Európai Parlament
2019-2024

Külügyi Bizottság

2023/0109(COD)

27.10.2023

VÉLEMÉNY

a Külügyi Bizottság részéről

az Ipari, Kutatási és Energiaügyi Bizottság részére

a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról
(COM(2023/0209) – C9-0136/2023 – 2023/0109(COD))

A vélemény előadója: Dragoş Tudorache

PA_Legam

Módosítás 1

Rendeletre irányuló javaslat
1 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az információs és kommunikációs technológiák alkalmazása és az azoktól való függés alapvetően fontos tényezővé vált a gazdasági tevékenységek valamennyi ágazatában, mivel az európai közigazgatási szervek, vállalatok és polgárok ágazatok közötti és határokon átnyúló összekapcsoltságának és egymástól való függésének mértéke minden eddiginél nagyobb méreteket ölt.	(1) Az információs és kommunikációs technológiák alkalmazása és az azoktól való függés alapvetően fontos tényezővé vált a gazdasági ***és katonai*** tevékenységek valamennyi ágazatában, mivel az európai közigazgatási szervek, vállalatok és polgárok***, valamint a katonai és védelmi szereplők*** ágazatok közötti és határokon átnyúló összekapcsoltságának és egymástól való függésének mértéke minden eddiginél nagyobb méreteket ölt.

Módosítás 2

Rendeletre irányuló javaslat
2 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A kiberbiztonsági események nagyságrendje, gyakorisága és hatása egyre számottevőbb, ideértve az ellátási láncok ellen elkövetett, kiberkémkedést, zsarolóvírusokkal való fenyegetést vagy zavarkeltést célzó támadásokat. E jelenségek komoly veszélyt jelentenek a hálózati és információs rendszerek működésére nézve. Tekintettel a fenyegetettségi helyzet gyorsan változó jellegére, a kritikus infrastruktúrákban jelentős fennakadásokat vagy károkat okozó esetleges nagyszabású kiberbiztonsági események veszélye az EU kiberbiztonsági keretének minden szintjén fokozott felkészültséget igényel. ***Ez*** a ***veszély túlmutat*** az Ukrajna elleni orosz katonai agresszión, és tekintettel a jelenlegi geopolitikai feszültségekben közreműködő, államközeli bűnözői és haktivista körök sokféleségére, valószínűleg nem ***fog*** alábbhagyni. Az ilyen események	(2) A kiberbiztonsági események nagyságrendje, gyakorisága és hatása egyre számottevőbb, ideértve az ellátási láncok ellen elkövetett, kiberkémkedést, zsarolóvírusokkal való fenyegetést vagy zavarkeltést célzó támadásokat. E jelenségek komoly veszélyt jelentenek a hálózati és információs rendszerek működésére nézve. Tekintettel a fenyegetettségi helyzet gyorsan változó jellegére, a kritikus infrastruktúrákban jelentős fennakadásokat vagy károkat okozó esetleges nagyszabású kiberbiztonsági események veszélye az EU kiberbiztonsági keretének minden szintjén fokozott felkészültséget igényel. ***E veszélyek komolysága még relevánsabbá vált a háború kontinensünkre történő visszatérése miatt. Ezek a veszélyek túlmutatnak*** az Ukrajna elleni orosz katonai agresszión, és tekintettel a jelenlegi geopolitikai feszültségekben közreműködő,

akadályozhatják a közszolgáltatások nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, aláásható a felhasználók bizalmát, jelentős károkat okozhatnak az Unió gazdaságában, és akár egészségügyi vagy az emberi életet veszélyeztető következményekkel is járhatnak. Ezenkívül a kiberbiztonsági események kiszámíthatatlanok, mivel gyakran igen rövid időn belül alakulnak ki és eszkalálódnak, nem korlátozódnak egy adott földrajzi területre, hiszen több országot érintően egyidejűleg is előfordulhatnak vagy gyorsan terjedhetnek.	államközeli bűnözői és haktivista körök sokféleségére, valószínűleg nem ***fognak*** alábbhagyni. Az ilyen események akadályozhatják a közszolgáltatások nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, aláásható a felhasználók bizalmát, jelentős károkat okozhatnak az Unió gazdaságában ***és biztonságában***, és akár egészségügyi vagy az emberi életet veszélyeztető következményekkel is járhatnak ***azáltal, hogy adott esetben tönkreteszik a helyi vagy nemzeti biztonsági berendezéseket***. Ezenkívül a kiberbiztonsági események kiszámíthatatlanok, mivel gyakran igen rövid időn belül alakulnak ki és eszkalálódnak, nem korlátozódnak egy adott földrajzi területre, hiszen több országot érintően egyidejűleg is előfordulhatnak vagy gyorsan terjedhetnek. ***A kiberbiztonság fontos európai értékeink védelme szempontjából, és biztosítja demokráciáink működését azáltal, hogy megvédi választási infrastruktúránkat és demokratikus eljárásainkat a külföldi beavatkozástól.***

Módosítás 3

Rendeletre irányuló javaslat
2 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(2a) A kiberbiztonság elengedhetetlen az Unió biztonságának megőrzéséhez, valamint annak megakadályozásához, hogy rosszindulatú – akár állami vagy nem állami – szereplők aláássák demokráciánkat, gazdaságunkat és biztonságunkat. Fontos megelőzni a széttagoltságot, mivel egy ilyen helyzet nem jelentene megfelelő megközelítést, különösen akkor, ha a jövőben egy időben több tagállamot vagy

	kritikus transznacionális infrastruktúrát célzó nagyszabású kibertámadások kihívásával nézünk szembe. Ezért egy olyan uniós szervre van szükség, amely koordinációs platformként működne valamennyi meglévő és jövőbeli kiberbiztonsági eszköz, alap és mechanizmus számára.

Módosítás 4

Rendeletre irányuló javaslat
3 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Szükséges a digitalizált gazdaság egészét tekintve megerősíteni az uniós ipari és szolgáltatási ágazat versenyhelyzetét, és a digitális egységes piac kiberbiztonsági szintjének megerősítése révén előmozdítani e szektorok digitális átalakulását. Az Európa jövőjéről szóló konferencia[16] három különböző javaslatában is szerepelt az ajánlás, miszerint növelni kell a polgárok, a vállalkozások és a kritikus infrastruktúrákat működtető szervezetek növekvő, adott esetben pusztító társadalmi és gazdasági hatásokkal járó kiberbiztonsági fenyegetésekkel szembeni rezilienciáját. Ezért olyan infrastruktúrákba és szolgáltatásokba történő beruházásokra van szükség, amelyek támogatják a kiberbiztonsági fenyegetések és események mielőbbi észlelését és az azokra való gyorsabb reagálást, továbbá a tagállamoknak segítségre van szükségük ahhoz, hogy jobban felkészüljenek és hatékonyabban reagáljanak a jelentős és nagyszabású kiberbiztonsági eseményekre. Az Uniónak e területeken is meg kell erősítenie képességeit**,** különösen a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos adatok gyűjtése és elemzése tekintetében.	(3) Szükséges a digitalizált gazdaság egészét tekintve megerősíteni az uniós ipari és szolgáltatási ágazat versenyhelyzetét, és a digitális egységes piac kiberbiztonsági szintjének megerősítése révén előmozdítani e szektorok digitális átalakulását. Az Európa jövőjéről szóló konferencia[16] három különböző javaslatában is szerepelt az ajánlás, miszerint növelni kell a polgárok, a vállalkozások és a kritikus infrastruktúrákat működtető szervezetek növekvő, adott esetben pusztító társadalmi és gazdasági hatásokkal járó kiberbiztonsági fenyegetésekkel szembeni rezilienciáját. Ezért olyan infrastruktúrákba és szolgáltatásokba történő beruházásokra van szükség, amelyek támogatják a kiberbiztonsági fenyegetések és események mielőbbi észlelését és az azokra való gyorsabb reagálást, továbbá a tagállamoknak segítségre van szükségük ahhoz, hogy jobban felkészüljenek és hatékonyabban reagáljanak a jelentős és nagyszabású kiberbiztonsági eseményekre. Az Uniónak e területeken is meg kell erősítenie képességeit **–** különösen a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos adatok gyűjtése és elemzése tekintetében **–*, valamint a kiberbiztonsági fenyegetésekre és eseményekre való proaktív fellépés és***

határozott reagálás képességét.

[16] https://futureu.europa.eu/hu/?locale=hu

[16] https://futureu.europa.eu/hu/?locale=hu

Módosítás 5

Rendeletre irányuló javaslat
4 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) Az Unió már számos intézkedést hozott a kritikus infrastruktúrák és a kritikus szervezetek kiberbiztonsági kockázatokkal szembeni sebezhetőségének csökkentése és fokozott rezilienciája érdekében, ezek közé tartozik különösen az (EU) 2022/2555 európai parlamenti és tanácsi irányelv[17], az (EU) 2017/1584 bizottsági ajánlás[18], a 2013/40/EU európai parlamenti és tanácsi irányelv[19] és az (EU) 2019/881 európai parlamenti és tanácsi rendelet[20]. Ezen túlmenően a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlás felkéri a tagállamokat, hogy hozzanak sürgős és hatékony intézkedéseket, továbbá hogy folytassanak lojális, hatékony, szolidáris és összehangolt együttműködést egymással, a Bizottsággal és más érintett hatóságokkal, valamint az érintett szervezetekkel a belső piacon az alapvető szolgáltatások nyújtásához használt kritikus infrastruktúrák fokozott rezilienciája érdekében.	(4) Az Unió már számos intézkedést hozott a kritikus infrastruktúrák és a kritikus szervezetek kiberbiztonsági kockázatokkal szembeni sebezhetőségének csökkentése és fokozott rezilienciája érdekében, ezek közé tartozik különösen az (EU) 2022/2555 európai parlamenti és tanácsi irányelv[17], az (EU) 2017/1584 bizottsági ajánlás[18], a 2013/40/EU európai parlamenti és tanácsi irányelv[19] és az (EU) 2019/881 európai parlamenti és tanácsi rendelet[20]. Ezen túlmenően a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlás felkéri a tagállamokat, hogy hozzanak sürgős és hatékony intézkedéseket, továbbá hogy folytassanak lojális, hatékony ***és proaktív***, szolidáris és összehangolt együttműködést egymással, a Bizottsággal és más érintett hatóságokkal, valamint az érintett szervezetekkel a belső piacon az alapvető szolgáltatások nyújtásához használt kritikus infrastruktúrák fokozott rezilienciája érdekében. ***Emellett az Unió 2022 márciusában jóváhagyta és elindította a biztonság és a védelem területére vonatkozó stratégiai iránytűt, amely többek között a kiberbiztonság megerősítésére, valamint a hasonlóan gondolkodású szövetségesekkel és demokratikus partnerekkel folytatott nemzetközi együttműködés fokozására összpontosít, különösen ebben az ügyben. Emellett a kiberbiztonság az EU-NATO együttműködésről szóló közelmúltbeli,***

2023. januári harmadik együttes nyilatkozat központi eleme is volt. Az EU-NATO munkacsoport végső értékelő jelentése kifejezetten az EU és a NATO közötti szinergiák teljes körű kihasználását ajánlotta[1], beleértve a bevált gyakorlatok cseréjét a polgári és katonai szereplők között a vonatkozó kibernetikai szakpolitikák és jogszabályok végrehajtása terén.

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

---

[17] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (HL L 333., 2022.12.27.).

[18] A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (HL L 239., 2017.9.19., 36. o.).

[19] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (HL L 218., 2013.8.14., 8. o.).

