ***могат*** да бъдат подпомагани от резерва за киберсигурност на ЕС, ***когато това е предвидено в съответното споразумение за асоцииране към програмата „Цифрова Европа“***. Финансирането на асоциираните трети държави следва да се подпомага от Съюза в рамките на съответните партньорства и инструменти за финансиране за тези държави. Подкрепата следва да обхваща услуги в областта на реагирането и незабавното възстановяване след значителни или мащабни киберинциденти. Условията, определени за резерва за киберсигурност на ЕС и доверителните доставчици в настоящия регламент, следва да се прилагат при предоставянето на подкрепа на трети държави, асоциирани към програмата „Цифрова Европа“.

географски район и пораждат висок риск от разпространение, укрепването на устойчивостта на съседните държави***, по-специално на Украйна и Молдова,*** и способностите им да реагират ефективно на значителни и мащабни киберинциденти допринася за защитата на Съюза като цяло. Поради това трети държави, асоциирани към програмата „Цифрова Европа“, ***следва*** да бъдат подпомагани от резерва за киберсигурност на ЕС***. Подкрепата следва да се прилага и за онези трети държави, в които е разположена мисия по линия на ОПСО със специален мандат за укрепване на устойчивостта на хибридни заплахи, включително киберзаплахи, или в които е приета мярка за помощ по линия на ЕМПМ с цел укрепване на киберустойчивостта на държавата***. Финансирането на асоциираните трети държави следва да се подпомага от Съюза в рамките на съответните партньорства и инструменти за финансиране за тези държави. Подкрепата следва да обхваща услуги в областта на реагирането и незабавното възстановяване след значителни или мащабни киберинциденти. Условията, определени за резерва за киберсигурност на ЕС и доверителните доставчици в настоящия регламент, следва да се прилагат при предоставянето на подкрепа на трети държави, асоциирани към програмата „Цифрова Европа“.

Изменение 27

Предложение за регламент
Член 1 – параграф 1 – буква в

Текст, предложен от Комисията	*Изменение*
в) създаване на европейски Механизъм за преглед на киберинциденти, който да разглежда и	в) създаване на европейски Механизъм за преглед на киберинциденти, който да разглежда и

оценява значителни или мащабни киберинциденти.	оценява значителни или мащабни киберинциденти ***или киберзаплахи***.

Изменение 28

Предложение за регламент
Член 1 – параграф 2 – буква а

Текст, предложен от Комисията	*Изменение*
а) засилване на общото за Съюза откриване на киберзаплахи и инциденти и ситуационна осведоменост, като по този начин се дава възможност за укрепване на конкурентната позиция на промишлеността и сектора на услугите в Съюза в цифровата икономика и се допринася за ***технологичния суверенитет*** на Съюза в областта на киберсигурността;	а) засилване на общото за Съюза откриване на киберзаплахи и инциденти и ситуационна осведоменост, като по този начин се дава възможност за укрепване на конкурентната позиция на промишлеността и сектора на услугите в Съюза в цифровата икономика и се допринася за ***технологичната издръжливост*** на Съюза в областта на киберсигурността;

Изменение 29

Предложение за регламент
Член 1 – параграф 2 - буква б

Текст, предложен от Комисията	*Изменение*
б) повишаване на готовността на субектите, извършващи дейност в критични и висококритични сектори в целия Съюз, и укрепване на солидарността чрез изграждане на общи способности за реагиране при значителни или мащабни киберинциденти, включително чрез предоставяне на подкрепа от Съюза за реагиране при киберинциденти на трети държави, асоциирани към програмата „Цифрова Европа“;	б) повишаване на готовността на субектите, извършващи дейност в критични и висококритични сектори в целия Съюз, и укрепване на солидарността чрез изграждане на общи способности за реагиране при значителни или мащабни киберинциденти, включително чрез предоставяне на подкрепа от Съюза за реагиране при киберинциденти на трети държави, асоциирани към програмата „Цифрова Европа“***, или на тези трети държави, които са кандидатки за присъединяване към Съюза и не противоречат на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в рамките на ОВППС съгласно дял V от ДЕС***;

	Държавите членки следва да обмислят интегрирането в своята национална стратегия за киберсигурност на активна програма за киберотбрана, която включва редовни съвместни учения между държавите членки и между международни организации. Такава програма следва да осигури синхронизиран в реално време капацитет за откриване, установяване, анализиране и смекчаване на заплахите;

