Európai Parlament
2019-2024

Ipari, Kutatási és Energiaügyi Bizottság

2023/0109(COD)

22.9.2023

MÓDOSÍTÁS: 46 - 216

Jelentéstervezet
Lina Gálvez Muñoz
(PE752.795v01-00)

A kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározása

Rendeletre irányuló javaslat
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Módosítás 46
Evžen Tošenovský

Rendeletre irányuló javaslat
1 cím

A Bizottság által javasolt szöveg	*Módosítás*
JavaslatAZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETEa kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról	JavaslatAZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETEa kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról ***(a kiberbiztonsági szolidaritásról szóló jogszabály)***

Or. en

Módosítás 47
Ville Niinistö
a Verts/ALE képviselőcsoport nevében

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 ***és sebezhetőséggé*** 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.

Or. en

Indokolás

E jogi szöveg szükségessége abból adódik, hogy az alapvető függések sebezhetőséggé is válnak.

Módosítás 48
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 akadályozhatják a közszolgáltatások nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, alááshatják 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.	(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 ***Unió-szerte*** 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 akadályozhatják a közszolgáltatások nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, alááshatják 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.

Ezért az Unió kiberbiztonsági helyzetének javítása érdekében szoros és összehangolt együttműködésre van szükség a közszféra, a magánszektor, a tagállamok, az uniós intézmények vagy ügynökségek, valamint a tudományos körök között. Az Unió válaszlépésének a megbízható és hasonlóan gondolkodó nemzetközi partnerekkel és nemzetközi intézményekkel együttműködve, valamint a nemzetközi együttműködési keretekkel és megállapodásokkal összhangban kell történnie.

Or. en

Módosítás 49
Ville Niinistö
a Verts/ALE képviselőcsoport nevében

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 akadályozhatják a közszolgáltatások	(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 ***és bűnözői*** körök sokféleségére, valószínűleg nem fog 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, alááshatják 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.	nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, alááshatják 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.

Or. en

Indokolás

A haktivizmus bűncselekmények közé való általános belefoglalása nem tükrözi az ilyen tevékenységek sokféleségét, beleértve a jogos tiltakozásokat és a visszaélések bejelentését. A szövegnek jót tenne, ha elkerülné a tisztázatlanságokat és védené a jogszerű tevékenységeket.

Módosítás 50
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi

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	(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 ***– köztük a mikro-, kis- és középvállalkozások (kkv-k)*** **–** és a kritikus infrastruktúrákat működtető szervezetek***, többek között a helyi vagy regionális hatóságok*** növekvő, adott

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.

esetben pusztító társadalmi és gazdasági hatásokkal járó kiberbiztonsági fenyegetésekkel szembeni rezilienciáját. Ezért olyan infrastruktúrákba***, szolgáltatásokba és a szükséges képességekkel rendelkező, magasan képzett személyzetbe*** 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***, többek között proaktív információgyűjtés révén***. Az Uniónak e területeken is meg kell erősítenie képességeit, különösen a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos adatok gyűjtése és elemzése tekintetében. ***[1] https://futureu.europa.eu/hu/***

16

https://futureu.europa.eu/hu/?locale=hu

Or. en

Módosítás 51
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
5 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(5) A növekvő kiberbiztonsági kockázatok és az általánosságban összetett fenyegetettségi helyzet okán – amely egyértelműen azzal a kockázattal jár, hogy a kiberbiztonsági események gyorsan tovagyűrűzhetnek az egyik tagállamból a másikba, illetve valamely harmadik országból az Unióba – a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb	(5) A növekvő kiberbiztonsági kockázatok és az általánosságban összetett fenyegetettségi helyzet okán – amely egyértelműen azzal a kockázattal jár, hogy a kiberbiztonsági események gyorsan tovagyűrűzhetnek az egyik tagállamból a másikba, illetve valamely harmadik országból az Unióba – a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb

felkészülés ***és reagálás*** érdekében meg kell erősíteni az uniós szintű szolidaritást. Az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben[21]a tagállamok felkérték a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.	felkészülés***, reagálás, valamint az azokat követő helyreállítás*** érdekében meg kell erősíteni az uniós szintű szolidaritást. Az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben[21] a tagállamok felkérték a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.
[21] A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról, amelyet a Tanács a 2022. május 23-i ülésén jóváhagyott (9364/22).	[21] A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról, amelyet a Tanács a 2022. május 23-i ülésén jóváhagyott (9364/22).

Or. en

Módosítás 52
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
9 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(9a) A geopolitikai fejlemények és a növekvő kiberfenyegetési helyzet fényében fontos az e rendeletben meghatározott intézkedések – különösen az Európai Kiberpajzs és az európai vészhelyzeti mechanizmus – folytonossága és továbbfejlesztése. Ezért a 2028–2034 közötti időszakra szóló többéves pénzügyi keretben külön költségvetési sort kell biztosítani. A tagállamoknak kötelezettséget kell vállalniuk arra is, hogy támogatnak minden szükséges intézkedést az Unión belüli szolidaritás megerősítése, valamint a kiberbiztonsági fenyegetések és események Unió-szerte történő csökkentése érdekében.

Or. en

Módosítás 53
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
12 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(12) A kiberbiztonsági fenyegetések és események eredményesebb megelőzése ***és*** értékelése, ***valamint*** az azokra való hatékonyabb reagálás érdekében átfogóbb ismereteket kell kialakítani az Unió területén található stratégiai eszközöket és kritikus infrastruktúrákat fenyegető veszélyekről, beleértve azok földrajzi elhelyezkedését, összekapcsoltságát és az ezen infrastruktúrákat érintő kibertámadások lehetséges hatásait is. Ki kell építeni a biztonsági műveleti központok nagyszabású uniós infrastruktúráját (a továbbiakban: Európai Kiberpajzs), amelyet olyan interoperabilitás jellemezte, határokon átnyúló platformok alkotnak, amelyek mindegyike több nemzeti biztonsági műveleti központot tömörít. Ennek a korszerű technológiákra támaszkodó fejlett adatgyűjtési és -elemzési eszközöket használó, a kiberfenyegetések észlelésére és kezelésére irányuló képességeket javító, és valós idejű helyzetismeretet biztosító infrastruktúrának a nemzeti és uniós kiberbiztonsági érdekeket és igényeket kell szolgálnia. Az infrastruktúra a kiberbiztonsági fenyegetések és események fokozott észlelését hivatott előmozdítani, és ezáltal kiegészíteni és támogatni az Unión belüli válságkezelésért felelős uniós szervezeteket és hálózatokat, nevezetesen az (EU) 2022/2555 európai parlamenti és tanácsi irányelvben[24]meghatározott Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (a továbbiakban: EU-CyCLONe).	(12) A kiberbiztonsági fenyegetések és események eredményesebb megelőzése***,*** értékelése, az azokra való hatékonyabb reagálás***, valamint az azokat követő helyreállítás*** érdekében átfogóbb ismereteket kell kialakítani az Unió területén található stratégiai eszközöket és kritikus infrastruktúrákat fenyegető veszélyekről, beleértve azok földrajzi elhelyezkedését, összekapcsoltságát és az ezen infrastruktúrákat érintő kibertámadások lehetséges hatásait is***, többek között proaktív információgyűjtés révén***. Ki kell építeni a biztonsági műveleti központok nagyszabású uniós infrastruktúráját (a továbbiakban: Európai Kiberpajzs), amelyet olyan interoperabilitás jellemezte, határokon átnyúló platformok alkotnak, amelyek mindegyike több nemzeti biztonsági műveleti központot tömörít. ***A nemzeti biztonsági műveleti központ egy központosított kapacitás, amely képes a fenyegetésekkel kapcsolatos hírszerzési információk folyamatos gyűjtésére és a nemzeti joghatóság alá tartozó szervezetek kiberbiztonsági helyzetének javítására a kiberbiztonsági fenyegetések megelőzése, észlelése és elemzése révén.*** Ennek a korszerű technológiákra támaszkodó fejlett adatgyűjtési és -elemzési eszközöket használó, a kiberfenyegetések észlelésére és kezelésére irányuló képességeket javító, és valós idejű helyzetismeretet biztosító infrastruktúrának a nemzeti és uniós kiberbiztonsági érdekeket és igényeket kell szolgálnia. Az infrastruktúra a kiberbiztonsági fenyegetések és események fokozott észlelését hivatott előmozdítani, és ezáltal kiegészíteni és támogatni az Unión belüli válságkezelésért felelős uniós

szervezeteket és hálózatokat, nevezetesen az (EU) 2022/2555 európai parlamenti és tanácsi irányelvben[24] meghatározott Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (a továbbiakban: EU-CyCLONe).

[24] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o.).

[24] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (HL L 333., 2022.12.27., 80. o.).