[20] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

---

[17] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről, a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról, valamint az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (HL L 333., 2022.12.27.).

[18] A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról (HL L 239., 2017.9.19., 36. o.).

[19] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (HL L 218., 2013.8.14., 8. o.).

[20] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (HL L 151., 2019.6.7., 15. o.).

Módosítás 6

Rendeletre irányuló javaslat
6 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) Az EU kibervédelmi politikájáról szóló, 2022. november 10-én elfogadott közös közlemény[22] bejelentette az uniós kiberszolidaritási kezdeményezést, amelynek céljai a következők: a biztonsági műveleti központok (a továbbiakban: SOC-k) alkotta uniós infrastruktúra kiépítésének előmozdítása révén a közös uniós észlelési, helyzetismereti és reagálási képességek megerősítése, a megbízható szolgáltatók szolgáltatásait igénybe vevő uniós szintű kiberbiztonsági tartalék fokozatos kiépítésének támogatása, valamint a kritikus szervezetek uniós kockázatértékeléseken alapuló tesztelése az esetleges sebezhetőségek tekintetében.	(6) Az EU kibervédelmi politikájáról szóló, 2022. november 10-én elfogadott közös közlemény[22] bejelentette az uniós kiberszolidaritási kezdeményezést, amelynek céljai a következők: a biztonsági műveleti központok (a továbbiakban: SOC-k) alkotta uniós infrastruktúra kiépítésének előmozdítása révén a közös uniós észlelési, helyzetismereti és reagálási képességek megerősítése, a megbízható szolgáltatók szolgáltatásait igénybe vevő uniós szintű kiberbiztonsági tartalék fokozatos kiépítésének támogatása, valamint a kritikus szervezetek uniós kockázatértékeléseken alapuló tesztelése az esetleges sebezhetőségek tekintetében. ***Emellett a kiberfenyegetések gyorsan változó környezete és a technológiai fejlődés gyors üteme is azt mutatja, hogy fokozott polgári–katonai koordinációra és együttműködésre van szükség, amint azt a Tanács az EU kibervédelmi politikájáról szóló következtetéseiben[1] is hangsúlyozta.*** ***[1] A Tanács következtetései az EU kibervédelmi politikájáról, amelyet a Tanács a 2022. május 22-i ülésén jóváhagyott (9618/23).***
[22] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022) 49 final.	[22] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022) 49 final.

Módosítás 7

Rendeletre irányuló javaslat
6 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(6a) Tekintettel arra, hogy a polgári és a katonai ügyek között nincsenek éles határvonalak, és hogy a kibereszközök és -technológiák kettős felhasználásra alkalmasak, a digitális területre vonatkozó megközelítésnek átfogónak és holisztikusnak kell lennie. Több tagállamot érintő nagyszabású kiberbiztonsági esemény és válság esetén megfelelő válságkezelést és -irányítást kell kialakítani. E struktúrák szervezett módon információkat cserélnek, egyeztetnek és együttműködnek az Unió külső biztonsági és katonai válságkezelési struktúráival, valamint a tagállamoknak a biztonságért és a védelemért felelős szerveivel (a kibervédelmi közösség). Ennek a közös biztonság- és védelempolitika keretében az Unió által a vele szomszédos és távolabbi területeken a béke és a stabilitás biztosítása érdekében végzett műveletekre és missziókra is érvényesnek kell lennie.

Módosítás 8

Rendeletre irányuló javaslat
7 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) Unió-szerte meg kell erősíteni a kiberbiztonsági fenyegetések és események észlelését és helyzetismeretét, valamint a tagállamok és az Unió jelentős és nagyszabású kiberbiztonsági eseményekre való felkészültségét és reagálását szolgáló képességeinek javítása révén meg kell erősíteni a szolidaritást is. Ezért a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében ki kell építeni a biztonsági műveleti központok páneurópai infrastruktúráját (a továbbiakban: Európai Kiberpajzs). Létre kell hozni a kiberbiztonsági vészhelyzeti mechanizmust, amely támogatja a	(7) Unió-szerte meg kell erősíteni a kiberbiztonsági fenyegetések és események észlelését és helyzetismeretét, valamint a tagállamok és az Unió jelentős és nagyszabású kiberbiztonsági eseményekre való felkészültségét és reagálását szolgáló képességeinek javítása révén meg kell erősíteni a szolidaritást is. Ezért a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében ki kell építeni a biztonsági műveleti központok páneurópai infrastruktúráját (a továbbiakban: Európai Kiberpajzs). Létre kell hozni a kiberbiztonsági vészhelyzeti mechanizmust, amely támogatja a

tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az azonnali helyreállításban. Létre kell hozni a kiberbiztonsági események felülvizsgálati mechanizmusát konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából. Ezek az intézkedések nem érintik az Európai Unió működéséről szóló szerződés (EUMSZ) 107. és 108. cikkét.	tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre***, köztük az egynél több tagállamban bekövetkező eseményekre*** való felkészülésben, reagálásban és az azonnali helyreállításban. ***Amikor megvalósítható és szükséges, a kiberbiztonsági szükséghelyzeti mechanizmus keretében meg kell szervezni az információmegosztást és együttműködést a tagállamok védelmi hatóságaival, amelyet az uniós intézmények, szervek és ügynökségek (az uniós kibervédelmi közösség) támogatnak;*** Létre kell hozni a kiberbiztonsági események felülvizsgálati mechanizmusát konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából***. Ezeknek az új struktúráknak az uniós KBVP-műveleteket és -missziókat is támogatniuk kell***. Ezek az intézkedések nem érintik az Európai Unió működéséről szóló szerződés (EUMSZ) 107. és 108. cikkét.

Módosítás 9

Rendeletre irányuló javaslat
11 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(11) A hatékony és eredményes pénzgazdálkodás érdekében egyedi szabályokat kell megállapítani a fel nem használt kötelezettségvállalási és kifizetési előirányzatok átvitelére vonatkozóan. Az uniós költségvetés évenkénti meghatározására vonatkozó elv tiszteletben tartása mellett e rendeletnek a kiberbiztonsági környezet kiszámíthatatlan, rendkívüli és egyedi jellege miatt rendelkeznie kell arról, hogy a fel nem használt források a költségvetési rendeletben meghatározottakon felül is átvihetők legyenek, ezáltal maximalizálva a kiberbiztonsági vészhelyzeti mechanizmus azon képességét, hogy támogassa a tagállamokat a	(11) A hatékony és eredményes pénzgazdálkodás érdekében egyedi szabályokat kell megállapítani a fel nem használt kötelezettségvállalási és kifizetési előirányzatok átvitelére vonatkozóan. Az uniós költségvetés évenkénti meghatározására vonatkozó elv tiszteletben tartása mellett e rendeletnek a kiberbiztonsági környezet kiszámíthatatlan, rendkívüli és egyedi jellege miatt rendelkeznie kell arról, hogy a fel nem használt források a költségvetési rendeletben meghatározottakon felül is átvihetők legyenek, ezáltal maximalizálva a kiberbiztonsági vészhelyzeti mechanizmus azon képességét, hogy támogassa a tagállamokat a

kiberfenyegetések elleni hatékony küzdelemben.	kiberfenyegetések elleni hatékony küzdelemben. ***Ezek a konkrét szabályok hosszabb távú pénzügyi támogatást is lehetővé tennének az új generációs ultrabiztonságos eszközök és infrastruktúra közös beszerzéséhez annak érdekében, hogy a legújabb mesterséges intelligencia (MI) és adatelemzések felhasználásával javítsák a kollektív felderítési képességeket.***

Módosítás 10

Rendeletre irányuló javaslat
13 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(13) Minden tagállamnak ki kell jelölnie egy nemzeti szintű közjogi szervet, amelynek feladata a kiberfenyegetés-észlelési tevékenységek összehangolása az adott tagállamban. Ezeknek a nemzeti biztonsági műveleti központoknak nemzeti szinten referenciapontként és átjáróként kell szolgálniuk az Európai Kiberpajzsban való részvételhez, és biztosítaniuk kell, hogy az állami és magánszervezetektől származó, kiberfenyegetésekkel kapcsolatos információkat nemzeti szinten hatékonyan és egységesen osszák meg és gyűjtsék össze.	(13) Minden tagállamnak ki kell jelölnie egy nemzeti szintű közjogi szervet, amelynek feladata a kiberfenyegetés-észlelési tevékenységek összehangolása az adott tagállamban. Ezeknek a nemzeti biztonsági műveleti központoknak nemzeti szinten referenciapontként és átjáróként kell szolgálniuk az Európai Kiberpajzsban való részvételhez, és biztosítaniuk kell, hogy az állami és magánszervezetektől származó, kiberfenyegetésekkel kapcsolatos információkat nemzeti szinten hatékonyan és egységesen osszák meg és gyűjtsék össze. ***Amikor megvalósítható és szükséges, a biztonsági műveleti központoknak lehetővé kell tenniük a védelmi szervezetek részvételét is, létrehozva egy „védelmi pillért” az irányítás és a megosztott információk típusa tekintetében, az EU kibervédelmi politikájáról szóló közös közleményben[1] meghatározottak szerint és a főképviselő támogatásával.*** ***[1] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022) 49 final.***

Módosítás 11

Rendeletre irányuló javaslat
14 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(14) Az Európai Kiberpajzs részeként több határokon átnyúló biztonsági műveleti központot (a továbbiakban: határokon átnyúló SOC) kell létrehozni. A határokon átnyúló fenyegetések észlelése, valamint az információmegosztás és -kezelés előnyeinek teljes körű kiaknázása érdekében e központoknak legalább három tagállam nemzeti biztonsági műveleti központjából kell állniuk. A határokon átnyúló biztonsági műveleti központok általános célkitűzése a kiberbiztonsági fenyegetések elemzésére, megelőzésére és észlelésére szolgáló kapacitások megerősítése, valamint a magas színvonalú kiberfenyegetettségi információk előállításának támogatása kell, hogy legyen, elsősorban a különböző – köz- vagy magánforrásokból származó – adatok megosztása, a legkorszerűbb eszközök megosztása és közös használata, valamint az észlelési, elemzési és megelőzési képességek megbízható környezetben történő közös fejlesztése révén. A meglévő biztonsági műveleti központokra, számítógép-biztonsági eseményekre reagáló csoportokra (a továbbiakban: CSIRT) és más érintett szereplőkre támaszkodva és azokat kiegészítve új további kapacitást kell biztosítaniuk.	(14) Az Európai Kiberpajzs részeként több határokon átnyúló biztonsági műveleti központot (a továbbiakban: határokon átnyúló SOC) kell létrehozni. A határokon átnyúló fenyegetések észlelése, valamint az információmegosztás és -kezelés előnyeinek teljes körű kiaknázása érdekében e központoknak legalább három tagállam nemzeti biztonsági műveleti központjából ***– ideértve egy „védelmi pillért” is –*** kell állniuk. A határokon átnyúló biztonsági műveleti központok általános célkitűzése a kiberbiztonsági fenyegetések elemzésére, megelőzésére és észlelésére szolgáló kapacitások megerősítése, valamint a magas színvonalú kiberfenyegetettségi információk előállításának támogatása kell, hogy legyen, elsősorban a különböző – köz- vagy magánforrásokból***, és amikor megvalósítható és szükséges, az információmegosztásra vonatkozó megfelelő iránymutatás mellett katonai forrásokból*** származó – adatok megosztása, a legkorszerűbb eszközök megosztása és közös használata, valamint az észlelési, elemzési és megelőzési képességek megbízható környezetben történő közös fejlesztése révén. A meglévő biztonsági műveleti központokra, számítógép-biztonsági eseményekre reagáló csoportokra (a továbbiakban: CSIRT) és más érintett szereplőkre támaszkodva és azokat kiegészítve új további kapacitást kell biztosítaniuk.