Изменение 30

Предложение за регламент
Член 1 – параграф 2а (нов)

Текст, предложен от Комисията	*Изменение*
	2а. намаляване на системните рискове за киберсигурността, породени от зависимостите от критично оборудване от държави, които биха били в противоречие на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в рамките на ОВППС съгласно дял V от ДЕС;

Изменение 31

Предложение за регламент
Член 2 – параграф 2а (нов)

Текст, предложен от Комисията	*Изменение*
	„общност за киберотбрана“ означава органите за отбрана на държавите членки, подкрепяни от институциите, органите и агенциите на ЕС, както е посочено в съвместното съобщение относно политиката на ЕС за киберотбрана

[1];

[1] Съвместно съобщение до Европейския парламент и Съвета „Политика на ЕС за киберотбрана“, JOIN/2022/49 final.

Изменение 32

Предложение за регламент
Член 3 – параграф 2 – алинея 1 – буква ба (нова)

Текст, предложен от Комисията	*Изменение*
	ба) подпомага модернизирането на всички системи за киберотбрана, като повишава качеството на способностите за киберотбрана чрез внедряване на системи с ИИ и ускорява обмена на информация между националните ЦОС и трансграничните ЦОС;

Изменение 33

Предложение за регламент
Член 3 – параграф 2 – алинея 1 – буква га (нова)

Текст, предложен от Комисията	*Изменение*
	га) прави преглед и оценка на критичните технологии и оборудване за киберсигурност, използвани от ЦОС в отговор на киберинциденти, за системни рискове от контрол върху високорискови доставчици от страна на държави, които биха били в противоречие на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в рамките на ОВППС съгласно дял V от ДЕС.

Изменение 34

Предложение за регламент
Член 4 – параграф 1 – алинея 2

Текст, предложен от Комисията	*Изменение*
Той има способност да действа като отправна точка и портал за други публични и частни организации на национално равнище за събиране и анализиране на информация относно киберзаплахите и инцидентите и да допринася за работата на трансграничен ЦОС. Той е оборудван с най-съвременни технологии, способни да откриват, обобщават и анализират данни, свързани с киберзаплахите и инцидентите.	Той има способност да действа като отправна точка и портал за други публични и частни организации***, а когато е необходимо и военни организации,*** на национално равнище за събиране и анализиране на информация относно киберзаплахите и инцидентите и да допринася за работата на трансграничен ЦОС. Той е оборудван с най-съвременни технологии, способни да откриват, обобщават и анализират данни, свързани с киберзаплахите и инцидентите.

Изменение 35

Предложение за регламент
Член 4 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. След покана за заявяване на интерес националните ЦОС се избират от Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („ЕССС“), за да участват с ЕССС в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпуска безвъзмездни средства на избраните национални ЦОС за финансиране на функционирането на тези инструменти и инфраструктури. Финансовото участие на Съюза покрива до 50 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи, а останалите разходи се поемат от държавата членка. Преди да започнат процедурата за придобиване на	2. След покана за заявяване на интерес националните ЦОС се избират от Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността („ЕССС“), за да участват с ЕССС в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпуска безвъзмездни средства на избраните национални ЦОС за финансиране на функционирането на тези инструменти и инфраструктури***, при стриктното условие че тези инструменти и инфраструктура се предоставят от доверени доставчици в съответствие с член 16***. Финансовото участие на Съюза покрива до 50 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от

инструментите и инфраструктурите, ЕССС и националният ЦОС сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.	оперативните разходи, а останалите разходи се поемат от държавата членка. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и националният ЦОС сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.