Or. en

Módosítás 54
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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) ***Az Európai Kiberpajzsban való részvétel érdekében*** minden tagállamnak ki kell jelölnie egy nemzeti szintű közjogi szervet, amelynek feladata ***az adott tagállamban*** a kiberfenyegetés-észlelési ***és információmegosztási*** tevékenységek ***koordinálása. A Bizottság határozottan arra ösztönzi a tagállamokat, hogy építsék be a nemzeti biztonsági műveleti központ kapacitásait a már meglévő kiberstruktúrájukba és -irányításukba, hogy ne hozzanak létre további irányítási szinteket, és hangolják össze a kiberszolidaritásról szóló jogszabályt a már meglévő jogszabályokkal, többek között az (EU) 2022/2555 irányelvvel***. Ezeknek a nemzeti biztonsági műveleti központoknak nemzeti szinten

referenciapontként és átjáróként kell szolgálniuk ***a magán- és állami szervezetek, különösen a biztonsági műveleti központok*** Európai Kiberpajzsban való ***részvételéhez***, és biztosítaniuk kell, hogy az állami és magánszervezetektől származó, kiberfenyegetésekkel kapcsolatos információkat nemzeti szinten hatékonyan és egységesen osszák meg és gyűjtsék össze. ***A nemzeti biztonsági műveleti központoknak meg kell erősíteniük az állami és a magánszervezetek közötti együttműködést és információmegosztást, hogy megszüntethessék a jelenleg létező kommunikációs silókat. Ennek során támogathatják adatcseremodellek létrehozását, valamint meg kell könnyíteniük és ösztönözniük kell az információk megbízható és biztonságos környezetben történő megosztását. Az állami és magánszervezetek közötti szoros és összehangolt együttműködés központi szerepet játszik az Unió kiberbiztonsági rezilienciájának megerősítésében.***

Or. en

Módosítás 55
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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.

általános célkitűzése a kiberbiztonsági fenyegetések elemzésére, megelőzésére és észlelésére szolgáló kapacitások megerősítése, valamint a magas színvonalú ***és proaktív*** 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 határokon átnyúló biztonsági műveleti központoknak meg kell könnyíteniük és ösztönözniük kell az információk megbízható és biztonságos környezetben történő megosztását. Az ENISA-nak támogatnia kell a határokon átnyúló biztonsági műveleti központokat az operatív együttműködéshez kapcsolódó kérdésekben***. 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.

Or. en

Módosítás 56
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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***.

keretében folytatnak információcserét. A határokon átnyúló biztonsági műveleti központoknak olyan új ***kapacitást*** kell kialakítaniuk, amely oly módon ***épül be a már létező kiberbiztonsági infrastruktúrába, különösen*** a CSIRT-ek ***hálózatába***, hogy összegyűjti és megosztja az állami és magánszervezetektől***, különösen azok biztonsági műveleti központjaiból*** származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatokat, majd szakértői elemzések, közösen beszerzett infrastruktúrák és a legkorszerűbb eszközök révén növeli az ilyen adatok értékét, valamint ***az Unió rezilienciájának megerősítése érdekében*** hozzájárul az uniós képességek és technológiai ***szuverenitás fejlődéséhez***.

Or. en

Módosítás 57
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	(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***.	eszközök révén növeli az ilyen adatok értékét, valamint hozzájárul az ***erős*** uniós ***képességekkel rendelkező jelentős kiberbiztonsági ökoszisztéma kialakításához és a hasonlóan gondolkodó partnerekkel való együttműködéshez***.

Or. en

Módosítás 58
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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.	(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) ***közötti*** széles körű terjesztését ***a jelenleg létező kommunikációs silók megszüntetésének megkönnyítése érdekében. Ennek során a határokon átnyúló biztonsági műveleti központok támogathatnák adatcsere-modellek létrehozását az egész Unióban***. A határokon átnyúló biztonsági műveleti központok résztvevői közötti információcsere kiterjedhet a hálózatokból és érzékelőkből származó adatokra, a kiberfenyegetettségi információk hírcsatornáira ***– többek között a proaktív információgyűjtésre –***, 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.

Or. en

Módosítás 59
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 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.	(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 információcsere kiterjedhet a hálózatokból***, érzékelőkből, naplózásból és telemetriából*** származó ***elemzett*** adatokra, a kiberfenyegetettségi információk hírcsatornáira, a fertőzöttségi mutatókra, valamint a ***taktikákra, technikákra és eljárásokra, a*** kiberbiztonsági eseményekre, ***a rosszindulatú szoftverek mintáira, a*** fenyegetésekre és ***a*** sebezhetőségekre vonatkozó, kontextusba helyezett információkra. Emellett a határokon átnyúló biztonsági műveleti központoknak együttműködési megállapodásokat kell kötniük más határokon átnyúló biztonsági műveleti központokkal is.

Or. en

Módosítás 60
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 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	(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***, összhangban az (EU) 2022/2555 irányelv szerinti, már létező rendelkezésekre***. 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.

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.

Or. en

Módosítás 61
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 legkorszerűbb mesterségesintelligencia- és adatelemzési technológiák alkalmazásával.	(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***, valamint magasan képzett személyzettel kell ellátni***. Ez várhatóan lehetővé teszi a közös észlelési képességek javítását és a hatóságok és az érintett szervezetek időben történő figyelmeztetését, különösen a legkorszerűbb mesterségesintelligencia- és adatelemzési technológiák alkalmazásával.

Or. en

Módosítás 62
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş

Bogdan

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 technológiai szuverenitását. A kiváló minőségű gondozott adatok összevonása minden bizonnyal hozzájárul a fejlett mesterségesintelligencia- és adatelemzési technológiák fejlesztéséhez is. ***Meg kell azonban jegyezni, hogy a mesterséges intelligencia akkor a leghatékonyabb, ha emberi elemzéssel párosítják. Ezért a magasan képzett személyzet továbbra is elengedhetetlen a magas színvonalú adatok összegyűjtéséhez és a fenyegetésekkel kapcsolatos proaktív információgyűjtéshez.*** 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.).

Or. en

Módosítás 63
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***jelentős kiberbiztonsági ökoszisztémáját***. 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.).

Or. en

Módosítás 64
Ville Niinistö
a Verts/ALE képviselőcsoport nevében

Rendeletre irányuló javaslat
21 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(21) Jóllehet az Európai Kiberpajzs polgári projekt, a kibervédelmi közösség számára is előnyt jelenthetnek a kritikus infrastruktúrák védelmére kifejlesztett, erősebb polgári észlelési és helyzetismereti képességek. A határokon átnyúló biztonsági műveleti központoknak a Bizottság és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) támogatásával, valamint az Unió	(21) Jóllehet az Európai Kiberpajzs polgári projekt, a kibervédelmi közösség számára is előnyt jelenthetnek a kritikus infrastruktúrák védelmére kifejlesztett, erősebb polgári észlelési és helyzetismereti képességek. A határokon átnyúló biztonsági műveleti központoknak a Bizottság és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) támogatásával, valamint az Unió

külügyi és biztonságpolitikai főképviselőjének (a továbbiakban: főképviselő) közreműködésével a kibervédelmi közösséggel való együttműködés érdekében célzott protokollokat és szabványokat kell fokozatosan kidolgozniuk, ***beleértve az ellenőrzési és biztonsági feltételeket is***. Az Európai Kiberpajzsnak a főképviselővel szoros együttműködésben folytatott fejlesztését olyan szemléletnek kell kísérnie, amely lehetővé teszi a kibervédelmi közösségen belüli információmegosztásért felelős hálózatokkal és platformokkal való együttműködést.	külügyi és biztonságpolitikai főképviselőjének (a továbbiakban: főképviselő) közreműködésével a kibervédelmi közösséggel való együttműködés érdekében célzott ***hozzáférési feltételeket, biztosítékokat,*** protokollokat és szabványokat **–** ***többek között ellenőrzési és biztonsági feltételeket*** **–** kell fokozatosan kidolgozniuk, ***tiszteletben tartva a kezdeményezések polgári jellegét és a finanszírozás rendeltetését, ezáltal felhasználva a védelmi közösség rendelkezésére álló forrásokat***. Az Európai Kiberpajzsnak a főképviselővel szoros együttműködésben ***és a jogok és szabadságok teljes körű tiszteletben tartása mellett*** folytatott fejlesztését olyan szemléletnek kell kísérnie, amely lehetővé teszi a kibervédelmi közösségen belüli információmegosztásért felelős hálózatokkal és platformokkal való együttműködést.

Or. en

Indokolás

A párhuzamosságok elkerülése, valamint a jogok és szabadságok védelmének szellemében a kiberbiztonság polgári és védelmi oldala közötti együttműködésnek biztosítékokon kell alapulnia, elkerülve a polgári finanszírozás rendeltetésének megváltoztatását.