Módosítás 12

Rendeletre irányuló javaslat
15 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(15) Nemzeti szinten a kiberfenyegetések nyomon követését, észlelését és elemzését jellemzően az állami és magánszervezetek biztonsági műveleti központjai biztosítják a CSIRT-ekkel együttműködve. Emellett a CSIRT-ek az (EU) 2022/2555 irányelvvel összhangban a CSIRT-ek hálózata keretében folytatnak információcserét. A határokon átnyúló biztonsági műveleti központoknak olyan új képességet kell kialakítaniuk, amely oly módon egészíti ki a CSIRT-ek hálózatát, hogy összegyűjti és megosztja az állami és magánszervezetektől származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatokat, majd szakértői elemzések, közösen beszerzett infrastruktúrák és a legkorszerűbb eszközök révén növeli az ilyen adatok értékét, valamint hozzájárul az uniós képességek és az EU ***technológiai szuverenitásának*** elmélyítéséhez.	(15) Nemzeti szinten a kiberfenyegetések nyomon követését, észlelését és elemzését jellemzően az állami és magánszervezetek biztonsági műveleti központjai biztosítják a CSIRT-ekkel együttműködve. Emellett a CSIRT-ek az (EU) 2022/2555 irányelvvel összhangban a CSIRT-ek hálózata keretében folytatnak információcserét. A határokon átnyúló biztonsági műveleti központoknak olyan új képességet kell kialakítaniuk, amely oly módon egészíti ki a CSIRT-ek hálózatát, hogy összegyűjti és megosztja az állami és magánszervezetektől származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatokat, majd szakértői elemzések, közösen beszerzett infrastruktúrák és a legkorszerűbb eszközök révén növeli az ilyen adatok értékét, valamint hozzájárul az uniós képességek és az EU ***rezilienciájának*** elmélyítéséhez.

Módosítás 13

Rendeletre irányuló javaslat
16 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(16) A határokon átnyúló biztonsági műveleti központoknak olyan központi pontként kell működniük, amely lehetővé teszi a releváns adatok és kiberfenyegetettségi információk kiterjedt gyűjtését, és a szóban forgó információk különféle szereplők ***közötti*** (pl. hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT), CSIRT-ek, információmegosztó és -elemző központok (ISAC), kritikus infrastruktúrák üzemeltetői) széles körű terjesztését. A határokon átnyúló biztonsági műveleti központok résztvevői közötti	(16) A határokon átnyúló biztonsági műveleti központoknak olyan központi pontként kell működniük, amely lehetővé teszi a releváns adatok és kiberfenyegetettségi információk kiterjedt gyűjtését, és a szóban forgó információk különféle szereplők (pl. hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT), CSIRT-ek, információmegosztó és -elemző központok (ISAC), kritikus infrastruktúrák üzemeltetői***, valamint a kibervédelmi közösség***) ***közötti*** széles körű terjesztését. A határokon átnyúló biztonsági műveleti központok résztvevői

információcsere kiterjedhet a hálózatokból és érzékelőkből származó adatokra, a kiberfenyegetettségi információk hírcsatornáira, a fertőzöttségi mutatókra, valamint a kiberbiztonsági eseményekre, fenyegetésekre és sebezhetőségekre vonatkozó, kontextusba helyezett információkra. Emellett a határokon átnyúló biztonsági műveleti központoknak együttműködési megállapodásokat kell kötniük más határokon átnyúló biztonsági műveleti központokkal is.

közötti információcsere kiterjedhet a hálózatokból és érzékelőkből származó adatokra, a kiberfenyegetettségi információk hírcsatornáira, a fertőzöttségi mutatókra, valamint a kiberbiztonsági eseményekre, fenyegetésekre és sebezhetőségekre vonatkozó, kontextusba helyezett információkra. Emellett a határokon átnyúló biztonsági műveleti központoknak együttműködési megállapodásokat kell kötniük más határokon átnyúló biztonsági műveleti központokkal ***és a milCERT-ek operatív hálózatával (MICNET)*** is***, amikor létrehozzák azokat***.

Módosítás 14

Rendeletre irányuló javaslat
17 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(17) Az érintett hatóságok közösen kialakított helyzetismerete elengedhetetlen előfeltétele a jelentős és nagyszabású kiberbiztonsági eseményekkel kapcsolatos uniós szintű felkészültségnek és koordinációnak. A nagyszabású kiberbiztonsági események és válsághelyzetek operatív szintű összehangolt kezelésének támogatása, valamint a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása érdekében az (EU) 2022/2555 irányelv létrehozta az EU-CyCLONe-t. A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1584 ajánlás valamennyi érintett szereplő feladataival foglalkozik. Az (EU) 2022/2555 irányelv emlékeztet továbbá a Bizottságnak az 1313/2013/EU európai parlamenti és tanácsi határozattal létrehozott uniós polgári védelmi mechanizmussal (a továbbiakban: UCPM) kapcsolatos	(17) Az érintett hatóságok közösen kialakított helyzetismerete elengedhetetlen előfeltétele a jelentős és nagyszabású kiberbiztonsági eseményekkel kapcsolatos uniós szintű felkészültségnek és koordinációnak. A nagyszabású kiberbiztonsági események és válsághelyzetek operatív szintű összehangolt kezelésének támogatása, valamint a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása érdekében az (EU) 2022/2555 irányelv létrehozta az EU-CyCLONe-t. A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1584 ajánlás valamennyi érintett szereplő feladataival foglalkozik. Az (EU) 2022/2555 irányelv emlékeztet továbbá a Bizottságnak az 1313/2013/EU európai parlamenti és tanácsi határozattal létrehozott uniós polgári védelmi mechanizmussal (a továbbiakban: UCPM) kapcsolatos

feladataira, valamint arra, hogy a Bizottság feladata az is, hogy elemző jelentéseket készítsen az (EU) 2018/1993 végrehajtási határozat szerinti uniós politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR-mechanizmus) számára. Ezért azokban az esetekben, amikor a határokon átnyúló biztonsági műveleti központok potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről szereznek információkat, releváns információkat kell szolgáltatniuk az EU-CyCLONe, a CSIRT-ek hálózata és a Bizottság számára. A helyzettől függően a megosztandó információk közé tartozhatnak különösen a technikai információk, a támadó vagy potenciális támadó jellegére és szándékaira vonatkozó információk, valamint a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos magasabb szintű, nem technikai jellegű információk. Ebben az összefüggésben kellő figyelmet kell fordítani a szükséges ismeret elvére és a megosztott információk potenciálisan érzékeny jellegére.

feladataira, valamint arra, hogy a Bizottság feladata az is, hogy elemző jelentéseket készítsen az (EU) 2018/1993 végrehajtási határozat szerinti uniós politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR-mechanizmus) számára. Ezért azokban az esetekben, amikor a határokon átnyúló biztonsági műveleti központok potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről szereznek információkat, releváns információkat kell szolgáltatniuk az EU-CyCLONe, a CSIRT-ek hálózata***, a kibervédelmi közösség*** és a Bizottság számára. A helyzettől függően a megosztandó információk közé tartozhatnak különösen a technikai információk, a támadó vagy potenciális támadó jellegére és szándékaira vonatkozó információk, valamint a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos magasabb szintű, nem technikai jellegű információk. Ebben az összefüggésben kellő figyelmet kell fordítani a szükséges ismeret elvére és a megosztott információk potenciálisan érzékeny jellegére.

Módosítás 15

Rendeletre irányuló javaslat
19 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(19) Annak érdekében, hogy a különböző forrásokból származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatcserére széles körben és megbízható környezetben kerülhessen sor, az Európai Kiberpajzsban részt vevő szervezeteket korszerű és rendkívül biztonságos eszközökkel, berendezésekkel és infrastruktúrákkal kell felszerelni. Ez várhatóan lehetővé teszi a közös észlelési képességek javítását és a hatóságok és az érintett szervezetek időben történő figyelmeztetését, különösen a	(19) Annak érdekében, hogy a különböző forrásokból származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatcserére széles körben és megbízható környezetben kerülhessen sor, ***a digitális elemeket tartalmazó kritikus fontosságú termékek magas kockázatot jelentő beszállítóinak kivételével,*** az Európai Kiberpajzsban részt vevő szervezeteket korszerű és rendkívül biztonságos eszközökkel, berendezésekkel és infrastruktúrákkal kell felszerelni. Ez várhatóan lehetővé teszi a közös észlelési

legkorszerűbb mesterségesintelligencia- és adatelemzési technológiák alkalmazásával.	képességek javítását és a hatóságok és az érintett szervezetek időben történő figyelmeztetését, különösen a legkorszerűbb mesterségesintelligencia- és adatelemzési technológiák alkalmazásával. ***A mesterséges intelligencia használata során biztosítani kell az emberi felügyeletet, és biztosítani kell a mesterséges intelligenciával kapcsolatos jártasság megfelelő szintjét, a szükséges támogatást és az e funkció ellátásához szükséges hatáskört.***

Módosítás 16

Rendeletre irányuló javaslat
19 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(19a) A(z) [XX/XXXX rendelettel (a kiberrezilienciáról szóló jogszabály)] összhangban az Európai Kiberpajzsban részt vevő szervezeteknek a digitális elemet tartalmazó összes termék tekintetében ki kell terjedniük az e rendeletben meghatározott követelményekre is. Tekintettel a gazdasági függőségekből eredő növekvő kockázatokra, az EU gazdasági biztonságára vonatkozó közös stratégiai keret révén minimálisra kell csökkenteni a kritikus fontosságú termékek magas kockázatot jelentő beszállítóinak való kitettséget. A digitális elemeket tartalmazó kritikus fontosságú termékek magas kockázatot jelentő beszállítóitól való függőség stratégiai kockázatot jelent, amelyet uniós szinten kell kezelni, különösen akkor, ha egy ország gazdasági kémkedést folytat vagy gazdasági kényszerítést alkalmaz, és jogszabályai önkényes hozzáférést írnak elő bármilyen vállalati művelethez vagy adathoz, különösen akkor, ha a kritikus termékeket az (EU) 2022/2555 irányelvben említett alapvető fontosságú szervezetek általi felhasználásra szánják.

Módosítás 17

Rendeletre irányuló javaslat
20 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(20) Az Európai Kiberpajzs az adatgyűjtésnek, -megosztásnak és -cserének köszönhetően várhatóan meg fogja erősíteni az Unió ***technológiai szuverenitását***. A kiváló minőségű gondozott adatok összevonása minden bizonnyal hozzájárul a fejlett mesterségesintelligencia- és adatelemzési technológiák fejlesztéséhez is. Ezt az Európai Kiberpajzsnak az (EU) 2021/1173 tanácsi rendelettel[25] létrehozott páneurópai nagy teljesítményű számítástechnikai infrastruktúrával való összekapcsolása révén kell elősegíteni.	(20) Az Európai Kiberpajzs az adatgyűjtésnek, -megosztásnak és -cserének köszönhetően várhatóan meg fogja erősíteni az Unió ***stratégiai autonómiáját, versenyképességét és rezilienciáját***. A kiváló minőségű gondozott adatok összevonása minden bizonnyal hozzájárul a fejlett mesterségesintelligencia- és adatelemzési technológiák fejlesztéséhez is. Ezt az Európai Kiberpajzsnak az (EU) 2021/1173 tanácsi rendelettel[25] létrehozott páneurópai nagy teljesítményű számítástechnikai infrastruktúrával való összekapcsolása révén kell elősegíteni.
[25] A Tanács (EU) 2021/1173 rendelete (2021. július 13.) az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás létrehozásáról és az (EU) 2018/1488 rendelet hatályon kívül helyezéséről (HL L 256., 2021.7.19., 3. o.).	[25] A Tanács (EU) 2021/1173 rendelete (2021. július 13.) az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás létrehozásáról és az (EU) 2018/1488 rendelet hatályon kívül helyezéséről (HL L 256., 2021.7.19., 3. o.).