Изменение 36

Предложение за регламент
Член 5 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. След покана за заявяване на интерес ЕССС избира консорциум, осигуряващ хостинг, който да участва в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпусне на консорциума, осигуряващ хостинг, безвъзмездни средства за финансиране на функционирането на инструментите и инфраструктурите. Финансовото участие на Съюза покрива до 75 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи, а останалите разходи се поемат от консорциума, осигуряващ хостинг. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и консорциумът, осигуряващ хостинг, сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.	2. След покана за заявяване на интерес ЕССС избира консорциум, осигуряващ хостинг, който да участва в съвместна обществена поръчка за инструменти и инфраструктури. ЕССС може да отпусне на консорциума, осигуряващ хостинг, безвъзмездни средства за финансиране на функционирането на инструментите и инфраструктурите***, при стриктното условие че тези инструменти и инфраструктура се предоставят от доверени доставчици в съответствие с член 16***. Финансовото участие на Съюза покрива до 75 % от разходите за придобиване на инструментите и инфраструктурите и до 50 % от оперативните разходи, а останалите разходи се поемат от консорциума, осигуряващ хостинг. Преди да започнат процедурата за придобиване на инструментите и инфраструктурите, ЕССС и консорциумът, осигуряващ хостинг, сключват споразумение за хостинг и използване, което урежда използването на инструментите и инфраструктурите.

Изменение 37

Предложение за регламент
Член 5 – параграф 2 а (нов)

Текст, предложен от Комисията	*Изменение*
	2а. Всяка инфраструктура или доставчик, произхождащ от високорискова трета държава, се изключва автоматично.

Изменение 38

Предложение за регламент
Член 6 – параграф 1 – буква б а (нова)

Текст, предложен от Комисията	*Изменение*
	ба) пряко подкрепя укрепването на военните и отбранителните способности на участващите членове или предотвратява пряка и непосредствена заплаха за тяхната сигурност. Тъй като използването на уязвимостите в сектора на отбраната може да причини значителни смущения и вреди, киберсигурността на този сектор изисква специални мерки, за да се гарантира сигурността на веригите на доставки, особено по отношение на субектите, които са по-ниско във веригите на доставки и не изискват достъп до класифицирана информация, но биха могли да доведат до сериозни рискове за целия сектор. Специално внимание следва да се обръща на въздействието, което би могло да има всяко нарушение, и заплахата от евентуално манипулиране на мрежови данни, което би могло да направи безполезни критичните отбранителни средства или дори да изключи техните операционни системи, с което ги прави уязвими на отвличания.

Изменение 39

Предложение за регламент
Член 6 – параграф 1 – буква б б (нова)

Текст, предложен от Комисията	*Изменение*
	бб) подпомага укрепването на отбранителните способности на участващите членове или предотвратява пряка и непосредствена заплаха за тяхната сигурност, като гарантира сигурността на веригите на доставки, особено по отношение на субектите, които са по-ниско във веригите на доставки и не изискват достъп до класифицирана информация, но биха могли да доведат до сериозни рискове за целия сектор.

Изменение 40

Предложение за регламент
Член 7 – параграф 1

Текст, предложен от Комисията	*Изменение*
1. Когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те незабавно предоставят съответната информация на EU-CyCLONe, мрежата на ЕРИКС и Комисията с оглед на съответните им функции по управление на кризи в съответствие с Директива (ЕС) 2022/2555.	1. Когато трансграничните ЦОС получат информация, свързана с потенциален или текущ мащабен киберинцидент, те незабавно предоставят съответната информация на EU-CyCLONe, мрежата на ЕРИКС и Комисията***, включително на върховния представител и ЕСВД, когато това засяга трета държава,*** с оглед на съответните им функции по управление на кризи в съответствие с Директива (ЕС) 2022/2555.

Изменение 41

Предложение за регламент
Член 8 – параграф 1

Текст, предложен от Комисията	*Изменение*
1. Държавите членки, участващи в европейския киберщит, осигуряват високо ниво на сигурност на данните и физическа сигурност на инфраструктурата на европейския киберщит и гарантират, че инфраструктурата се управлява и контролира по подходящ начин, така че да бъде защитена от заплахи и да се гарантира нейната сигурност и тази на системите, включително ***сигурността*** на данните, обменяни чрез инфраструктурата.	1. Държавите членки, участващи в европейския киберщит, осигуряват високо ниво на сигурност на данните и физическа сигурност на инфраструктурата на европейския киберщит и гарантират, че инфраструктурата се управлява и контролира по подходящ начин, така че да бъде защитена от заплахи и да се гарантира нейната сигурност и тази на системите***, като се намалява рискът и се поощряване технологичното предимство на ЕС в критични сектори***, включително ***чрез мерки за ограничаване или изключване на високорискови доставчици, както и за защита на сигурността*** на данните, обменяни чрез инфраструктурата.