Módosítás 65
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
24 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(24) Tekintettel arra, hogy a tagállamokat érintő kiberbiztonsági események egyre nagyobb kockázatot jelentenek és egyre gyakoribbak, létre kell hozni egy válsághelyzetek kezelését célzó támogatási eszközt, amely javítja az Unió jelentős és nagyszabású kiberbiztonsági	(24) Tekintettel arra, hogy a tagállamokat érintő kiberbiztonsági események egyre nagyobb kockázatot jelentenek és egyre gyakoribbak, létre kell hozni egy válsághelyzetek kezelését célzó támogatási eszközt, amely javítja az Unió jelentős és nagyszabású kiberbiztonsági

eseményekkel szembeni rezilienciáját, és a felkészültséghez, a reagáláshoz és az alapvető szolgáltatások azonnali helyreállításához nyújtott vészhelyzeti pénzügyi támogatás révén kiegészíti a tagállamok intézkedéseit. Ennek az eszköznek lehetővé kell tennie a meghatározott körülmények közötti és egyértelmű feltételek melletti gyors segítségnyújtást, valamint a források felhasználásának részletes nyomon követését és értékelését. Míg a kiberbiztonsági események és válsághelyzetek megelőzése, valamint az azokra való felkészülés és reagálás elsősorban a tagállamok feladata, a kiberbiztonsági vészhelyzeti mechanizmus az Európai Unióról szóló szerződés (a továbbiakban: EUSZ) 3. cikkének (3) bekezdésével összhangban előmozdítja a tagállamok közötti szolidaritást.	eseményekkel szembeni rezilienciáját, és a felkészültséghez, a reagáláshoz és az alapvető szolgáltatások azonnali helyreállításához nyújtott vészhelyzeti pénzügyi támogatás révén kiegészíti a tagállamok intézkedéseit. Ennek az eszköznek lehetővé kell tennie a meghatározott körülmények közötti és egyértelmű feltételek melletti gyors ***és tényleges*** segítségnyújtást, valamint a források felhasználásának részletes nyomon követését és értékelését. Míg a kiberbiztonsági események és válsághelyzetek megelőzése, valamint az azokra való felkészülés és reagálás elsősorban a tagállamok feladata, a kiberbiztonsági vészhelyzeti mechanizmus az Európai Unióról szóló szerződés (a továbbiakban: EUSZ) 3. cikkének (3) bekezdésével összhangban előmozdítja a tagállamok közötti szolidaritást.

Or. en

Módosítás 66
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
27 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(27) Az e rendelet alapján biztosított segítségnyújtásnak támogatnia kell a tagállamok által nemzeti szinten hozott intézkedéseket, és ki kell egészítenie azokat. E célból biztosítani kell a Bizottság és az érintett tagállam közötti szoros együttműködést és konzultációt. Amikor valamely tagállam támogatást kér a kiberbiztonsági vészhelyzeti mechanizmus keretében, meg kell adnia a támogatás iránti igényét alátámasztó releváns információkat.	(27) Az e rendelet alapján biztosított segítségnyújtásnak támogatnia kell a tagállamok által nemzeti szinten hozott intézkedéseket, és ki kell egészítenie azokat. E célból biztosítani kell a Bizottság***, az ENISA*** és az érintett tagállam közötti szoros együttműködést és konzultációt. Amikor valamely tagállam támogatást kér a kiberbiztonsági vészhelyzeti mechanizmus keretében, meg kell adnia a támogatás iránti igényét alátámasztó releváns információkat.

Or. en

Módosítás 67
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, ugyanakkor meg kell erősíteni az Unió rezilienciáját és versenyképességét, beleértve a kkv-nak minősülő, európai irányítású biztonsági szolgáltatók részvételét is. A megbízható szolgáltatók, köztük a kkv-k számára lehetővé kell tenni, hogy a fenti kritériumok teljesítése érdekében együttműködjenek egymással***. 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***. A szolgáltatásoknak lehetőség szerint a legkorszerűbb technológiákon kell alapulniuk, beleértve a felhőalapú technológiákat és a mesterséges intelligenciát is. Ezért a kiberbiztonsági tartalék keretében ösztönözni kell a kutatásba és innovációba történő beruházásokat e technológiák fejlesztésének fellendítése érdekében. Szükség esetén a megbízható szolgáltatókkal és a kiberbiztonsági tartalék potenciális felhasználóival közös gyakorlatokat lehet végezni a tartalék***

hatékony működésének biztosítása érdekében. 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.

Or. en

Módosítás 68
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	(33) Fokozatosan létre kell hozni egy uniós szintű kiberbiztonsági tartalékot, ***amelynek kezdeti finanszírozása e rendelet keretében az értékelésig 10 millió euró. A kiberbiztonsági tartalék*** 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

kiberbiztonsági tartalék szolgáltatásai hasonló feltételek mellett az uniós intézményeknek, szerveknek és ügynökségeknek is támogatást nyújthatnak.	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. ***A Bizottság biztosítja, hogy ne alakuljon ki átfedés a NATO-n belüli hasonló kezdeményezésekkel.***

Or. en

Indokolás

The Commission foresees a "gradual set up" of the Reserve but this is not reflected in the rest of the proposed Regulation. This amendment therefore proposes to reduce the initial budget for the Reserve from 36 million to 10 million euro until the evaluation of this Regulation. This would return 26 million euro to the Digital Europe Program - Special Objective 4 on Advanced Digital Skills (of the 35 million taken from it). Developing a EU Cybersecurity Reserve next to an existing NATO cyber reserve comes with a high risk of duplication and should not be at the expense of investing more in developing and attracting cybersecurity talent in Europe.

Módosítás 69
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
35 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(35) Az uniós kiberbiztonsági tartalék létrehozásának előmozdítása érdekében a ***Bizottság fontolóra vehetné, hogy felkérje*** az ENISA-t, hogy az (EU) 2019/881 rendelet alapján dolgozzon ki egy javasolt tanúsítási rendszert a kiberbiztonsági vészhelyzeti mechanizmus hatálya alá tartozó területeken nyújtott irányított biztonsági szolgáltatásokra vonatkozóan.	(35) Az uniós kiberbiztonsági tartalék létrehozásának előmozdítása érdekében a ***Bizottságnak fel kell kérnie*** az ENISA-t, hogy az (EU) 2019/881 rendelet alapján dolgozzon ki egy javasolt tanúsítási rendszert a kiberbiztonsági vészhelyzeti mechanizmus hatálya alá tartozó területeken nyújtott irányított biztonsági szolgáltatásokra vonatkozóan.

Or. en

Módosítás 70

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Rendeletre irányuló javaslat
35 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(35a) Az e rendeletben és [a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló javaslatban] előírt további feladatok fényében az ENISA számára biztosítani kell a szükséges emberi és pénzügyi erőforrásokat az uniós költségvetésből.

Or. en

Módosítás 71
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
37 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(37a) Szükség lehet harmadik országok – többek között a Digitális Európa programhoz társult harmadik országok, NATO-tagok vagy más hasonló gondolkodású nemzetközi partnerországok – biztonsági eseményekre való reagálással foglalkozó szolgáltatóira az uniós kiberbiztonsági tartalék keretében nyújtott konkrét szolgáltatásokhoz. Az Unió rezilienciájának és szuverenitásának megerősítése, valamint az Unió stratégiai eszközeinek, érdekeinek vagy biztonságának védelme érdekében szükség lehet a nem társult országokban letelepedett vagy nem társult országok által ellenőrzött jogalanyok részvételének korlátozására vagy kizárására.

Or. en

Módosítás 72
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
38 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(38a) Az európai kiberbiztonsági pajzs és a kiberbiztonsági vészhelyzeti mechanizmus hatékony végrehajtásához elengedhetetlen a magasan képzett személyzet, amely képes megbízhatóan, a legmagasabb normáknak megfelelően nyújtani releváns kiberbiztonsági szolgáltatásokat. Ezért aggályos, hogy az Unió tehetséghiánnyal szembesül, amelyet a képzett szakemberek hiánya jellemez, miközben gyorsan változó fenyegetettségi helyzettel néz szembe, amint azt a Kiberkészségek Akadémiájáról szóló, 2023. április 18-i bizottsági közlemény is elismeri. Fontos áthidalni ezt a szakemberhiányt a különböző érdekelt felek – többek között a magánszektor, a tudományos körök, a tagállamok, a Bizottság és az ENISA – közötti együttműködés és koordináció erősítésével az oktatásba és képzésbe való beruházás, a köz- és magánszféra közötti partnerségek fejlesztése, a kutatási és innovációs kezdeményezések támogatása, a közös szabványok kidolgozása és kölcsönös elismerése, valamint a kiberbiztonsági készségek tanúsítása terén, többek között a kiberbiztonsági készségek európai keretrendszerén keresztül. Ez várhatóan megkönnyíti a kiberbiztonsági szakemberek Unión belüli mobilitását is. E rendeletnek a sokszínűbb kiberbiztonsági munkaerő előmozdítására kell irányulnia.

Or. en

Módosítás 73
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
38 b preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(38b) A tagállamok kapacitásépítése elengedhetetlen az uniós kiberbiztonsági helyzet rezilienciájának megerősítésére irányuló, az egész Unióra kiterjedő összehangolt megközelítéshez. Amint azt a Kiberkészségek Akadémiájáról szóló, 2023. április 18-i bizottsági közlemény is hangsúlyozza, az Unió biztonsága nem garantálható az Unió legértékesebb eszköze, vagyis a népe nélkül. A kiberbiztonsági készségek európai keretrendszere segíthet az uniós munkaerő összetételének jobb megértésében, beleértve a részt vevő szervezeteken belüli jelenlegi és szükséges kompetenciákat is.