Módosítás 18

Rendeletre irányuló javaslat
25 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(25) Jelentős és nagyszabású kiberbiztonsági eseményekre való reagálás alkalmával és az eseményt követő azonnali helyreállítás során a kiberbiztonsági vészhelyzeti mechanizmusnak a tagállami intézkedéseket és erőforrásokat, valamint a rendelkezésre álló egyéb támogatási	(25) Jelentős és nagyszabású kiberbiztonsági eseményekre való reagálás alkalmával és az eseményt követő azonnali helyreállítás során a kiberbiztonsági vészhelyzeti mechanizmusnak a tagállami intézkedéseket és erőforrásokat, valamint a rendelkezésre álló egyéb támogatási

lehetőségeket – például az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által a megbízatásával összhangban nyújtott szolgáltatásokat, a CSIRT-ek hálózata nyújtotta összehangolt reagálást és segítséget, az EU-CyCLONe mérséklési támogatását, valamint a tagállamok közötti, többek között az EUSZ 42. cikkének (7) bekezdésével összefüggésben az állandó strukturált együttműködés (PESCO) kiberbiztonsági eseményekkel foglalkozó gyorsreagálású ***csoportjai***[26] és a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatai keretében nyújtott kölcsönös segítségnyújtást – kiegészítve kell támogatnia a tagállamokat. A mechanizmusnak az igényekre reagálva biztosítania kell, hogy Unió-szerte és harmadik országokban speciális eszközök álljanak rendelkezésre, amelyek támogatják a kiberbiztonsági eseményekre való felkészültséget és reagálást.

[26] A Tanács (KKBP) 2017/2315 határozata (2017. december 11.) az állandó strukturált együttműködés (PESCO) létrehozásáról és

lehetőségeket – például az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által a megbízatásával összhangban nyújtott szolgáltatásokat, a CSIRT-ek hálózata nyújtotta összehangolt reagálást és segítséget, az EU-CyCLONe mérséklési támogatását, valamint a tagállamok közötti, többek között az EUSZ 42. cikkének (7) bekezdésével összefüggésben az állandó strukturált együttműködés (PESCO) kiberbiztonsági eseményekkel foglalkozó gyorsreagálású ***csoportjai[1], az új PESCO-projekt, a Kiber- és az Információs Terület Koordinációs Központja (CIDCC) és annak javasolt utódszervezete, az EU kibervédelmi koordinációs központja (EUCDCC),*** és a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatai keretében nyújtott kölcsönös segítségnyújtást – kiegészítve kell támogatnia a tagállamokat. A mechanizmusnak az igényekre reagálva biztosítania kell, hogy Unió-szerte és harmadik országokban ***– különösen azon uniós tagjelölt országok esetében, amelyek joganyagukat már harmonizálták az EU közös kül- és biztonságpolitikájával és közös biztonság- és védelempolitikájával –*** speciális eszközök álljanak rendelkezésre, amelyek támogatják a kiberbiztonsági eseményekre való felkészültséget és reagálást***, támogatva őket kiberképességeik kiépítésében, valamint a tagjelölt országok közötti határokon átnyúló és regionális együttműködés fokozásában a kibertérben***.

[1] A Tanács (KKBP) 2017/2315 határozata (2017. december 11.) az állandó strukturált együttműködés (PESCO) létrehozásáról és a részt vevő tagállamok jegyzékének meghatározásáról.

[26] A Tanács (KKBP) 2017/2315 határozata (2017. december 11.) az állandó strukturált együttműködés (PESCO) létrehozásáról és

a részt vevő tagállamok jegyzékének meghatározásáról.

a részt vevő tagállamok jegyzékének meghatározásáról.

Módosítás 19

Rendeletre irányuló javaslat
26 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(26) Ez az eszköz nem érinti a válságelhárítás uniós szintű összehangolására szolgáló eljárásokat és kereteket, így különösen az uniós polgári védelmi mechanizmust[27], az uniós politikai szintű integrált válságelhárítási mechanizmust[28], sem az (EU) 2022/2555 irányelvet. Hozzájárulhat ugyanakkor az EUSZ 42. cikkének (7) bekezdésével összefüggésben vagy az EUMSZ 222. cikkében meghatározott helyzetekben végrehajtott intézkedésekhez, illetve kiegészítheti azokat. Ezen eszköz használatát ***adott esetben*** össze kell hangolni a kiberdiplomáciai eszköztár intézkedéseinek végrehajtásával is.	(26) Ez az eszköz nem érinti a válságelhárítás uniós szintű összehangolására szolgáló eljárásokat és kereteket, így különösen az uniós polgári védelmi mechanizmust[27], az uniós politikai szintű integrált válságelhárítási mechanizmust[28], sem az (EU) 2022/2555 irányelvet. Hozzájárulhat ugyanakkor az EUSZ 42. cikkének (7) bekezdésével összefüggésben vagy az EUMSZ 222. cikkében meghatározott helyzetekben végrehajtott intézkedésekhez, illetve kiegészítheti azokat. Ezen eszköz használatát össze kell hangolni a kiberdiplomáciai eszköztár intézkedéseinek végrehajtásával is***, fokozva a kibervédelmi és más kiberközösségek közötti stratégiai, operatív és technikai szintű együttműködést, különösen az Unión kívülről érkező kiberbiztonsági fenyegetésekkel szembeni képességek megerősítése érdekében, beleértve a korlátozó intézkedéseket is, amelyek felhasználhatók a rosszindulatú kibertevékenységek megelőzésére és az azokra való reagálásra***.
[27] Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).	[27] Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).
[28] Uniós politikai szintű integrált válságelhárítási mechanizmus (IPCR-mechanizmus) és a nagyszabású kiberbiztonsági eseményekre és	[28] Uniós politikai szintű integrált válságelhárítási mechanizmus (IPCR-mechanizmus) és a nagyszabású kiberbiztonsági eseményekre és

válsághelyzetekre való összehangolt reagálásról szóló, 2017. szeptember 13-i (EU) 2017/1584 bizottsági ajánlással összhangban.

válsághelyzetekre való összehangolt reagálásról szóló, 2017. szeptember 13-i (EU) 2017/1584 bizottsági ajánlással összhangban.

Módosítás 20

Rendeletre irányuló javaslat
28 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(28) Az (EU) 2022/2555 irányelv előírja a tagállamok számára, hogy jelöljenek ki vagy hozzanak létre egy vagy több, kiberválságok kezelésével foglalkozó hatóságot, és biztosítsák, hogy azok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes ellátásához. Előírja továbbá a tagállamok számára, hogy meghatározzák azon képességeket, eszközöket és eljárásokat, amelyek válság esetén alkalmazhatók, valamint hogy fogadjanak el nemzeti szintű nagyszabású kiberbiztonsági esemény- és válságelhárítási tervet, amelyben meghatározzák a nagyszabású kiberbiztonsági események és válsághelyzetek kezelésének célkitűzéseit és szabályait. A tagállamoknak továbbá létre kell hozniuk egy vagy több CSIRT-et, amelyek feladata a biztonsági események egy jól meghatározott folyamat szerinti kezelése, amely kiterjed legalább az említett irányelv hatálya alá tartozó ágazatokra, alágazatokra és szervezettípusokra, és biztosítaniuk kell, hogy hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen feladatai hatékony ellátásához. Ez a rendelet nem érinti a Bizottság szerepét annak biztosításában, hogy a tagállamok megfeleljenek az (EU) 2022/2555 irányelvben foglalt kötelezettségeknek. A kiberbiztonsági vészhelyzeti mechanizmusnak segítséget kell nyújtania a felkészültség megerősítésére irányuló	(28) Az (EU) 2022/2555 irányelv előírja a tagállamok számára, hogy jelöljenek ki vagy hozzanak létre egy vagy több, kiberválságok kezelésével foglalkozó hatóságot, és biztosítsák, hogy azok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes ellátásához. Előírja továbbá a tagállamok számára, hogy meghatározzák azon képességeket, eszközöket és eljárásokat, amelyek válság esetén alkalmazhatók, valamint hogy fogadjanak el nemzeti szintű nagyszabású kiberbiztonsági esemény- és válságelhárítási tervet, amelyben meghatározzák a nagyszabású kiberbiztonsági események és válsághelyzetek kezelésének célkitűzéseit és szabályait. A tagállamoknak továbbá létre kell hozniuk egy vagy több CSIRT-et, amelyek feladata a biztonsági események egy jól meghatározott folyamat szerinti kezelése, amely kiterjed legalább az említett irányelv hatálya alá tartozó ágazatokra, alágazatokra és szervezettípusokra, és biztosítaniuk kell, hogy hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen feladatai hatékony ellátásához. Ez a rendelet nem érinti a Bizottság szerepét annak biztosításában, hogy a tagállamok megfeleljenek az (EU) 2022/2555 irányelvben foglalt kötelezettségeknek. A kiberbiztonsági vészhelyzeti mechanizmusnak segítséget kell nyújtania a felkészültség megerősítésére irányuló

intézkedésekhez, valamint a jelentős és nagyszabású kiberbiztonsági események hatásának enyhítését, az azonnali helyreállítás támogatását és/vagy az alapvető szolgáltatások működésének helyreállítását célzó, kiberbiztonsági eseményekre való reagálással kapcsolatos intézkedésekhez.

intézkedésekhez, valamint a jelentős és nagyszabású kiberbiztonsági események hatásának enyhítését, az azonnali helyreállítás támogatását és/vagy az alapvető szolgáltatások működésének helyreállítását célzó, kiberbiztonsági eseményekre való reagálással kapcsolatos intézkedésekhez***, a polgári és katonai közösségek rendelkezésére álló védelmi lehetőségek teljes skálájának megfelelő felhasználásával***.