Изменение 42

Предложение за регламент
Член 8 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Държавите членки, участващи в европейския киберщит, гарантират, че обменът на информация в рамките на европейския киберщит със субекти, които не са публични органи на държава членка, не засяга отрицателно интересите на Съюза в областта на сигурността.	2. Държавите членки, участващи в европейския киберщит, гарантират, че обменът на информация в рамките на европейския киберщит със субекти, които не са публични органи на държава членка, не засяга отрицателно интересите на Съюза в областта на сигурността***, както и че всеки обмен на информация с високорискови доставчици е с ограничен обхват и не засяга сигурността и стратегическите интереси на Съюза***.

Изменение 43

Предложение за регламент
Член 8 – параграф 3

Текст, предложен от Комисията	*Изменение*
3. Комисията може да приема актове за изпълнение за определяне на техническите изисквания, които държавите членки трябва да спазват, за да изпълнят задълженията си по параграфи 1 и 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2 от настоящия регламент. При това Комисията, подпомагана от върховния представител, взема предвид съответните стандарти за сигурност на ниво отбрана, за да улесни сътрудничеството с военните участници.	3. Комисията може да приема актове за изпълнение за определяне на техническите изисквания, които държавите членки трябва да спазват, за да изпълнят задълженията си по параграфи 1 и 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 21, параграф 2 от настоящия регламент. При това Комисията, подпомагана от върховния представител, взема предвид съответните стандарти за сигурност на ниво отбрана, за да улесни сътрудничеството с военните участници***, като използва по подходящ начин целия набор от възможности за защита, с които разполагат гражданските и военните общности, за по-широката сигурност и отбрана на ЕС и информира Европейския парламент***.

Изменение 44

Предложение за регламент
Член 9 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Действията за прилагане на Механизма за действие при извънредни ситуации в областта на киберсигурността се подкрепят с финансиране от програмата „Цифрова Европа“ и се изпълняват в съответствие с Регламент (ЕС) 2021/694, и по-специално със специфична цел 3 от него.	2. Действията за прилагане на Механизма за действие при извънредни ситуации в областта на киберсигурността се подкрепят с финансиране от програмата „Цифрова Европа“ и се изпълняват в съответствие с Регламент (ЕС) 2021/694, и по-специално със специфична цел 3 от него***, както и от Европейския механизъм за подкрепа на мира (ЕМПМ), когато се предоставят мерки за помощ на трети държави, по-специално на Украйна и Молдова;***

Изменение 45

Предложение за регламент
Член 10 – параграф 1 – буква а

Текст, предложен от Комисията	*Изменение*
а) действия за готовност, включително координирано изпитване на готовността на субектите, извършващи дейност във висококритични сектори в целия Съюз;	а) действия за готовност, включително координирано изпитване на готовността на субектите, извършващи дейност във висококритични сектори***, като например публична инфраструктура, изборна инфраструктура, транспорт, здравеопазване, финанси, телекомуникации, доставки на храни и продоволствена сигурност,*** в целия Съюз;

Изменение 46

Предложение за регламент
Член 10 – параграф 1 – буква в

Текст, предложен от Комисията	*Изменение*
в) действия за взаимопомощ, състоящи се в предоставяне на помощ от националните органи на една държава членка на друга държава членка, по-специално както е предвидено в член 11, параграф 3, буква е) от Директива (ЕС) 2022/2555**.**	в) действия за взаимопомощ, състоящи се в предоставяне на помощ от националните органи на една държава членка на друга държава членка, по-специално както е предвидено в член 11, параграф 3, буква е) от Директива (ЕС) 2022/2555 ***и в контекста на член 42, параграф 7 от ДЕС и член 222 от ДФЕС;***

Изменение 47

Предложение за регламент
Член 10 – параграф 1 – буква ва (нова)

Текст, предложен от Комисията	*Изменение*
	ва) подмяна и постепенно извеждане от експлоатация на критично оборудване от високорискови доставчици, които

	биха били в противоречие на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в рамките на ОВППС съгласно дял V от ДЕС.