Or. en

Módosítás 74
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
39 preambulumbekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(39) E rendelet célkitűzése jobban megvalósítható uniós szinten, mint tagállami szinten. Az Unió ezért intézkedéseket fogadhat el az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritási és arányossági elvnek megfelelően. Ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket,	(39) E rendelet célkitűzése***, nevezetesen a kommunikációs silók lebontása és az Unió kiberfenyegetés-megelőzési, -észlelési, -reagálási és helyreállítási kapacitásainak megerősítése*** jobban megvalósítható uniós szinten, mint tagállami szinten. Az Unió ezért intézkedéseket fogadhat el az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritási és arányossági elvnek megfelelően. Ez a rendelet nem lépi túl az

e cél eléréséhez szükséges mértéket,

Or. en

Módosítás 75
Nicola Danti

Rendeletre irányuló javaslat
39 a preambulumbekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(39a) Az e rendeletben és [a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló javaslatban] előírt további feladatok fényében az ENISA számára biztosítani kell a szükséges emberi és pénzügyi erőforrásokat az uniós költségvetésből.

Or. en

Módosítás 76
Johan Nissinen

Rendeletre irányuló javaslat
1 cikk – 1 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(1) Ez a rendelet intézkedéseket állapít meg a kiberbiztonsági fenyegetések és események észlelésére, valamint az azokra való felkészülésre és reagálásra irányuló uniós ***képességek*** megerősítésére, különösen a következő intézkedések révén:	(1) Ez a rendelet intézkedéseket állapít meg a kiberbiztonsági fenyegetések és események észlelésére, valamint az azokra való felkészülésre és reagálásra irányuló uniós ***kapacitások*** megerősítésére***, tiszteletben tartva ugyanakkor, hogy a nemzetbiztonság – többek között a kibertérben is – továbbra is az egyes tagállamok kizárólagos felelőssége marad, amint azt az EUSZ 4. cikkének (2) bekezdése megállapítja***, különösen a következő intézkedések révén:

Or. en

Módosítás 77
Evžen Tošenovský

Rendeletre irányuló javaslat
1 cikk – 1 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) ***a biztonsági műveleti központok páneurópai infrastruktúrájának kiépítése (Európai Kiberpajzs*****)*** ***a*** közös észlelési és helyzetismereti képességek ***kialakítása és fejlesztése*** érdekében;	a) ***az (EU) 2022/2555 irányelv 10. cikkében említett számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) és az (EU*****)*** ***2022/2555 irányelv 15. cikkében említett CSIRT-hálózat megerősítése, valamint biztonsági műveleti központok (SOC-ok) telepítése a nemzeti és*** közös észlelési és helyzetismereti képességek ***kiépítése és javítása*** érdekében ***(a továbbiakban: Európai Kiberpajzs)***;

Or. en

Módosítás 78
Evžen Tošenovský

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.	***törölve***

Or. en

Módosítás 79
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, köztük a kkv-k*** versenyhelyzetének megerősítését a digitális gazdaság egészében, valamint hozzájárulás az Unió technológiai szuverenitásához a kiberbiztonság területén;

Or. en

Módosítás 80
Johan Nissinen

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 ***önkéntes*** 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;

Or. en

Módosítás 81
Johan Nissinen

Rendeletre irányuló javaslat
1 cikk – 2 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) a kritikus és a kiemelten kritikus	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;	ágazatokban működő szervezetek felkészültségének megerősítése Unió-szerte, valamint ***az önkéntes együttműködés*** 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;

Or. en

Módosítás 82
Evžen Tošenovský

Rendeletre irányuló javaslat
1 cikk – 2 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) az Unió rezilienciájának fokozása és a hatékony reagáláshoz való hozzájárulás a jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése révén, beleértve a levont tanulságokat és adott esetben az ajánlásokat is.	***törölve***

Or. en

Módosítás 83
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

A Bizottság által javasolt szöveg	*Módosítás*
	ca) a kiberbiztonsági ágazatban dolgozó munkaerő készségeinek és kompetenciáinak koordinált módon történő fejlesztése és javítása a Kiberkészségek Akadémiájával való

együttműködés révén, hogy képzést és lehetőségeket biztosítsanak a kiberbiztonsági ágazatban tapasztalható szakemberhiány megszüntetése céljából.

Or. en

Módosítás 84
Johan Nissinen

Rendeletre irányuló javaslat
1 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) E rendelet nem érinti a tagállamoknak a nemzetbiztonsággal, a közbiztonsággal, valamint a bűncselekmények megelőzésével, kivizsgálásával, felderítésével és büntetőeljárás alá vonásával kapcsolatos elsődleges felelősségét.	(3) E rendelet nem érinti a tagállamoknak a nemzetbiztonsággal, a közbiztonsággal, valamint a bűncselekmények megelőzésével, kivizsgálásával, felderítésével és büntetőeljárás alá vonásával kapcsolatos elsődleges felelősségét***, és elkerüli a meglévő kezdeményezésekkel való szükségtelen átfedéseket***.

Or. en

Módosítás 85
Evžen Tošenovský

Rendeletre irányuló javaslat
1 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) E rendelet nem érinti a tagállamoknak a ***nemzetbiztonsággal, a közbiztonsággal***, valamint a bűncselekmények ***megelőzésével, kivizsgálásával, felderítésével*** és büntetőeljárás alá ***vonásával kapcsolatos elsődleges felelősségét***.	(3) E rendelet nem érinti a tagállamoknak a ***nemzetbiztonság, a közbiztonság***, valamint a bűncselekmények ***megelőzése, kivizsgálása, felderítése*** és büntetőeljárás alá ***vonása területén való kizárólagos hatáskörét***.

Or. en

Módosítás 86
Nicola Danti

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

A Bizottság által javasolt szöveg	*Módosítás*
	(3a) A Bizottság minden évben, a következő évre vonatkozó költségvetési tervezet előterjesztésekor részletes értékelést nyújt be az ENISA e rendelet szerinti, valamint [a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló javaslatban] és más uniós jogszabályokban meghatározott feladatairól, és részletesen felsorolja az e feladatok ellátásához szükséges pénzügyi és emberi erőforrásokat.

Or. en

Módosítás 87
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 1 pont

A Bizottság által javasolt szöveg	*Módosítás*
1. „határokon átnyúló biztonsági műveleti központ” (a továbbiakban: határokon átnyúló SOC): több országra kiterjedő platform, amely összehangolt hálózati struktúrában egyesíti legalább három tagállam üzemeltetési konzorciumot alkotó nemzeti biztonsági műveleti központjait, és amelynek célja a kiberbiztonsági fenyegetések és események megelőzése, valamint a magas színvonalú információk előállításának támogatása, elsősorban a különböző – köz- vagy magánforrásokból származó – adatok cseréje, a legkorszerűbb eszközök megosztása, valamint az észlelési, elemzési, megelőzési és védelmi képességek megbízható környezetben	***törölve***

történő közös fejlesztése révén;

Or. en

Módosítás 88
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 1 pont

A Bizottság által javasolt szöveg	*Módosítás*
1. „határokon átnyúló biztonsági műveleti központ” (a továbbiakban: határokon átnyúló SOC): több országra kiterjedő platform, amely összehangolt hálózati struktúrában egyesíti legalább három tagállam üzemeltetési konzorciumot alkotó nemzeti biztonsági műveleti központjait, és amelynek célja a kiberbiztonsági fenyegetések ***és*** események megelőzése, valamint a magas színvonalú információk előállításának támogatása, elsősorban a különböző – köz- vagy magánforrásokból származó – adatok cseréje, a legkorszerűbb eszközök megosztása, valamint az észlelési, elemzési, megelőzési és védelmi képességek megbízható környezetben történő közös fejlesztése révén;	1. „határokon átnyúló biztonsági műveleti központ” (a továbbiakban: határokon átnyúló SOC): több országra kiterjedő platform, amely összehangolt hálózati struktúrában egyesíti legalább három tagállam üzemeltetési konzorciumot alkotó nemzeti biztonsági műveleti központjait, és amelynek célja a kiberbiztonsági fenyegetések ***észlelése és elemzése és a kiberbiztonsági*** események megelőzése, valamint a magas színvonalú információk előállításának támogatása, elsősorban a különböző – köz- vagy magánforrásokból származó – adatok cseréje, a legkorszerűbb eszközök megosztása, valamint az észlelési, elemzési, megelőzési és védelmi képességek megbízható környezetben történő közös fejlesztése révén;

Or. en

Módosítás 89
Johan Nissinen

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 1 pont

A Bizottság által javasolt szöveg	*Módosítás*
1. „határokon átnyúló biztonsági műveleti központ” (a továbbiakban: határokon átnyúló SOC): több országra kiterjedő platform, amely összehangolt	1. „határokon átnyúló biztonsági műveleti központ” (a továbbiakban: határokon átnyúló SOC): több országra kiterjedő platform, amely összehangolt

hálózati struktúrában egyesíti legalább három tagállam üzemeltetési konzorciumot alkotó nemzeti biztonsági műveleti központjait, és amelynek célja a kiberbiztonsági fenyegetések és események megelőzése, valamint a magas színvonalú információk előállításának támogatása, elsősorban a különböző – köz- vagy magánforrásokból származó – adatok cseréje, a legkorszerűbb eszközök megosztása, valamint az észlelési, elemzési, megelőzési és védelmi képességek megbízható környezetben történő közös fejlesztése révén;	hálózati struktúrában egyesíti legalább három tagállam üzemeltetési konzorciumot alkotó nemzeti biztonsági műveleti központjait, és amelynek célja a kiberbiztonsági fenyegetések és események megelőzése, valamint a magas színvonalú információk előállításának támogatása, elsősorban a különböző – köz- vagy magánforrásokból származó – adatok ***önkéntes*** cseréje, a legkorszerűbb eszközök megosztása, valamint az észlelési, elemzési, megelőzési és védelmi képességek megbízható környezetben történő közös fejlesztése révén;

Or. en

Módosítás 90
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

A Bizottság által javasolt szöveg	*Módosítás*
	1a. „biztonsági műveleti központ”: egy szervezet kiberbiztonsági helyzetének folyamatos nyomon követéséért és javításáért felelős, házon belüli vagy kiszervezett központi kapacitás a kiberbiztonsági fenyegetések megelőzése, észlelése, elemzése és az azokra való reagálás érdekében.