Módosítás 21

Rendeletre irányuló javaslat
29 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(29) A következetes megközelítés előmozdítása, valamint az Unió és belső piaca biztonságának megerősítése érdekében a felkészültségi intézkedések részeként támogatást kell nyújtani az (EU) 2022/2555 irányelv alapján azonosított, kiemelten kritikus ágazatokban működő szervezetek kiberbiztonságának összehangolt teszteléséhez és értékeléséhez. E célból a Bizottságnak az ENISA támogatásával és az (EU) 2022/2555 irányelvvel létrehozott Kiberbiztonsági Együttműködési Csoporttal együttműködésben rendszeresen azonosítania kell azokat az érintett ágazatokat vagy alágazatokat, amelyeket az uniós szinten összehangolt tesztelés összefüggésében pénzügyi támogatásra jogosultnak kell minősíteni. Az ***ágazatokat vagy alágazatokat*** az (EU) 2022/2555 irányelv I. mellékletéből („A kiemelten kritikus ágazatok”) ***kell kiválasztani***. Az összehangolt tesztelésnek közös kockázati forgatókönyveken és módszereken kell alapulnia. Az ágazatok kiválasztása és a kockázati forgatókönyvek kidolgozása során figyelembe kell venni a vonatkozó uniós szintű kockázatértékeléseket és kockázati forgatókönyveket, többek között	(29) A következetes megközelítés előmozdítása, valamint az Unió és belső piaca biztonságának megerősítése érdekében a felkészültségi intézkedések részeként támogatást kell nyújtani az (EU) 2022/2555 irányelv alapján azonosított, kiemelten kritikus ágazatokban működő szervezetek kiberbiztonságának összehangolt teszteléséhez és értékeléséhez. E célból a Bizottságnak az ENISA támogatásával és az (EU) 2022/2555 irányelvvel létrehozott Kiberbiztonsági Együttműködési Csoporttal együttműködésben rendszeresen azonosítania kell azokat az érintett ágazatokat vagy alágazatokat, amelyeket az uniós szinten összehangolt tesztelés összefüggésében pénzügyi támogatásra jogosultnak kell minősíteni. ***Adott esetben*** az ***Európai Külügyi Szolgálatot (EKSZ) – különösen az Európai Unió Hírszerző Központján (INTCEN) és annak hibrid fenyegetésekkel foglalkozó információs és elemzőcsoportján keresztül, az Európai Unió Katonai Törzsének (EUKT) az egységes információelemzési kapacitás (SIAC) alá tartozó hírszerzési igazgatóságának támogatásával – szintén be kell vonni a naprakész értékelések***

a párhuzamosságok elkerülése végett, például az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a Bizottsághoz, a főképviselőhöz és a Kiberbiztonsági Együttműködési Csoporthoz intézett felkérés szerinti, az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – többek között az EU-CyCLONe-nal – koordinációban elvégzendő kockázatértékeléssel és kidolgozandó kiberbiztonsági szempontú kockázati forgatókönyvvel, vagy a távközlési hálózatokra és infrastruktúrákra vonatkozóan a nevers-i közös miniszteri felhívás nyomán a Kiberbiztonsági Együttműködési Csoport által, a Bizottság és az ENISA támogatásával, az Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben elvégzendő kockázatértékeléssel, vagy az (EU) 2022/2555 irányelv 22. cikke alapján elvégzendő összehangolt kockázatértékelésekkel, illetve az (EU) 2022/2554 európai parlamenti és tanácsi ***rendeletben[29]*** előírt digitális működési reziliencia tesztelésével. Az ágazatok kiválasztásakor figyelembe kell venni a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlást is.

elkészítésébe, és ezáltal hozzá kell járulnia az (EU) 2022/2555 irányelv I. mellékletéből („A kiemelten kritikus ágazatok”) ***kiválasztandó ágazatok vagy alágazatok azonosításához***. Az összehangolt tesztelésnek közös kockázati forgatókönyveken és módszereken kell alapulnia***. Ezeknek a gyakorlatoknak fontos szerepet kell játszaniuk a polgári és katonai szervezetek közötti együttműködés javításában is. A gyakorlatok szervezésekor ezért a Bizottságnak, az EKSZ-nek és az ENISA-nak szisztematikusan mérlegelniük kell más kiberközösségek, például az Európai Védelmi Ügynökség (EDA) és más releváns szervezetek résztvevőinek bevonását.*** Az ágazatok kiválasztása és a kockázati forgatókönyvek kidolgozása során figyelembe kell venni a vonatkozó uniós szintű kockázatértékeléseket és kockázati forgatókönyveket, többek között a párhuzamosságok elkerülése végett, például az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a Bizottsághoz, a főképviselőhöz és a Kiberbiztonsági Együttműködési Csoporthoz intézett felkérés szerinti, az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – többek között az EU-CyCLONe-nal – koordinációban elvégzendő kockázatértékeléssel és kidolgozandó kiberbiztonsági szempontú kockázati forgatókönyvvel, vagy a távközlési hálózatokra és infrastruktúrákra vonatkozóan a nevers-i közös miniszteri felhívás nyomán a Kiberbiztonsági Együttműködési Csoport által, a Bizottság és az ENISA támogatásával, az Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben elvégzendő kockázatértékeléssel, vagy az (EU) 2022/2555 irányelv 22. cikke alapján elvégzendő összehangolt kockázatértékelésekkel, illetve az (EU) 2022/2554 európai parlamenti és tanácsi ***rendeletben[1]*** előírt digitális működési

reziliencia tesztelésével. Az ágazatok kiválasztásakor figyelembe kell venni a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlást is.

[1] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról.

---

[29] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról.

[29] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról.

Módosítás 22

Rendeletre irányuló javaslat
32 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(32) A kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell biztosítania azokban az esetekben, amikor a tagállamok segítséget nyújtanak egy jelentős vagy nagyszabású kiberbiztonsági esemény által érintett tagállamnak, többek között az (EU) 2022/2555 irányelv 15. cikkében meghatározott CSIRT-ek hálózata révén. A segítséget nyújtó tagállamok számára lehetővé kell tenni, hogy kérelmeket nyújtsanak be a szakértői csoportok kölcsönös segítségnyújtás keretében történő kiküldésével kapcsolatos költségek fedezésére. Az elszámolható költségek közé tartozhatnak a kiberbiztonsági szakértők utazási, szállás- és napidíjköltségei.	(32) A kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell biztosítania azokban az esetekben, amikor a tagállamok segítséget nyújtanak egy jelentős vagy nagyszabású kiberbiztonsági esemény által érintett tagállamnak, többek között az (EU) 2022/2555 irányelv 15. cikkében meghatározott CSIRT-ek hálózata révén. A segítséget nyújtó tagállamok számára lehetővé kell tenni, hogy kérelmeket nyújtsanak be a szakértői csoportok kölcsönös segítségnyújtás keretében történő kiküldésével kapcsolatos költségek fedezésére***, biztosítva a vonatkozó uniós programok és eszközök – többek között az Európai Békekeret, a KKBP és az NDICI – közötti hatékony koordinációt, amikor harmadik***

	országoknak, különösen Ukrajnának és Moldovának nyújtanak támogatást. Az elszámolható költségek közé tartozhatnak a kiberbiztonsági szakértők utazási, szállás- és napidíjköltségei.

Módosítás 23

Rendeletre irányuló javaslat
33 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(33) Fokozatosan létre kell hozni egy uniós szintű kiberbiztonsági tartalékot, amely az irányított biztonsági szolgáltatások magánszolgáltatói által nyújtott szolgáltatásokból áll, amelyek jelentős vagy nagyszabású kiberbiztonsági események alkalmával támogatják a reagálást és az azonnali helyreállítási intézkedéseket. Az uniós kiberbiztonsági tartalék keretében biztosítani kell a szolgáltatások rendelkezésre állását és készenlétét. Az uniós kiberbiztonsági tartalék szolgáltatásai a nemzeti hatóságokat hivatottak támogatni abban, hogy a saját nemzeti szintű intézkedéseik kiegészítéseként segítséget nyújtsanak a kritikus vagy kiemelten kritikus ágazatokban működő érintett szervezeteknek. Az uniós kiberbiztonsági tartalék keretében nyújtott támogatás kérelmezésekor a tagállamoknak meg kell határozniuk az érintett szervezetnek nemzeti szinten nyújtott támogatást, amelyet figyelembe kell venni a tagállami kérelem értékelésekor. Az uniós kiberbiztonsági tartalék szolgáltatásai hasonló feltételek mellett az uniós intézményeknek, szerveknek és ügynökségeknek is támogatást nyújthatnak.	(33) Fokozatosan létre kell hozni egy uniós szintű kiberbiztonsági tartalékot, amely az irányított biztonsági szolgáltatások magánszolgáltatói által nyújtott szolgáltatásokból áll, amelyek jelentős vagy nagyszabású kiberbiztonsági események alkalmával támogatják a reagálást és az azonnali helyreállítási intézkedéseket. Az uniós kiberbiztonsági tartalék keretében biztosítani kell a szolgáltatások rendelkezésre állását és készenlétét. Az uniós kiberbiztonsági tartalék szolgáltatásai a nemzeti hatóságokat hivatottak támogatni abban, hogy a saját nemzeti szintű intézkedéseik kiegészítéseként segítséget nyújtsanak a kritikus vagy kiemelten kritikus ágazatokban működő érintett szervezeteknek. Az uniós kiberbiztonsági tartalék keretében nyújtott támogatás kérelmezésekor a tagállamoknak meg kell határozniuk az érintett szervezetnek nemzeti szinten nyújtott támogatást, amelyet figyelembe kell venni a tagállami kérelem értékelésekor. Az uniós kiberbiztonsági tartalék szolgáltatásai hasonló feltételek mellett az uniós intézményeknek, szerveknek és ügynökségeknek***, többek között a KBVP-missziónak,*** is támogatást nyújthatnak.

Módosítás 24

Rendeletre irányuló javaslat
34 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(34) Az uniós kiberbiztonsági tartalék keretében szolgáltatásokat nyújtó magánszolgáltatók kiválasztása céljából meg kell határozni az e szolgáltatók kiválasztására irányuló ajánlati felhívásban szereplő minimumkritériumokat, biztosítva, hogy a tagállami hatóságok és a kritikus vagy kiemelten kritikus ágazatokban működő szervezetek igényei teljesüljenek.	(34) Az uniós kiberbiztonsági tartalék keretében szolgáltatásokat nyújtó magánszolgáltatók kiválasztása céljából meg kell határozni az e szolgáltatók kiválasztására irányuló ajánlati felhívásban szereplő minimumkritériumokat, biztosítva, hogy a tagállami hatóságok és a kritikus vagy kiemelten kritikus ágazatokban működő szervezetek igényei teljesüljenek***, figyelembe véve a stratégiai jelentőségű gazdasági versenytárs országok szolgáltatóinak részvételével kapcsolatos kockázatokat is, amelyek gazdasági biztonsági kockázatokat, valamint az Unió stratégiai biztonságára gyakorolt hatásokat eredményezhetnek***.

Módosítás 25

Rendeletre irányuló javaslat
36 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(36) E rendelet azon célkitűzéseinek támogatása érdekében, amelyek a közös helyzetismeret előmozdítására, az Unió rezilienciájának fokozására és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálás lehetővé tételére irányulnak, lehetővé kell tenni, hogy egy adott jelentős vagy nagyszabású kiberbiztonsági esemény kapcsán az EU-CyCLONe, a CSIRT-ek hálózata vagy a Bizottság felkérje az ENISA-t, hogy vizsgálja felül és értékelje a fenyegetéseket, a sebezhetőségeket és a mérséklési intézkedéseket. Az esemény felülvizsgálatának és értékelésének befejeztével az ENISA-nak az érintett érdekelt felekkel, többek között a	(36) E rendelet azon célkitűzéseinek támogatása érdekében, amelyek a közös helyzetismeret előmozdítására, az Unió rezilienciájának fokozására és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálás lehetővé tételére irányulnak, lehetővé kell tenni, hogy egy adott jelentős vagy nagyszabású kiberbiztonsági esemény kapcsán az EU-CyCLONe, a CSIRT-ek hálózata vagy a Bizottság felkérje az ENISA-t, hogy vizsgálja felül és értékelje a fenyegetéseket, a sebezhetőségeket és a mérséklési intézkedéseket. ***Tekintettel az európai kvantumkommunikációs infrastruktúrára (EuroQCI) és az Európai Unió állami műholdas kommunikációjára***

magánszektor, a tagállamok, a Bizottság és más érintett uniós intézmények, szervek és ügynökségek képviselőivel együttműködésben eseményértékelési jelentést kell készítenie. Ami a magánszektort illeti, az ENISA a szakosodott szolgáltatókkal – többek között az irányított biztonsági megoldások szolgáltatóival és értékesítőivel – folytatott információcserét szolgáló csatornákat fejleszt ki annak érdekében, hogy hozzájáruljon az ENISA azon küldetéséhez, hogy Unió-szerte egységesen magas szintű kiberbiztonságot érjen el. Az érdekelt felekkel – többek között a magánszektorral – folytatott együttműködésre építve a konkrét kiberbiztonsági eseményekkel kapcsolatos eseményértékelési jelentésnek arra kell irányulnia, hogy bekövetkezte után értékelje az esemény okait, hatásait és az azzal kapcsolatos mérséklési intézkedéseket. Különös figyelmet kell fordítani az e rendeletben előírt legmagasabb szintű szakmai feddhetetlenség, pártatlanság és szükséges technikai szakértelem feltételeinek megfelelő irányított biztonsági szolgáltatók által megosztott információkra és tapasztalatokra. A jelentést az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak kell benyújtani, amelyeknek azt munkájuk során figyelembe kell venniük. Ha az esemény harmadik országgal kapcsolatos, a Bizottságnak meg kell osztania a jelentést a főképviselővel.