Изменение 48

Предложение за регламент
Член 11 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Групата за сътрудничество за МИС, в сътрудничество с Комисията, ENISA ***и*** върховния представител, разработва общи сценарии за риска и методологии за координираните изпитвания.	2. Групата за сътрудничество за МИС, в сътрудничество с Комисията, ENISA, върховния представител, ***ЕСВД и, когато е целесъобразно, EDA***, разработва общи сценарии за риска и методологии за координираните изпитвания.

Изменение 49

Предложение за регламент
Член 12 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Резервът за киберсигурност на ЕС се състои от услуги за реагиране при инциденти, предоставяни от доверителни доставчици, избрани в съответствие с критериите, посочени в член 16. Резервът включва предварително заявени услуги. Услугите могат да бъдат предоставяни във всички държави членки.	2. Резервът за киберсигурност на ЕС се състои от услуги за реагиране при инциденти, предоставяни от доверителни доставчици, избрани в съответствие с критериите, посочени в член 16. Резервът включва предварително заявени услуги. Услугите могат да бъдат предоставяни във всички държави членки ***и трети държави, които отговарят на приложимите изисквания на настоящия регламент***.

Изменение 50

Предложение за регламент
Член 12 – параграф 3 - буква б

Текст, предложен от Комисията	*Изменение*
б) институции, органи, служби и агенции на Съюза.	б) институции, органи, служби и агенции на Съюза***, включително мисии по линия на ОПСО***.

Изменение 51

Предложение за регламент
Член 12 – параграф 4

Текст, предложен от Комисията	*Изменение*
4. Ползвателите, посочени в параграф 3, буква а), използват услугите от резерва за киберсигурност на ЕС с цел да реагират или да подпомогнат реагирането и незабавното възстановяване след значителни или мащабни инциденти, засягащи субекти, извършващи дейност в критични или висококритични сектори.	4. Ползвателите, посочени в параграф 3, буква а), използват услугите от резерва за киберсигурност на ЕС с цел да реагират или да подпомогнат реагирането и незабавното възстановяване след значителни или мащабни инциденти, засягащи субекти, извършващи дейност в критични или висококритични сектори***, като например публична инфраструктура, изборна инфраструктура, транспорт, здравеопазване, финанси, телекомуникации, доставки на храни и продоволствена сигурност***.

Изменение 52

Предложение за регламент
Член 12 – параграф 5

Текст, предложен от Комисията	*Изменение*
5. Комисията носи цялостна отговорност за изпълнението на резерва за киберсигурност на ЕС. Комисията определя приоритетите и развитието на резерва за киберсигурност на ЕС в съответствие с изискванията на ползвателите, посочени в параграф 3, и	5. Комисията носи цялостна отговорност за изпълнението на резерва за киберсигурност на ЕС. Комисията определя приоритетите и развитието на резерва за киберсигурност на ЕС в съответствие с изискванията на ползвателите, посочени в параграф 3, и

упражнява надзор върху неговото изпълнение, като осигурява взаимно допълване, съгласуваност, полезни взаимодействия и връзки с други действия за подкрепа съгласно настоящия регламент, както и с други действия ***и*** програми на Съюза.	упражнява надзор върху неговото изпълнение, като осигурява взаимно допълване, съгласуваност, полезни взаимодействия и връзки с други действия за подкрепа съгласно настоящия регламент, както и с други действия***,*** програми ***и цели*** на Съюза***, по-специално със стратегическата цел за намаляване на зависимостта от високорискови доставчици, които биха били в противоречие на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в рамките на ОВППС съгласно дял V от ДЕС***.

Изменение 53

Предложение за регламент
Член 12 – параграф 7

Текст, предложен от Комисията	*Изменение*
7. За да подпомогне Комисията при създаването на резерва за киберсигурност на ЕС, ENISA изготвя картографиране на необходимите услуги, след като се консултира с държавите членки и Комисията. След консултация с Комисията ENISA изготвя подобно картографиране за определяне на нуждите на трети държави, които отговарят на условията за получаване на подкрепа от резерва за киберсигурност на ЕС съгласно член 17. Когато е уместно, Комисията се консултира с върховния представител.	7. За да подпомогне Комисията при създаването на резерва за киберсигурност на ЕС, ENISA изготвя картографиране на необходимите услуги, след като се консултира с държавите членки и Комисията. След консултация с Комисията ENISA изготвя подобно картографиране за определяне на нуждите на трети държави, които отговарят на условията за получаване на подкрепа от резерва за киберсигурност на ЕС съгласно член 17***, като това се подпомага от ЕСВД***. Когато е уместно, Комисията се консултира с върховния представител.