Or. en

Módosítás 91
Evžen Tošenovský

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

A Bizottság által javasolt szöveg	*Módosítás*
	1a. „biztonsági műveleti központ”:

magán- és állami szervek vagy nemzeti hatóságok által létrehozott központ, amely folyamatosan figyelemmel kíséri és elemzi a kommunikációs hálózatokat és a számítógépes rendszereket a behatolások és rendellenességek valós idejű észlelése céljából.

Or. en

Módosítás 92
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

A Bizottság által javasolt szöveg	*Módosítás*
	1b. „nemzeti biztonsági műveleti központ”: olyan központosított kapacitás, amely a fenyegetésekkel kapcsolatos információk folyamatos összegyűjtéséért és a nemzeti joghatóság alá tartozó szervezetek kiberbiztonsági helyzetének javításáért felel a kiberbiztonsági fenyegetések megelőzése, észlelése és elemzése révén, hogy hatékonyabban tudjon reagálni a kiberbiztonsági fenyegetésekre. Ezt a kapacitást adott esetben be kell építeni a már meglévő nemzeti struktúrákba, például az (EU) 2022/2555 irányelv alapján létrehozott CSIRT-ekbe.

Or. en

Módosítás 93
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 2 pont

A Bizottság által javasolt szöveg	*Módosítás*
2. „***közjogi*** szerv”: ***a 2014/24/EU***	2. „***közigazgatási*** szerv”: ***az (EU)***

európai parlamenti és tanácsi irányelv[30] ***2. cikke (1) bekezdésének 4***. pontjában meghatározott ***közjogi intézmény***;	***2022/2555*** irányelv ***6. cikkének 35***. pontjában meghatározott ***közigazgatási szerv***;

[30] Az Európai Parlament és a Tanács 2014/24/EU irányelve (2014. február 26.) a közbeszerzésről és a 2004/18/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 65. o.).

Or. en

Módosítás 94
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 3 pont

A Bizottság által javasolt szöveg	*Módosítás*
3. „üzemeltetési konzorcium”: konzorcium, amelyet a nemzeti biztonsági műveleti központok által képviselt részt vevő államok alkotnak, amelyek megegyeztek arról, hogy a határokon átnyúló biztonsági műveleti központok számára és azok üzemeltetése érdekében eszközöket és infrastruktúrát hoznak létre, valamint hozzájárulnak az ilyen eszközök és infrastruktúra beszerzéséhez;	***törölve***

Or. en

Módosítás 95
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 5 a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	5a. „eseménykezelés”: az (EU) 2022/2555 irányelv 6. cikkének 8. pontjában meghatározott eseménykezelés;

Or. en

Módosítás 96
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 5 b pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	5b. „kockázat”: az (EU) 2022/2555 rendelet 6. cikkének 9. pontjában meghatározott kockázat;

Or. en

Módosítás 97
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 6 a pont (új)

A Bizottság által javasolt szöveg	*Módosítás*
	6a. „jelentős kiberfenyegetés”: az (EU) 2022/2555 irányelv 6. cikkének 11. pontjában meghatározott jelentős kiberfenyegetés;

Or. en

Módosítás 98
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 9 pont

A Bizottság által javasolt szöveg	*Módosítás*
9. „felkészültség”: egy jelentős vagy nagyszabású kiberbiztonsági eseményre való hatékony és gyors reagálást biztosító, előre meghozott kockázatértékelési és nyomonkövetési intézkedések eredményeként kialakult készenlét és	***törölve***

képesség;

Or. en

Módosítás 99
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 10 pont

A Bizottság által javasolt szöveg	*Módosítás*
10. „reagálás”: jelentős vagy nagyszabású kiberbiztonsági esemény alkalmával, illetve ilyen esemény során vagy után hozott intézkedés az esemény azonnali és rövid távú káros következményeinek kezelése érdekében;	***törölve***

Or. en

Módosítás 100
Evžen Tošenovský

Rendeletre irányuló javaslat
2 cikk – 1 bekezdés – 11 pont

A Bizottság által javasolt szöveg	*Módosítás*
11. „megbízható ***szolgáltatók***”: az (EU) 2022/2555 irányelv 6. cikkének 40. pontjában meghatározott, e rendelet 16. cikkével összhangban kiválasztott irányított biztonsági szolgáltatók.	11. „megbízható ***irányított biztonsági szolgáltatásokat nyújtó szolgáltató***”: az (EU) 2022/2555 irányelv 6. cikkének 40. pontjában meghatározott, e rendelet 16. cikkével összhangban ***az uniós kiberbiztonsági tartalékba*** kiválasztott irányított biztonsági ***szolgáltatásokat nyújtó*** szolgáltatók.

Or. en

Módosítás 101
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat

3 cikk – 1 bekezdés – 1 albekezdés

A Bizottság által javasolt szöveg	*Módosítás*
Létre kell hozni a biztonsági műveleti központok egymással összekapcsolt páneurópai infrastruktúráját (a továbbiakban: Európai Kiberpajzs) annak érdekében, hogy az Unió fejlett képességeket alakítson ki az Unión belüli kiberbiztonsági fenyegetések ***és események*** észlelése, elemzése és a vonatkozó adatok feldolgozása érdekében. A pajzsot az összes nemzeti biztonsági műveleti központ (a továbbiakban: nemzeti SOC) és határokon átnyúló biztonsági műveleti központ (a továbbiakban: határokon átnyúló SOC) alkotja.	Létre kell hozni a biztonsági műveleti központok egymással összekapcsolt páneurópai infrastruktúráját (a továbbiakban:Európai Kiberpajzs) annak érdekében, hogy az Unió fejlett képességeket alakítson ki az Unión belüli kiberbiztonsági fenyegetések észlelése, elemzése és a vonatkozó adatok feldolgozása***, valamint a kiberbiztonsági események megelőzése*** érdekében. A pajzsot az összes nemzeti biztonsági műveleti központ (a továbbiakban:nemzeti SOC) és határokon átnyúló biztonsági műveleti központ (a továbbiakban:határokon átnyúló SOC) alkotja.

Or. en

Módosítás 102
Johan Nissinen

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) a határokon átnyúló biztonsági műveleti központok révén összegyűjti és megosztja a különböző forrásokból származó, kiberbiztonsági fenyegetésekre és eseményekre vonatkozó adatokat;	a) a határokon átnyúló biztonsági műveleti központok ***önkéntes információmegosztása*** révén összegyűjti és megosztja a különböző forrásokból származó, kiberbiztonsági fenyegetésekre és eseményekre vonatkozó adatokat;

Or. en

Módosítás 103
Evžen Tošenovský

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) a határokon átnyúló biztonsági műveleti központok révén összegyűjti és megosztja a különböző forrásokból származó, kiberbiztonsági fenyegetésekre és eseményekre vonatkozó adatokat;	a) a határokon átnyúló biztonsági műveleti központok révén összegyűjti és megosztja a különböző forrásokból származó, kiberbiztonsági fenyegetésekre és eseményekre vonatkozó adatokat ***nemzeti és uniós szinten egyaránt***;

Or. en

Módosítás 104
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) hozzájárul a fokozott védelemhez és a kiberfenyegetésekre való hatékonyabb reagáláshoz;	c) hozzájárul a fokozott védelemhez és a kiberfenyegetésekre való hatékonyabb reagáláshoz***, többek között azáltal, hogy konkrét ajánlásokat fogalmaz meg a szervezetek számára***;

Or. en

Módosítás 105
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – d pont

A Bizottság által javasolt szöveg	*Módosítás*
d) Unió-szerte hozzájárul a kiberfenyegetések gyorsabb észleléséhez és a helyzetismerethez;	d) Unió-szerte hozzájárul a kiberfenyegetések gyorsabb észleléséhez és a helyzetismerethez***, többek között proaktív információgyűjtés révén***;

Or. en

Módosítás 106
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
3 cikk – 2 bekezdés – 1 albekezdés – e pont

A Bizottság által javasolt szöveg	*Módosítás*
e) szolgáltatásokat és tevékenységeket nyújt az Unió kiberbiztonsági közössége számára, többek között hozzájárul a fejlett mesterséges intelligenciát és adatelemzést szolgáló eszközök fejlesztéséhez.	(A magyar változatot nem érinti.)