(GOVSATCOM) épülő biztonságos összeköttetési rendszer kidolgozására és különösen a GALILEO BNSS védelmi felhasználók számára történő bevezetésére, minden lehetséges jövőbeli fejlesztésnek figyelembe kell vennie a gyors és kifinomult kvantuminformatika rendkívül autonóm katonai rendszerekkel történő összekapcsolásából fakadó „hyperwar” új keletű veszélyét. Az esemény felülvizsgálatának és értékelésének befejeztével az ENISA-nak az érintett érdekelt felekkel, többek között a magánszektor, a tagállamok, a Bizottság és más érintett uniós intézmények, szervek és ügynökségek képviselőivel együttműködésben eseményértékelési jelentést kell készítenie. Ami a magánszektort illeti, az ENISA a szakosodott szolgáltatókkal – többek között az irányított biztonsági megoldások szolgáltatóival és értékesítőivel – folytatott információcserét szolgáló csatornákat fejleszt ki annak érdekében, hogy hozzájáruljon az ENISA azon küldetéséhez, hogy Unió-szerte egységesen magas szintű kiberbiztonságot érjen el. Az érdekelt felekkel – többek között a magánszektorral – folytatott együttműködésre építve a konkrét kiberbiztonsági eseményekkel kapcsolatos eseményértékelési jelentésnek arra kell irányulnia, hogy bekövetkezte után értékelje az esemény okait, hatásait és az azzal kapcsolatos mérséklési intézkedéseket. Különös figyelmet kell fordítani az e rendeletben előírt legmagasabb szintű szakmai feddhetetlenség, pártatlanság és szükséges technikai szakértelem feltételeinek megfelelő irányított biztonsági szolgáltatók által megosztott információkra és tapasztalatokra. A jelentést az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak kell benyújtani, amelyeknek azt munkájuk során figyelembe kell venniük. Ha az esemény harmadik országgal kapcsolatos, a Bizottságnak meg kell osztania a jelentést a

főképviselővel***, az EKSZ-szel és az esemény által érintett országban működő bármely KBVP-misszióval is központján keresztül***.

Módosítás 26

Rendeletre irányuló javaslat
37 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(37) Figyelembe véve a kiberbiztonsági támadások kiszámíthatatlan jellegét és azt, hogy azok gyakran nem korlátozódnak egy adott földrajzi területre, és így a tovagyűrűzés magas kockázatát hordozzák magukban, a szomszédos országok rezilienciájának és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálási képességüknek a megerősítése hozzájárul az Unió egészének védelméhez. Ezért a Digitális Európa programhoz társult harmadik ***országok*** is ***részesülhetnek*** az uniós kiberbiztonsági tartalékból nyújtott támogatásban, ***amennyiben erről*** a ***Digitális Európa programban való részvételükről kötött társulási megállapodás rendelkezik***. A társult harmadik országok a vonatkozó partnerségek és finanszírozási eszközök keretében részesülnek az Unió nyújtotta finanszírozásból. A támogatásnak ki kell terjednie a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálás és az eseményt követő azonnali helyreállítás területén nyújtott szolgáltatásokra. Az e rendeletben az uniós kiberbiztonsági tartalékra és a megbízható szolgáltatókra vonatkozóan meghatározott feltételeket alkalmazni kell a Digitális Európa programhoz társult harmadik országoknak nyújtott támogatásokra.	(37) Figyelembe véve a kiberbiztonsági támadások kiszámíthatatlan jellegét és azt, hogy azok gyakran nem korlátozódnak egy adott földrajzi területre, és így a tovagyűrűzés magas kockázatát hordozzák magukban, a szomszédos országok***, különösen Ukrajna és Moldova*** rezilienciájának és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálási képességüknek a megerősítése hozzájárul az Unió egészének védelméhez. Ezért a Digitális Európa programhoz társult harmadik ***országoknak*** is ***részesülniük kell*** az uniós kiberbiztonsági tartalékból nyújtott támogatásban***. A támogatás azokra a harmadik országokra is vonatkozik***, ***amelyekben a KBVP-missziót a hibrid fenyegetésekkel – többek között*** a ***kiberfenyegetésekkel – szembeni reziliencia megerősítésére irányuló konkrét megbízatással telepítették, vagy amelyekben az Európai Békekeretből nyújtott támogatást az ország kiberrezilienciájának megerősítése érdekében elfogadták***. A társult harmadik országok a vonatkozó partnerségek és finanszírozási eszközök keretében részesülnek az Unió nyújtotta finanszírozásból. A támogatásnak ki kell terjednie a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálás és az eseményt követő azonnali helyreállítás területén nyújtott szolgáltatásokra. Az e rendeletben az uniós kiberbiztonsági tartalékra és a megbízható

szolgáltatókra vonatkozóan meghatározott feltételeket alkalmazni kell a Digitális Európa programhoz társult harmadik országoknak nyújtott támogatásokra.

Módosítás 27

Rendeletre irányuló javaslat
1 cikk – 1 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) a kiberbiztonsági események európai felülvizsgálati mechanizmusának létrehozása konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából.	c) a kiberbiztonsági események európai felülvizsgálati mechanizmusának létrehozása konkrét jelentős vagy nagyszabású kiberbiztonsági események ***vagy veszélyek*** felülvizsgálata és értékelése céljából.

Módosítás 28

Rendeletre irányuló javaslat
1 cikk – 2 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) a kiberbiztonsági fenyegetések és események közös uniós észlelésének és helyzetismeretének megerősítése, lehetővé téve ezáltal az uniós ipari és szolgáltatási ágazatok versenyhelyzetének megerősítését a digitális gazdaság egészében, valamint hozzájárulás az Unió technológiai ***szuverenitásához*** a kiberbiztonság területén;	a) a kiberbiztonsági fenyegetések és események közös uniós észlelésének és helyzetismeretének megerősítése, lehetővé téve ezáltal az uniós ipari és szolgáltatási ágazatok versenyhelyzetének megerősítését a digitális gazdaság egészében, valamint hozzájárulás az Unió technológiai ***rezilienciához*** a kiberbiztonság területén;

Módosítás 29

Rendeletre irányuló javaslat
1 cikk – 2 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) a kritikus és a kiemelten kritikus ágazatokban működő szervezetek felkészültségének megerősítése Unió-	b) a kritikus és a kiemelten kritikus ágazatokban működő szervezetek felkészültségének megerősítése Unió-

szerte, valamint a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, többek között a Digitális Európa programhoz társult harmadik országok számára kiberbiztonsági eseményekre való reagáláshoz nyújtott uniós támogatással;	szerte, valamint a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, többek között a Digitális Európa programhoz társult harmadik országok számára kiberbiztonsági eseményekre való reagáláshoz nyújtott uniós támogatással***, vagy olyan harmadik országok számára, amelyek tagjelölt országok, és amelyek nem ellentétesek az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel; A tagállamoknak nemzeti kiberbiztonsági stratégiájuk aktív kibervédelmi programot kell kialakítaniuk, amely a tagállamok és nemzetközi szervezetek által közösen szervezett képzéseket foglal magában. E programnak képesnek kell lennie, hogy összehangolt módon és valós időben feltárja, felderítse, elemezze és mérsékelje a fenyegetéseket***;

Módosítás 30

Rendeletre irányuló javaslat
1 cikk – 2 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(2a) az olyan országokból származó kritikus berendezésektől való függőségből eredő rendszerszintű kiberbiztonsági kockázatok csökkentése, amelyek ellentétesek lennének az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel;.

Módosítás 31

Rendeletre irányuló javaslat
2 cikk – 2 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	„kibervédelmi közösség”: a tagállamok védelmi hatóságtagállamok védelmi hatóságaiból álló és az uniós intézmények, szervek és hivatalok által támogatott közösség, az EU kibervédelmi politikájáról szóló közös közleményben[1] meghatározottak szerint
	[1] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022) 49 final.

Módosítás 32

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – b a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	ba) a teljes kibervédelmi rendszer korszerűsítésének elősegítése, a kibervédelmi képességek minőségének javítása MI-rendszerek telepítése révén, valamint a nemzeti SOC-ok és a határokon átnyúló SOC-ok közötti információcsere felgyorsítása;

Módosítás 33

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – d a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	da) felülvizsgálja és értékeli az olyan országok által a nagy kockázatú szolgáltatók feletti ellenőrzésből eredő rendszerszintű kockázatokkal kapcsolatos kiberbiztonsági eseményekre való reagálás során a biztonsági műveleti központok által alkalmazott kritikus kiberbiztonsági technológiákat és berendezéseket, amelyek ellentétesek

	lennének az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel.

Módosítás 34

Rendeletre irányuló javaslat
4 cikk – 1 bekezdés – 2 albekezdés

A Bizottság által javasolt szöveg	*Módosítás*
Képesnek kell lennie arra, hogy nemzeti szintű referenciapontként és átjáróként szolgáljon más állami és ***magánszervezetek*** számára a kiberbiztonsági fenyegetésekre és eseményekre vonatkozó információk gyűjtése és elemzése, valamint a valamely határokon átnyúló biztonsági műveleti központhoz való hozzájárulás tekintetében. Fel kell szerelni a kiberbiztonsági fenyegetések és események észlelésére, valamint a kapcsolódó adatok összesítésére és elemzésére alkalmas legkorszerűbb technológiákkal.	Képesnek kell lennie arra, hogy nemzeti szintű referenciapontként és átjáróként szolgáljon más állami és ***magán-, és szükség esetén katonai szervezetek*** számára a kiberbiztonsági fenyegetésekre és eseményekre vonatkozó információk gyűjtése és elemzése, valamint a valamely határokon átnyúló biztonsági műveleti központhoz való hozzájárulás tekintetében. Fel kell szerelni a kiberbiztonsági fenyegetések és események észlelésére, valamint a kapcsolódó adatok összesítésére és elemzésére alkalmas legkorszerűbb technológiákkal.