Изменение 54

Предложение за регламент
Член 14 – параграф 2 – буква аа (нова)

Текст, предложен от Комисията	*Изменение*
	аа) въздействието на инцидента върху сигурността и отбраната на Съюза;

Изменение 55

Предложение за регламент
Член 15 – параграф 3

Текст, предложен от Комисията	*Изменение*
3. След консултация с върховния представител подкрепата в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността може да допълва помощта, предоставяна в контекста на общата външна политика и политика на сигурност и общата политика за сигурност и отбрана, включително чрез екипите за бързо реагиране в областта на киберсигурността. Тя може също така да допълва или да допринася за помощта, предоставяна от една държава членка на друга държава членка в контекста на член 42, параграф 7 от Договора за Европейския съюз.	3. След консултация с върховния представител подкрепата в рамките на Механизма за действие при извънредни ситуации в областта на киберсигурността може да допълва помощта, предоставяна в контекста на общата външна политика и политика на сигурност и общата политика за сигурност и отбрана, включително чрез екипите за бързо реагиране в областта на киберсигурността***, за да се оказва по-добра подкрепа на държавите – членки на ЕС, мисиите и операциите по линия на ОПСО и на тези трети държави, които са в съответствие с общата външна политика и политика на сигурност и общата политика за сигурност и отбрана, в усилията им за изграждане на капацитет за киберотбрана, по-специално Украйна и Молдова***. Тя може също така да допълва или да допринася за помощта, предоставяна от една държава членка на друга държава членка в контекста на член 42, параграф 7 от Договора за Европейския съюз.

Изменение 56

Предложение за регламент
Член 16 – параграф 2 – буква ба (нова)

Текст, предложен от Комисията	*Изменение*
	аа) доставчикът доказва, че неговите структури за вземане на решения и управление са свободни от неправомерно влияние от страна на правителствата на държави, които биха били в противоречие на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в Рамката на ОВППС съгласно дял V от ДЕС;

Изменение 57

Предложение за регламент
Член 16 – параграф 2 – буква е

Текст, предложен от Комисията	*Изменение*
е) доставчикът разполага с хардуерно и софтуерно техническо оборудване, необходимо за поддържане на търсената услуга;	е) доставчикът разполага с хардуерно и софтуерно техническо оборудване, необходимо за поддържане на търсената услуга***, и отговаря на изискванията, посочени в член X от Регламент XX/XXXX (Законодателен акт за киберустойчивост)***;

Изменение 58

Предложение за регламент
Член 16 – параграф 2 – буква йа (нова)

Текст, предложен от Комисията	*Изменение*
	йа) не се допускат доставчици с произход от високорискова трета държава.

Изменение 59

Предложение за регламент
Член 16 – параграф 2 – буква йб (нова)

Текст, предложен от Комисията	*Изменение*
	йб) доставчикът е в тясно сътрудничество със съответните МСП, когато е възможно;

Изменение 60

Предложение за регламент
Член 17 – параграф 1

Текст, предложен от Комисията	*Изменение*
1. Трети държави могат да поискат подкрепа от резерва за киберсигурност на ЕС, когато това е предвидено в споразуменията за асоцииране, сключени във връзка с участието им в програмата „Цифрова Европа“.	1. Трети държави могат да поискат подкрепа от резерва за киберсигурност на ЕС, когато***:***
	а) това е предвидено в споразуменията за асоцииране, сключени във връзка с участието им в програмата „Цифрова Европа“***;***
	б) в тези трети държави е разположена мисия по линия на ОПСО със специален мандат за укрепване на устойчивостта на хибридни заплахи, включително киберзаплахи, или е приета мярка за помощ по линия на ЕМПМ с цел укрепване на киберустойчивостта на държавата.

Изменение 61

Предложение за регламент
Член 17 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Подкрепата от резерва за киберсигурност на ЕС е в съответствие с настоящия регламент и е съобразена с всички специфични условия, предвидени в споразуменията за	2. Подкрепата от резерва за киберсигурност на ЕС е в съответствие с настоящия регламент и е съобразена с всички специфични условия, предвидени в споразуменията за асоцииране, посочени в параграф 1***, с***

асоцииране, посочени в параграф 1.	***изключение на онези трети държави, обхванати от разпоредбите, посочени в параграф 1, буква б)***.