Or. en

Módosítás 107
Evžen Tošenovský

Rendeletre irányuló javaslat
4 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Nemzeti biztonsági műveleti központok	***Megerősített együttműködés és információmegosztás nemzeti szinten***

Or. en

Módosítás 108
Evžen Tošenovský

Rendeletre irányuló javaslat
4 cikk – 1 bekezdés – 1 albekezdés

A Bizottság által javasolt szöveg	*Módosítás*
Az Európai ***Kiberpajzsban való részvétel*** érdekében minden ***tagállamnak ki kell jelölnie legalább egy nemzeti biztonsági műveleti központot. A nemzeti biztonsági műveleti központ közjogi szerv***.	Az európai ***kiberbiztonsági pajzshoz való hozzájárulás*** érdekében minden ***tagállam kijelöli az (EU) 2022/2555 irányelv 10. cikkében említett számítógép-biztonsági eseményekre reagáló csoportját (CSIRT) mint információmegosztási és -elemző központot (ISAC)***.

Or. en

Módosítás 109
Evžen Tošenovský

Rendeletre irányuló javaslat
4 cikk – 1 bekezdés – 1 a albekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	A magán- és állami szervezeteket vagy a nemzeti hatóságokat, különösen a kritikus vagy kiemelten kritikus ágazatokban működő szervezeteket ösztönözni kell arra, hogy önálló vagy közös biztonsági műveleti központot hozzanak létre vagy működtessenek.

Or. en

Módosítás 110
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 magánszervezetek számára a kiberbiztonsági fenyegetésekre 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. ***A biztonsági műveleti központ vagy a nemzeti CSIRT a 2022/2555-ben meghatározott, kiemelten kritikus ágazatokra vonatkozó telemetriai, szenzor- vagy naplózási adatokat kérhet a megbízható szolgáltatóktól vagy az irányított biztonsági szolgáltatásokat nyújtó szolgáltatóktól. Ezek az adatok***

	csak a nemzeti biztonsági műveleti központ vagy CSIRT kiberbiztonsági események észlelésével és megelőzésével kapcsolatos feladatainak és felelősségi köreinek támogatása érdekében oszthatók meg.

Or. en

Módosítás 111
Evžen Tošenovský

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 ***elsősorban a magán- és állami szervezetek vagy nemzeti hatóságok, ugyanazon tagállam más CSIRT-jei, a nagyszabású kiberbiztonsági események és válságok kezelésének koordinátora, valamint más nemzeti szintű köz-*** és magánszervezetek számára a kiberbiztonsági fenyegetésekre és eseményekre vonatkozó információk gyűjtése és elemzése, valamint ***adott esetben ezen információknak a CSIRT-hálózat más tagjaival való megosztása céljából***. Fel kell szerelni a kiberbiztonsági fenyegetések és események észlelésére, valamint a kapcsolódó adatok összesítésére és elemzésére alkalmas legkorszerűbb technológiákkal.

Or. en

Módosítás 112
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 magánszervezetek***, különösen azok biztonsági műveleti központjai*** 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.

Or. en

Módosítás 113
Evžen Tošenovský

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 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	***törölve***

előtt az ECCC és a nemzeti biztonsági műveleti központ az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

Or. en

Módosítás 114
Ville Niinistö
a Verts/ALE képviselőcsoport nevében

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 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.	(2) Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) részvételi szándék kifejezésére való felhívás nyomán ***választhatja*** 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 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.

Or. en

Indokolás

A „választja” kötelező jellege megfosztja a tartalmat a részvételi szándék kifejezésére való felhívás és a kiválasztási eljárások fogalmától. A biztonsági műveleti központok természetesen

részt vehetnek és kiválaszthatók.

Módosítás 115
Evžen Tošenovský

Rendeletre irányuló javaslat
4 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A (2) bekezdés szerint kiválasztott nemzeti biztonsági műveleti központ kötelezettséget vállal arra, hogy az eszközök és infrastruktúrák beszerzésétől vagy a támogatás odaítélésétől számított két éven belül – attól függően, hogy melyik következik be előbb – pályázik határokon átnyúló biztonsági műveleti központban való részvételre. Ha egy nemzeti biztonsági műveleti központ a szóban forgó időpontig nem válik valamely határokon átnyúló biztonsági műveleti központ résztvevőjévé, akkor e rendelet alapján nem jogosult további uniós támogatásra.	***törölve***

Or. en

Módosítás 116
Evžen Tošenovský

Rendeletre irányuló javaslat
5 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Határokon átnyúló biztonsági műveleti központok	***Eszközök és infrastruktúrák közös beszerzése***

Or. en

Módosítás 117
Evžen Tošenovský

Rendeletre irányuló javaslat
5 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) A nemzeti biztonsági műveleti központok által képviselt, a kiberbiztonsági események észlelését és a fenyegetések nyomon követését célzó tevékenységek összehangolására kötelezettséget vállaló, legalább három tagállamból álló üzemeltetési konzorcium jogosult részt venni a határokon átnyúló biztonsági műveleti központ létrehozására irányuló fellépésekben.	***törölve***

Or. en

Módosítás 118
Evžen Tošenovský

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 ***azokat a CSIRT-ISAC-okat, amelyek*** részt ***vesznek*** az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda ***a CSIRT-ISAC-oknak*** 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 ***a CSIRT-ISAC-okra*** hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és ***a részt vevő CSIRT-ISAC*** az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt***, beleértve az adott tagállambeli más CSIRT-ek és biztonsági védelmi központok általi***

használatukat.

Or. en

Módosítás 119
Ville Niinistö
a Verts/ALE képviselőcsoport nevében

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 ***választhatja*** 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.

Or. en

Indokolás

Bár ez a rendelet nem tartalmaz kifejezett kritériumokat, más alkalmazandó jogszabályok csökkenthetik annak bizonyosságát, hogy egy/minden egyes kérelmező sikeres.

Módosítás 120
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat

5 cikk – 2 a bekezdés (új)

A Bizottság által javasolt szöveg	*Módosítás*
	(2a) Lehetővé kell tenni a hasonlóan gondolkodó harmadik országban letelepedett magánjogi szervezet beszerzését és részvételét, amennyiben az nem ellentétes az Uniónak és a tagállamoknak az EUSZ V. címe szerinti közös kül- és biztonságpolitika keretében meghatározott biztonsági és védelmi érdekeivel vagy az e rendeletben meghatározott célkitűzésekkel. Ezeket a magánszervezetek nem tartozhatnak nem társult harmadik ország ellenőrzése alá, vagy azokat az (EU) 2019/452 európai parlamenti és tanácsi rendelet szerinti átvilágításnak kell alávetni.

Or. en

Módosítás 121
Evžen Tošenovský

Rendeletre irányuló javaslat
5 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Az üzemeltetési konzorcium tagjai írásos konzorciumi megállapodást kötnek, amely meghatározza az üzemeltetési és használati megállapodás végrehajtásának belső szabályait.	***törölve***

Or. en

Módosítás 122
Evžen Tošenovský

Rendeletre irányuló javaslat
5 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*

(4) A határokon átnyúló biztonsági műveleti központot jogi szempontból a koordináló biztonsági műveleti központként eljáró nemzeti biztonsági műveleti központ, vagy ha jogi személyiséggel rendelkezik, az üzemeltetési konzorcium képviseli. A koordináló biztonsági műveleti központ felel az üzemeltetési és használati megállapodásban, valamint az e rendeletben foglalt követelmények teljesítéséért.	***törölve***

Or. en

Módosítás 123
Evžen Tošenovský

Rendeletre irányuló javaslat
6 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Együttműködés és információmegosztás ***a határokon átnyúló biztonsági műveleti központokon belül és azok között***	***Megerősített*** együttműködés és információmegosztás ***uniós szinten***

Or. en

Módosítás 124
Johan Nissinen

Rendeletre irányuló javaslat
6 cikk – 1 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az üzemeltetési konzorcium tagjai a határokon átnyúló biztonsági műveleti központ keretében ***folytatják*** egymás között a releváns információk cseréjét, beleértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sebezhetőségekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra vonatkozó	(1) Az üzemeltetési konzorcium tagjai a határokon átnyúló biztonsági műveleti központ keretében ***folytathatják*** egymás között a releváns információk cseréjét, beleértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sebezhetőségekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra vonatkozó

információkat, az elkövetővel kapcsolatos információkat, a kiberbiztonsági figyelmeztetéseket, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokat, amennyiben az említett információmegosztás:

információkat, az elkövetővel kapcsolatos információkat, a kiberbiztonsági figyelmeztetéseket, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokat, amennyiben az említett információmegosztás:

Or. en

Módosítás 125
Evžen Tošenovský

Rendeletre irányuló javaslat
6 cikk – 1 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(1) ***Az üzemeltetési konzorcium*** tagjai a ***határokon átnyúló biztonsági műveleti központ*** keretében folytatják egymás között a releváns információk cseréjét, beleértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sebezhetőségekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra vonatkozó információkat, az elkövetővel kapcsolatos információkat, a kiberbiztonsági figyelmeztetéseket, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokat, amennyiben az említett információmegosztás:	(1) ***A CSIRT-ISAC-ok, valamint más CSIRT-ek*** tagjai a ***CSIRT-ek hálózatának*** keretében folytatják egymás között a releváns információk cseréjét, beleértve a kiberfenyegetésekre, a majdnem bekövetkezett eseményekre, a sebezhetőségekre, a technikákra és eljárásokra, a fertőzöttségi mutatókra, az ellenséges taktikákra vonatkozó információkat, az elkövetővel kapcsolatos információkat, a kiberbiztonsági figyelmeztetéseket, valamint a kibertámadások észlelésére szolgáló biztonságieszköz-konfigurációkra vonatkozó ajánlásokat, amennyiben az említett információmegosztás:

Or. en

Módosítás 126
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
6 cikk – 1 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) ***célja, hogy megelőzze, észlelje az***	a) ***javítja a kiberfenyegetésekkel***

eseményeket, reagáljon azokra vagy az eseményeket követően helyreállítsa a működést, illetve mérsékelje az események hatását;	***kapcsolatos hírszerzési információk cseréjét a biztonsági műveleti központok és az ágazati ISAC-ok között az események megelőzése, észlelése vagy enyhítése céljából***;

Or. en

Módosítás 127
Evžen Tošenovský

Rendeletre irányuló javaslat
6 cikk – 2 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(2) ***Az 5. cikk (3) bekezdésében említett írásbeli konzorciumi megállapodásban meg kell határozni*** a következőket:	(2) ***A CSIRT-ISAC-ok vagy adott esetben más CSIRT-ek közötti információ- és hírszerzésiinformáció-megosztási megállapodás*** a következőket ***állapíthatja meg***:

Or. en

Módosítás 128
Johan Nissinen

Rendeletre irányuló javaslat
6 cikk – 2 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) az (1) bekezdésben említett ***jelentős mennyiségű adat*** megosztására vonatkozó kötelezettségvállalás, valamint a szóban forgó információcsere feltételei;	a) az (1) bekezdésben említett ***adatok önkéntes*** megosztására vonatkozó kötelezettségvállalás, valamint a szóban forgó információcsere feltételei;

Or. en

Módosítás 129
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
6 cikk – 2 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) az (1) bekezdésben említett jelentős ***mennyiségű adat*** megosztására vonatkozó kötelezettségvállalás, valamint a szóban forgó információcsere feltételei;	a) az (1) bekezdésben említett jelentős ***adatok*** megosztására vonatkozó kötelezettségvállalás, valamint a szóban forgó információcsere feltételei;

Or. en

Módosítás 130
Evžen Tošenovský

Rendeletre irányuló javaslat
6 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Az egymás közötti információcsere ösztönzése érdekében a határokon átnyúló biztonsági műveleti központoknak gondoskodniuk kell arról, hogy egymás között magas szintű interoperabilitást alakítsanak ki. A határokon átnyúló biztonsági műveleti központok közötti interoperabilitás megkönnyítése érdekében a Bizottság végrehajtási jogi aktusok útján, az ECCC-vel folytatott konzultációt követően meghatározhatja ezen interoperabilitás feltételeit. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***törölve***

Or. en

Módosítás 131
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
6 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) ***Az egymás közötti*** információcsere	(3) ***A határokon átnyúló biztonsági***

ösztönzése érdekében a határokon átnyúló biztonsági műveleti központoknak ***gondoskodniuk kell arról, hogy*** egymás között ***magas szintű interoperabilitást alakítsanak ki***. A határokon átnyúló biztonsági műveleti központok közötti interoperabilitás megkönnyítése érdekében ***a Bizottság végrehajtási*** jogi aktusok útján***, az ECCC-vel folytatott konzultációt követően meghatározhatja*** ezen interoperabilitás ***feltételeit. Ezeket a végrehajtási jogi aktusokat*** az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás ***keretében kell elfogadni***.

műveleti központok közötti és az ágazati információmegosztási központokkal folytatott információcsere ösztönzése érdekében a határokon átnyúló biztonsági műveleti központoknak ***magas szintű interoperabilitást kell biztosítaniuk*** egymás között ***és – amennyiben lehetséges – az ágazati információmegosztási központokkal***. A határokon átnyúló biztonsági műveleti ***központok és az ágazati információmegosztási*** központok közötti interoperabilitás megkönnyítése érdekében ***az információmegosztási szabványokat és protokollokat össze kell hangolni a nemzetközi szabványokkal és az ágazat bevált gyakorlataival. Az ECCC továbbá felhatalmazáson alapuló*** jogi aktusok útján ***felkérheti a Bizottságot, hogy a regionális biztonsági műveleti központokkal szoros együttműködésben, valamint a nemzetközi szabványok és az ágazat bevált gyakorlatai alapján tegyen javaslatot*** ezen interoperabilitás ***feltételeire. E felhatalmazáson alapuló jogi aktusok*** az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás ***szerint kerülnek elfogadásra***.

Or. en

Módosítás 132
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
6 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Az egymás közötti információcsere ösztönzése érdekében a határokon átnyúló biztonsági műveleti központoknak gondoskodniuk kell arról, hogy egymás között magas szintű interoperabilitást alakítsanak ki. A határokon átnyúló biztonsági műveleti központok közötti interoperabilitás ***megkönnyítése*** érdekében a Bizottság végrehajtási jogi aktusok útján,	(3) Az egymás közötti információcsere ösztönzése érdekében a határokon átnyúló biztonsági műveleti központoknak gondoskodniuk kell arról, hogy egymás között magas szintű interoperabilitást alakítsanak ki. A ***kiberinfrastruktúrák, -szolgáltatások és -eszközök közös beszerzése megkönnyítheti a határokon átnyúló biztonsági műveleti központok***

az ECCC-vel folytatott konzultációt követően meghatározhatja ezen interoperabilitás feltételeit. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***közötti interoperabilitást. A*** határokon átnyúló biztonsági műveleti központok közötti interoperabilitás ***feltételeinek meghatározása*** érdekében a Bizottság végrehajtási jogi aktusok útján, az ECCC-vel ***és az ENISA-val*** folytatott konzultációt követően meghatározhatja ezen interoperabilitás feltételeit. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

Or. en

Módosítás 133
Evžen Tošenovský

Rendeletre irányuló javaslat
6 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással, amelyben meghatározzák a határokon átnyúló platformok közötti információmegosztás elveit.	***törölve***

Or. en

Módosítás 134
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
6 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással, amelyben meghatározzák a határokon átnyúló platformok közötti	(4) A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással, amelyben meghatározzák a határokon átnyúló platformok közötti

információmegosztás elveit.	információmegosztás elveit***, figyelembe véve az (EU) 2022/2555 irányelv szerinti, már meglévő releváns információmegosztási mechanizmusokat. A lehetséges vagy folyamatban lévő nagyszabású kiberbiztonsági incidensekkel összefüggésben az információmegosztási mechanizmusoknak meg kell felelniük az (EU) 2022/2555 irányelv vonatkozó rendelkezéseinek***.

Or. en

Módosítás 135
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
6 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással, amelyben meghatározzák a határokon átnyúló platformok közötti információmegosztás elveit.	***4.*** A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással ***és az ágazaton belüli információmegosztási és -elemző központokkal (ISAC)***, amelyben meghatározzák a határokon átnyúló platformok közötti információmegosztás ***és interoperabilitás*** elveit.

Or. en

Módosítás 136
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
7 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Együttműködés és információmegosztás ***az uniós szervezetekkel***	Együttműködés és információmegosztás ***a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) hálózatával***

Or. en

Módosítás 137
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 ***megosztott helyzetfelismerés céljából*** információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a ***koordinációt végző biztonsági műveleti központok a*** releváns információkat az (EU) 2022/2555 irányelv szerinti válságkezelési szerepük figyelembevételével indokolatlan késedelem nélkül eljuttatják ***saját számítógép-biztonsági eseményekre reagáló csoportjuknak vagy az illetékes hatóságnak, akik erről jelentést tesznek*** az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak.

Or. en

Indokolás

Javasolja, hogy a nagy horderejű váratlan események esetében tartsák be a NIS 2 eljárást.

Módosítás 138
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	***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 ***szerepükkel összhangban*** indokolatlan

késedelem nélkül eljuttatják az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak.	késedelem nélkül eljuttatják az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak***, valamint az ENISA-nak***.

Or. en

Módosítás 139
Evžen Tošenovský

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 számítógép-biztonsági eseményekre reagáló csoportok, az információmegosztó és -elemző*** 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 ***és*** a CSIRT-ek hálózatának.