Módosítás 35

Rendeletre irányuló javaslat
4 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) részvételi szándék kifejezésére való felhívás nyomán választja ki azokat a nemzeti biztonsági műveleti központokat, amelyek részt vesznek az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda a kiválasztott nemzeti biztonsági műveleti központoknak az említett eszközök és infrastruktúrák működtetésének finanszírozására. Az uniós	(2) Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) részvételi szándék kifejezésére való felhívás nyomán választja ki azokat a nemzeti biztonsági műveleti központokat, amelyek részt vesznek az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda a kiválasztott nemzeti biztonsági műveleti központoknak az említett eszközök és infrastruktúrák működtetésének finanszírozására***, azzal a***

pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 50 %-át és a működési költségek legfeljebb 50 %-át fedezi, a fennmaradó költségek pedig a tagállamra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és a nemzeti biztonsági műveleti központ az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.	***szigorú feltétellel, hogy ezeket az eszközöket és infrastruktúrát a 16. cikkel összhangban megbízható szolgáltatók biztosítják***. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 50%-át és a működési költségek legfeljebb 50%-át fedezi, a fennmaradó költségek pedig a tagállamra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és a nemzeti biztonsági műveleti központ az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

Módosítás 36

Rendeletre irányuló javaslat
5 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az ECCC részvételi szándék kifejezésére való felhívás nyomán választja ki azt az üzemeltetési konzorciumot, amely részt vesz az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda az üzemeltetési konzorciumnak az említett eszközök és infrastruktúrák működtetésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 75 %-át és a működési költségek legfeljebb 50 %-át fedezi, a fennmaradó költségek pedig az üzemeltetési konzorciumra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és az üzemeltetési konzorcium az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.	(2) Az ECCC részvételi szándék kifejezésére való felhívás nyomán választja ki azt az üzemeltetési konzorciumot, amely részt vesz az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda az üzemeltetési konzorciumnak az említett eszközök és infrastruktúrák működtetésének finanszírozására***, azzal a szigorú feltétellel, hogy ezeket az eszközöket és infrastruktúrát a 16. cikkel összhangban megbízható szolgáltatók biztosítják***. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 75%-át és a működési költségek legfeljebb 50%-át fedezi, a fennmaradó költségek pedig az üzemeltetési konzorciumra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és az üzemeltetési konzorcium az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

Módosítás 37

Rendeletre irányuló javaslat
5 cikk – 2 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(2a) A kiemelt kockázatot jelentő harmadik országból származó infrastruktúrát vagy szolgáltatót automatikusan ki kell zárni.

Módosítás 38

Rendeletre irányuló javaslat
6 cikk – 2 bekezdés – b a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	ba) közvetlenül támogatja a részt vevő tagok katonai és védelmi képességeinek megerősítését, vagy megelőzi a biztonságukat fenyegető közvetlen és azonnali veszélyt. Mivel a védelmi ágazatban a gyenge pontok ellen indított támadás jelentős fennakadásokat és károkat okozhat, a védelmi ipar kiberbiztonsága különleges intézkedéseket tesz szükségessé az ellátási láncok biztonságának garantálása érdekében, különösen az ellátási láncok alacsonyabb szintjein elhelyezkedő szervezetek esetében, amelyek hozzáférése minősített adatokhoz nem szükséges, mégis komoly kockázatokat jelenthetnek az egész ágazatra nézve. Különös figyelmet kell fordítani az esetleges jogsértések lehetséges hatásaira, valamint a hálózati adatok olyan manipulálásának veszélyére, amely kritikus védelmi eszközöket tehet használhatatlanná, vagy akár felülírhatja operációs rendszereiket, ami kiszolgáltatottá teheti őket az adattartományok elrablásával szemben.

Módosítás 39

Rendeletre irányuló javaslat
6 cikk – 2 bekezdés – b b pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	bb) támogatja a részt vevő tagok védelmi képességeinek megerősítését, vagy megelőzi a biztonságukat fenyegető közvetlen és azonnali veszélyt, garantálva az ellátási láncok biztonságát, különösen az ellátási láncok alacsonyabb szintjein elhelyezkedő szervezetek esetében, amelyek hozzáférése minősített adatokhoz nem szükséges, mégis komoly kockázatokat jelenthetnek az egész ágazatra nézve.

Módosítás 40

Rendeletre irányuló javaslat
7 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Ha a határokon átnyúló biztonsági műveleti központok információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a releváns információkat az (EU) 2022/2555 irányelv szerinti válságkezelési szerepük figyelembevételével indokolatlan késedelem nélkül eljuttatják az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak.	(1) Ha a határokon átnyúló biztonsági műveleti központok információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a releváns információkat az (EU) 2022/2555 irányelv szerinti válságkezelési szerepük figyelembevételével indokolatlan késedelem nélkül eljuttatják az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak***, beleértve a főképviselőt és az EKSZ-t is, ha az egy harmadik országot érint***.

Módosítás 41

Rendeletre irányuló javaslat
8 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az Európai Kiberpajzsban részt	(1) Az Európai Kiberpajzsban részt

vevő tagállamok gondoskodnak az Európai Kiberpajzs infrastruktúrájának magas szintű adatbiztonságáról és fizikai biztonságáról, biztosítják, hogy az infrastruktúrát megfelelő irányítás és ellenőrzés révén megvédjék a fenyegetésektől, továbbá biztosítják az infrastruktúra és a rendszerek **–** ***többek között*** az infrastruktúrán keresztül kicserélt adatok **–** ***biztonságát is***.	vevő tagállamok gondoskodnak az Európai Kiberpajzs infrastruktúrájának magas szintű adatbiztonságáról és fizikai biztonságáról, biztosítják, hogy az infrastruktúrát megfelelő irányítás és ellenőrzés révén megvédjék a fenyegetésektől, továbbá biztosítják az infrastruktúra és a rendszerek ***biztonságát is, csökkentve a kockázatot és elősegítve az EU technológiai előnyét a kritikus ágazatokban, beleértve a nagy kockázatot jelentő beszállítók korlátozására vagy kizárására irányuló intézkedéseket, valamint*** az infrastruktúrán keresztül kicserélt adatok ***biztonságának védelmét***.

Módosítás 42

Rendeletre irányuló javaslat
8 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak arról, hogy az Európai Kiberpajzs keretében nem tagállami közjogi szerveknek minősülő szervezetekkel folytatott információmegosztás ne érintse hátrányosan az Unió biztonsági érdekeit.	(2) Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak arról, hogy az Európai Kiberpajzs keretében nem tagállami közjogi szerveknek minősülő szervezetekkel folytatott információmegosztás ne érintse hátrányosan az Unió biztonsági érdekeit***, és hogy a nagy kockázatot jelentő szolgáltatókkal való bármilyen információmegosztás korlátozott terjedelmű legyen, és ne sértse az Unió biztonsági és stratégiai érdekeit***.

Módosítás 43

Rendeletre irányuló javaslat
8 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben technikai követelményeket állapít meg a tagállamok számára az (1) és (2) bekezdés	(3) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben technikai követelményeket állapít meg a tagállamok számára az (1) és (2) bekezdés

szerinti kötelezettségeik teljesítéséhez. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. Ennek során a katonai szereplőkkel való együttműködés megkönnyítése érdekében a Bizottság – a főképviselő támogatásával – figyelembe veszi a vonatkozó védelmi szintű biztonsági előírásokat.	szerinti kötelezettségeik teljesítéséhez. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. Ennek során a katonai szereplőkkel való együttműködés megkönnyítése érdekében a Bizottság – a főképviselő támogatásával – figyelembe veszi a vonatkozó védelmi szintű biztonsági előírásokat***, megfelelően kihasználva a polgári és katonai közösségek számára az EU szélesebb körű biztonsága és védelme érdekében rendelkezésre álló védelmi lehetőségek teljes körét, és tájékoztatja az Európai Parlamentet***.

Módosítás 44

Rendeletre irányuló javaslat
9 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A kiberbiztonsági vészhelyzeti mechanizmust végrehajtó intézkedéseket a Digitális Európa programból nyújtott finanszírozással kell támogatni, és az (EU) 2021/694 rendelettel és különösen annak 3. egyedi célkitűzésével összhangban kell végrehajtani**.**	(2) A kiberbiztonsági vészhelyzeti mechanizmust végrehajtó intézkedéseket a Digitális Európa programból nyújtott finanszírozással kell támogatni, és az (EU) 2021/694 rendelettel és különösen annak 3. egyedi célkitűzésével összhangban kell végrehajtani***, továbbá az Európai Békekeretből kell támogatni, amikor harmadik országok, különösen Ukrajna és Moldova számára hoznak támogatási intézkedéseket;***

Módosítás 45

Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) felkészültségi intézkedések, amelyek magukban foglalják a kiemelten kritikus ágazatokban működő szervezetek Unió-szerte összehangolt felkészültségi	a) felkészültségi intézkedések, amelyek magukban foglalják a kiemelten kritikus ágazatokban ***– például állami infrastruktúrák, választási***

tesztelését;	***infrastruktúrák, közlekedés, egészségügy, pénzügyek, telekommunikáció, élelmiszer-ellátás és biztonság –*** működő szervezetek Unió-szerte összehangolt felkészültségi tesztelését;

Módosítás 46

Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) kölcsönös segítségnyújtási intézkedések, amelyek magukban foglalják az egyik tagállam nemzeti hatóságai által egy másik tagállamnak nyújtott segítséget, különösen az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének f) pontjában előírtak szerint.	c) kölcsönös segítségnyújtási intézkedések, amelyek magukban foglalják az egyik tagállam nemzeti hatóságai által egy másik tagállamnak nyújtott segítséget, különösen az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének f) pontjában előírtak szerint***, valamint az EUSZ 42. cikkének (7) bekezdésével és az EUMSZ 222. cikkével összefüggésben***.

Módosítás 47

Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – c a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	ca) az olyan nagy kockázatot jelentő beszállítók kritikus berendezéseinek lecserélése és fokozatos kivonása, amelyek ellentétesek lennének az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel.

Módosítás 48

Rendeletre irányuló javaslat
11 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Kiberbiztonsági Együttműködési	(2) A Kiberbiztonsági Együttműködési

Csoport a Bizottsággal, az ENISA-val és ***a főképviselővel*** együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt teszteléshez.	Csoport a Bizottsággal, az ENISA-val***, a főképviselővel, az EKSZ-szel,*** és ***adott esetben az EDA-val*** együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt teszteléshez.

Módosítás 49

Rendeletre irányuló javaslat
12 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az uniós kiberbiztonsági tartalék a 16. cikkben meghatározott kritériumoknak megfelelően kiválasztott megbízható szolgáltatók eseményreagálási szolgáltatásaiból áll össze. A tartalék előzetes kötelezettségvállalás keretében rendelkezésre bocsátott szolgáltatásokat tartalmaz. A szolgáltatások valamennyi tagállamban igénybe vehetők.	(2) Az uniós kiberbiztonsági tartalék a 16. cikkben meghatározott kritériumoknak megfelelően kiválasztott megbízható szolgáltatók eseményreagálási szolgáltatásaiból áll össze. A tartalék előzetes kötelezettségvállalás keretében rendelkezésre bocsátott szolgáltatásokat tartalmaz. A szolgáltatások ***az e rendelet alkalmazandó követelményeinek megfelelő*** valamennyi tagállamban ***és harmadik országban*** igénybe vehetők.

Módosítás 50

Rendeletre irányuló javaslat
12 cikk – 3 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) az uniós intézmények, szervek és ügynökségek.	b) az uniós intézmények, szervek és ügynökségek***, beleértve a KBVP-missziókat is***.