Изменение 62

Предложение за регламент
Член 18 – параграф 1

Текст, предложен от Комисията	*Изменение*
1. По искане на Комисията, EU-CyCLONe или мрежата на ЕРИКС ENISA извършва преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA предоставя доклад за прегледа на инцидента на мрежата на ЕРИКС, EU-CyCLONe и Комисията, за да ги подкрепи при изпълнението на техните задачи, по-специално с оглед на посочените задачи в членове 15 и 16 от Директива (ЕС) 2022/2555. Когато е целесъобразно, Комисията предоставя доклада на върховния представител.	1. По искане на Комисията, EU-CyCLONe или мрежата на ЕРИКС ENISA извършва преглед и оценка на заплахите, уязвимостите и действията за смекчаване на последиците по отношение на конкретен значителен или мащабен киберинцидент. След приключване на прегледа и оценката на даден инцидент ENISA предоставя доклад за прегледа на инцидента на мрежата на ЕРИКС, EU-CyCLONe и Комисията, за да ги подкрепи при изпълнението на техните задачи, по-специално с оглед на посочените задачи в членове 15 и 16 от Директива (ЕС) 2022/2555. Когато е целесъобразно***, особено когато инцидентът е свързан с трета държава,*** Комисията предоставя доклада на върховния представител ***и на ЕСВД***.

Изменение 63

Предложение за регламент
Член 18 – параграф 3а (нов)

Текст, предложен от Комисията	*Изменение*
	3а. Докладът се предоставя на Европейския парламент в съответствие с правото на Съюза или националното право относно защитата на чувствителна класифицирана информация.

Изменение 64

Предложение за регламент
Член 19 – параграф 1 – точка 1 – буква а – подточка 1
Регламент (ЕС) 2021/694
Член 6, параграф 1

Текст, предложен от Комисията	*Изменение*
„аа) подкрепяне на разработването на киберщит на ЕС, включително разработването, разгръщането и функционирането на национални и трансгранични платформи за ЦОС, които допринасят за ситуационната осведоменост в Съюза и за повишаване на способностите на Съюза за разузнаване на киберзаплахи“;	„аа) подкрепяне на разработването на киберщит на ЕС, включително разработването, разгръщането и функционирането на национални и трансгранични платформи за ЦОС, които допринасят за ситуационната осведоменост в Съюза и за повишаване на способностите на Съюза за разузнаване на киберзаплахи, ***както и за намаляване на зависимостта на Съюза от високорискови доставчици на критично оборудване или компоненти за киберсигурност, които биха били в противоречие на интересите на Съюза и неговите държави членки в областта на сигурността и отбраната, установени в рамките на ОВППС съгласно дял V от ДЕС***“;

Изменение 65

Предложение за регламент
Член 20 – параграф 1

Текст, предложен от Комисията	*Изменение*
До [***четири*** години след датата на прилагането настоящия регламент] Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент.	До [***три*** години след датата на прилагането настоящия регламент ***и на всеки две години след това***] Комисията представя на Европейския парламент и на Съвета доклад относно оценката и прегледа на настоящия регламент.

ПРОЦЕДУРА НА ПОДПОМАГАЩАТА КОМИСИЯ

Заглавие	Определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти
Позовавания	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Водеща комисия Дата на обявяване в заседание	ITRE 1.6.2023
Дадено становище Дата на обявяване в заседание	AFET 1.6.2023
Докладчик по становище: Дата на назначаване	Dragoş Tudorache 16.6.2023
Разглеждане в комисия	18.9.2023
Дата на приемане	24.10.2023
Резултат от окончателното гласуване	+: 39 –: 4 0: 0
Членове, присъствали на окончателното гласуване	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
Заместници, присъствали на окончателното гласуване	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

ПОИМЕННО ОКОНЧАТЕЛНО ГЛАСУВАНЕ В ПОДПОМАГАЩАТА КОМИСИЯ

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

Легенда на използваните знаци:
+ : „за“
- : „против“
0 : „въздържал се“