Módosítás 51

Rendeletre irányuló javaslat
12 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A (3) bekezdés a) pontjában említett felhasználóknak az uniós	(4) A (3) bekezdés a) pontjában említett felhasználóknak az uniós

kiberbiztonsági tartalék szolgáltatásait kell igénybe venniük a kritikus vagy kiemelten kritikus ágazatokban működő szervezeteket érintő jelentős vagy nagyszabású biztonsági eseményekre való reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.	kiberbiztonsági tartalék szolgáltatásait kell igénybe venniük a kritikus vagy kiemelten kritikus ágazatokban ***– például az állami infrastruktúrában, a választási infrastruktúrában, a közlekedésben, az egészségügyben, a pénzügyi szférában, a telekommunikációban, az élelmiszer-ellátásban és a biztonság területén –*** működő szervezeteket érintő jelentős vagy nagyszabású biztonsági eseményekre való reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.

Módosítás 52

Rendeletre irányuló javaslat
12 cikk – 5 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(5) A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság a (3) bekezdésben említett felhasználók igényeivel összhangban határozza meg az uniós kiberbiztonsági tartalék prioritásait és alakulását, továbbá felügyeli annak végrehajtását, és biztosítja az e rendelet szerinti egyéb támogatási intézkedésekkel, valamint az egyéb uniós intézkedésekkel és programokkal való kiegészítő jelleget, következetességet, szinergiákat és kapcsolatokat.	(5) A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság a (3) bekezdésben említett felhasználók igényeivel összhangban határozza meg az uniós kiberbiztonsági tartalék prioritásait és alakulását, továbbá felügyeli annak végrehajtását, és biztosítja az e rendelet szerinti egyéb támogatási intézkedésekkel, valamint az egyéb uniós intézkedésekkel és programokkal való kiegészítő jelleget, következetességet, szinergiákat és kapcsolatokat ***és célkitűzéseket, különösen azt a stratégiai célkitűzést, hogy csökkentsük az olyan nagy kockázatot jelentő beszállítóktól való függőséget, amelyek ellentétesek lennének az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel***.

Módosítás 53

Rendeletre irányuló javaslat
12 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) Annak érdekében, hogy támogassa a Bizottságot az uniós kiberbiztonsági tartalék létrehozásában, az ENISA a tagállamokkal és a Bizottsággal folytatott konzultációt követően feltérképezi a szükséges szolgáltatásokat. Az ENISA a Bizottsággal folytatott konzultációt követően hasonló feltérképezést készít az uniós kiberbiztonsági tartalék keretében a 17. cikk alapján támogatásra jogosult harmadik országok szükségleteinek azonosítása érdekében. A Bizottság adott esetben konzultál a főképviselővel.	(7) Annak érdekében, hogy támogassa a Bizottságot az uniós kiberbiztonsági tartalék létrehozásában, az ENISA a tagállamokkal és a Bizottsággal folytatott konzultációt követően feltérképezi a szükséges szolgáltatásokat. Az ENISA a Bizottsággal folytatott konzultációt követően hasonló feltérképezést készít az uniós kiberbiztonsági tartalék keretében a 17. cikk alapján támogatásra jogosult ***és az EKSZ által támogatott*** harmadik országok szükségleteinek azonosítása érdekében. A Bizottság adott esetben konzultál a főképviselővel.

Módosítás 54

Rendeletre irányuló javaslat
14 cikk – 2 bekezdés – a a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	aa) az esemény hatása az Unió biztonságára és védelmére;

Módosítás 55

Rendeletre irányuló javaslat
15 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A főképviselővel folytatott konzultáció alapján a kiberbiztonsági vészhelyzeti mechanizmus keretében nyújtott támogatás kiegészítheti a közös kül- és biztonságpolitika, valamint a közös biztonság- és védelempolitika keretében – többek között a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású	(3) A főképviselővel folytatott konzultáció alapján a kiberbiztonsági vészhelyzeti mechanizmus keretében nyújtott támogatás kiegészítheti a közös kül- és biztonságpolitika, valamint a közös biztonság- és védelempolitika keretében – többek között a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású

csoportok révén – nyújtott segítséget. Kiegészítheti továbbá az egyik tagállam által egy másik tagállamnak az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésével összefüggésben nyújtott segítséget, vagy hozzájárulhat ahhoz.	csoportok ***(CCRT-k)*** révén – nyújtott segítséget ***annak érdekében, hogy jobban támogassa az uniós tagállamokat, a KBVP-missziókat és -műveleteket, valamint azokat a harmadik országokat, különösen Ukrajnát és Moldovát, amelyek joganyagukat már harmonizálták az EU közös kül- és biztonságpolitikájával és közös biztonság- és védelempolitikájával a kibervédelmi kapacitásépítési erőfeszítéseik során***. Kiegészítheti továbbá az egyik tagállam által egy másik tagállamnak az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésével összefüggésben nyújtott segítséget, vagy hozzájárulhat ahhoz.

Módosítás 56

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – b a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	aa) a szolgáltatónak bizonyítania kell, hogy döntési és irányítási struktúrái mentesek bármely állam kormányának olyan indokolatlan befolyásától, amely ellentétes lenne az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel;

Módosítás 57

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – f pont

A Bizottság által javasolt szöveg	*Módosítás*
f) a szolgáltatónak rendelkeznie kell a kért szolgáltatáshoz szükséges műszaki berendezésekkel, beleértve a hardvereket és szoftvereket is;	f) a szolgáltatónak rendelkeznie kell a kért szolgáltatáshoz szükséges műszaki berendezésekkel, beleértve a hardvereket és szoftvereket is***, és meg kell felelnie a(z) XX/XXXX rendelet (a kiberrezilienciáról szóló jogszabály) X. cikkében***

meghatározott követelményeknek;

Módosítás 58

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – j a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	ja) a kiemelt kockázatot jelentő harmadik országból származó szolgáltatók nem fogadhatók el.

Módosítás 59

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – j b pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	jb) a szolgáltatónak lehetőség szerint szorosan együtt kell működnie az érintett kkv-kkal;

Módosítás 60

Rendeletre irányuló javaslat
17 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az uniós kiberbiztonsági tartalék nyújtotta támogatást harmadik országok is kérelmezhetik, ha a velük kötött társulási megállapodás a Digitális Európa programban való részvételükről ekképpen rendelkezik.	(1) Az uniós kiberbiztonsági tartalék nyújtotta támogatást harmadik országok is kérelmezhetik, ha***:***
	a) a velük kötött társulási megállapodás a Digitális Európa programban való részvételükről ekképpen rendelkezik***;***
	b) azok a harmadik országok, amelyekben a KBVP-missziót a hibrid fenyegetésekkel – többek között a kiberfenyegetésekkel – szembeni

	reziliencia megerősítésére irányuló konkrét megbízatással telepítették, vagy amelyekben az Európai Békekeretből nyújtott támogatást az ország kiberrezilienciájának megerősítése érdekében elfogadták.

Módosítás 61

Rendeletre irányuló javaslat
17 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az uniós kiberbiztonsági tartalékból nyújtott támogatásnak összhangban kell lennie e rendelettel, és meg kell felelnie az (1) ***bekezdésben*** említett társulási megállapodásokban meghatározott bármely egyedi feltételnek.	(2) Az uniós kiberbiztonsági tartalékból nyújtott támogatásnak összhangban kell lennie e rendelettel, és meg kell felelnie az (1) ***bekezdés b) pontjában*** említett társulási megállapodásokban meghatározott bármely egyedi feltételnek***, kivéve az (1) bekezdés b) pontjában meghatározott rendelkezések hatálya alá tartozó harmadik országokat***.

Módosítás 62

Rendeletre irányuló javaslat
18 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) A Bizottság, az EU-CyCLONe vagy a CSIRT-ek hálózatának kérésére az ENISA felülvizsgálja és értékeli az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó fenyegetéseket, sebezhetőségeket és mérséklési intézkedéseket. Egy adott kiberbiztonsági esemény felülvizsgálatának és értékelésének lezárultával az ENISA eseményértékelési jelentést nyújt be a CSIRT-ek hálózatának, az EU-CyCLONe-nak és a Bizottságnak, hogy támogassa őket – különösen az (EU) 2022/2555 irányelv 15. és 16. cikkében foglalt – feladataik ellátásában. A Bizottság adott esetben megosztja a jelentést a	(1) A Bizottság, az EU-CyCLONe vagy a CSIRT-ek hálózatának kérésére az ENISA felülvizsgálja és értékeli az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó fenyegetéseket, sebezhetőségeket és mérséklési intézkedéseket. Egy adott kiberbiztonsági esemény felülvizsgálatának és értékelésének lezárultával az ENISA eseményértékelési jelentést nyújt be a CSIRT-ek hálózatának, az EU-CyCLONe-nak és a Bizottságnak, hogy támogassa őket – különösen az (EU) 2022/2555 irányelv 15. és 16. cikkében foglalt – feladataik ellátásában. A Bizottság***, különösen, ha az incidens harmadik***

főképviselővel.	***országot érint,*** adott esetben megosztja a jelentést a főképviselővel ***és az EKSZ-szel***.

Módosítás 63

Rendeletre irányuló javaslat
18 cikk – 3 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(3a) A jelentést a minősített érzékeny adatok védelmére vonatkozó uniós vagy nemzeti jogszabályokkal összhangban kell megosztani az Európai Parlamenttel.

Módosítás 64

Rendeletre irányuló javaslat
19 cikk – 1 bekezdés – 1 pont – a pont –1 pont
(EU) 2021/694 rendelet
6 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
aa) az Európai Kiberpajzs kialakításának támogatása, beleértve a nemzeti és a határokon átnyúló biztonsági műveleti központok platformjainak fejlesztését, telepítését és működtetését, amelyek hozzájárulnak az Unión belüli helyzetismerethez és az Unió kiberfenyegetettségi információszerző képességeinek megerősítéséhez;	aa) az Európai Kiberpajzs kialakításának támogatása, beleértve a nemzeti és a határokon átnyúló biztonsági műveleti központok platformjainak fejlesztését, telepítését és működtetését, amelyek hozzájárulnak az Unión belüli helyzetismerethez és az Unió kiberfenyegetettségi információszerző képességeinek megerősítéséhez***, valamint az Uniónak a kritikus fontosságú kiberbiztonsági berendezések vagy alkatrészek magas kockázatú szolgáltatóitól való függőségének csökkentéséhez, amely ellentétes lenne az Uniónak és tagállamainak az EUSZ V. címe szerinti, a KKBP keretében meghatározott biztonsági és védelmi érdekeivel***;

Módosítás 65

Rendeletre irányuló javaslat
20 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
A Bizottság ***[négy*** évvel e rendelet alkalmazásának kezdőnapját követően]-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet értékeléséről és felülvizsgálatáról.	A Bizottság ***[három*** évvel e rendelet alkalmazásának kezdőnapját követően]-ig ***majd azt követően kétévente*** jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet értékeléséről és felülvizsgálatáról.

A VÉLEMÉNYNYILVÁNÍTÁSRA FELKÉRT BIZOTTSÁG ELJÁRÁSA

Cím	A kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározása
Hivatkozások	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Illetékes bizottság A plenáris ülésen való bejelentés dátuma	ITRE 1.6.2023
Véleményt nyilvánított A plenáris ülésen való bejelentés dátuma	AFET 1.6.2023
A vélemény előadója A kijelölés dátuma	Dragoş Tudorache 16.6.2023
Vizsgálat a bizottságban	18.9.2023
Az elfogadás dátuma	24.10.2023
A zárószavazás eredménye	+: 39 –: 4 0: 0
A zárószavazáson jelen lévő tagok	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
A zárószavazáson jelen lévő póttagok	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

A VÉLEMÉNYNYILVÁNÍTÁSRA FELKÉRT BIZOTTSÁG

NÉV SZERINTI ZÁRÓSZAVAZÁSA

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

Jelmagyarázat:
+ : mellette
- : ellene
0 : tartózkodás