Or. en

Módosítás 140
Evžen Tošenovský

Rendeletre irányuló javaslat
7 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdésben előírt információmegosztásra vonatkozó eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***törölve***

Módosítás 141
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
7 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdésben előírt információmegosztásra vonatkozó eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***2.*** A Bizottság ***a határokon átnyúló platformokkal és a számítógép-biztonsági eseményekre reagáló csoportok hálózatával folytatott konzultációt követően*** végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdésben előírt információmegosztásra vonatkozó eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni ***az (EU) 2022/2555 irányelvvel összhangban***.

Or. en

Indokolás

Javasolja, hogy tartsák be a NIS 2 eljárást a nagyszabású váratlan események vonatkozásában, és ezért először konzultáljanak a számítógép-biztonsági eseményekre reagáló csoportok hálózatával.

Módosítás 142
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
7 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdésben előírt információmegosztásra vonatkozó eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell	***2.*** A Bizottság ***az ENISA-val folytatott konzultációt követően*** végrehajtási jogi aktusok útján meghatározhatja az (1) bekezdésben előírt információmegosztásra vonatkozó eljárási szabályokat. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2)

elfogadni.

bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

Or. en

Módosítás 143
Johan Nissinen

Rendeletre irányuló javaslat
8 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(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.	***1.*** Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak az Európai Kiberpajzs infrastruktúrájának magas szintű ***titkosságát,*** 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.

Or. en

Módosítás 144
Evžen Tošenovský

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 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	***törölve***

főképviselő támogatásával – figyelembe veszi a vonatkozó védelmi szintű biztonsági előírásokat.

Or. en

Módosítás 145
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 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.	***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 ***az (EU) 2022/2555 és az (EU) 2022/2557 irányelvvel összhangban***. Ennek során a katonai szereplőkkel való együttműködés megkönnyítése érdekében a Bizottság – a főképviselő támogatásával – figyelembe veszi a vonatkozó védelmi szintű biztonsági előírásokat.

Or. en

Módosítás 146
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***az ENISA-val folytatott konzultációt követően*** végrehajtási jogi aktusokat fogadhat el, amelyekben technikai

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.

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.

Or. en

Módosítás 147
Johan Nissinen

Rendeletre irányuló javaslat
9. cikk – (1) bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Létrejön a kiberbiztonsági vészhelyzeti ***mechanizmus***, amelynek célja az Unió súlyos kiberbiztonsági fenyegetésekkel szembeni rezilienciájának javítása, valamint a szolidaritás szellemében a jelentős és nagyszabású kiberbiztonsági események rövid távú hatásaira való felkészülés és e hatások enyhítése (a továbbiakban: mechanizmus).	***1. Az érintett tagállam(ok) kifejezett kérésére létrehozzák*** a kiberbiztonsági vészhelyzeti ***mechanizmust***, amelynek célja az Unió súlyos kiberbiztonsági fenyegetésekkel szembeni rezilienciájának javítása, valamint a szolidaritás szellemében a jelentős és nagyszabású kiberbiztonsági események rövid távú hatásaira való felkészülés és e hatások enyhítése (a továbbiakban: mechanizmus).

Or. en

Módosítás 148
Evžen Tošenovský

Rendeletre irányuló javaslat
9. cikk – (1) bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Létrejön a kiberbiztonsági vészhelyzeti mechanizmus, amelynek célja	***1.*** Létrejön a kiberbiztonsági vészhelyzeti mechanizmus, amelynek célja

az Unió ***súlyos*** kiberbiztonsági fenyegetésekkel szembeni rezilienciájának javítása, valamint a szolidaritás szellemében a jelentős és nagyszabású kiberbiztonsági események rövid távú hatásaira való felkészülés és e hatások enyhítése (a továbbiakban: mechanizmus).	az Unió ***jelentős*** kiberbiztonsági fenyegetésekkel szembeni rezilienciájának javítása, valamint a szolidaritás szellemében a jelentős és nagyszabású kiberbiztonsági események rövid távú hatásaira való felkészülés és e hatások enyhítése (a továbbiakban: mechanizmus).

Or. en

Módosítás 149
Johan Nissinen

Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) a jelentős és nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást támogató reagálási intézkedések, amelyeket a 12. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő megbízható szolgáltatók biztosítanak;	b) a jelentős és nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást támogató reagálási intézkedések, amelyeket a 12. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő megbízható szolgáltatók biztosítanak***, az érintett tagállam(ok) kifejezett kérésére***;

Or. en

Módosítás 150
Evžen Tošenovský

Rendeletre irányuló javaslat
10 cikk – 1 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) a jelentős és nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást támogató reagálási intézkedések, amelyeket a 12. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő megbízható szolgáltatók biztosítanak;	b) a jelentős és nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást támogató reagálási intézkedések, amelyeket a 12. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő***, irányított biztonsági szolgáltatásokat nyújtó,*** megbízható

szolgáltatók biztosítanak;

Or. en

Módosítás 151
Ville Niinistö
a Verts/ALE képviselőcsoport nevében

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

A Bizottság által javasolt szöveg	*Módosítás*
	1a. A kibervészhelyzeti mechanizmus aktiválását követően a Bizottság minden évben jelentést tesz a mechanizmus pozitív és negatív működésének értékeléséről, beleértve azt is, hogy szükség van-e további együttműködésre vagy képzési követelményekre.

Or. en

Módosítás 152
Evžen Tošenovský

Rendeletre irányuló javaslat
11 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) A szervezetek 10. cikk (1) bekezdésének a) pontjában említett összehangolt felkészültségi tesztelésének Unió-szerte történő támogatása céljából a Bizottság a Kiberbiztonsági Együttműködési Csoporttal és az ENISA-val folytatott konzultációt követően azonosítja az (EU) 2022/2555 irányelv I. mellékletében felsorolt kiemelten kritikus ágazatokon belüli érintett ágazatokat vagy alágazatokat, amelyek szervezetei a meglévő és tervezett összehangolt uniós szintű kockázatértékelések és rezilienciatesztek figyelembevételével összehangolt felkészültségi tesztelés alá	***1.*** A szervezetek 10. cikk (1) bekezdésének a) pontjában említett összehangolt felkészültségi tesztelésének Unió-szerte történő támogatása céljából a Bizottság a Kiberbiztonsági Együttműködési Csoporttal és az ENISA-val folytatott konzultációt követően azonosítja az (EU) 2022/2555 irányelv I. mellékletében felsorolt kiemelten kritikus ágazatokon belüli érintett ágazatokat vagy alágazatokat, amelyek szervezetei a meglévő és tervezett összehangolt uniós szintű kockázatértékelések és rezilienciatesztek figyelembevételével összehangolt ***önkéntes*** felkészültségi

vonhatók.	tesztelés alá vonhatók.

Or. en

Módosítás 153
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
11 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az ENISA-val és a főképviselővel együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt teszteléshez.	***2.*** A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az ENISA-val és a főképviselővel együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt ***felkészültségi*** teszteléshez. ***Ez alapul szolgál azon érintett ágazatok vagy alágazatok azonosításához, amelyek esetében a jogalanyokat az (1) bekezdésben leírt összehangolt előkészítési vizsgálatnak vethetik alá.***

Or. en

Módosítás 154
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
11 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az ENISA-val ***és a főképviselővel*** együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt teszteléshez.	***2.*** A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az ENISA-val***, a főképviselővel, az EKSZ-szel, és adott esetben az EDA-val és a felkészültségi tesztelésnek adott esetben alávetett jogalanyokkal*** együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt teszteléshez.

Or. en

Módosítás 155
Johan Nissinen

Rendeletre irányuló javaslat
12 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Létre kell hozni az uniós kiberbiztonsági tartalékot annak érdekében, hogy jelentős vagy nagyszabású kiberbiztonsági események alkalmával a (3) bekezdésben említett felhasználók segítséget kapjanak a reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.	***1.*** Létre kell hozni az uniós kiberbiztonsági tartalékot annak érdekében, hogy ***az érintett tagállam(ok) kifejezett kérésére és az egyes tagállamok biztonság- és védelempolitikája sajátos jellegének sérelme nélkül a*** jelentős vagy nagyszabású kiberbiztonsági események alkalmával a (3) bekezdésben említett felhasználók segítséget kapjanak a reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.

Or. en

Módosítás 156
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 valamennyi tagállamban igénybe vehetők***, erősítik az Unió rezilienciáját és szuverenitását, és javítják az Unió versenyképességét. A kiválasztott megbízható szolgáltatók nevét és szolgáltatásaikat bizalmasan kell***

kezelni.

Or. en

Módosítás 157
Johan Nissinen

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 valamennyi tagállamban igénybe vehetők. ***Az uniós kiberbiztonsági tartalék nem korlátozza annak szükségességét, hogy az országok figyelemmel kísérhessék és felmérhessék saját szükségleteiket.***

Or. en

Módosítás 158
Evžen Tošenovský

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***, irányított biztonsági szolgáltatásokat nyújtó,*** megbízható szolgáltatók eseményreagálási szolgáltatásaiból áll össze. A tartalék előzetes kötelezettségvállalás keretében rendelkezésre bocsátott szolgáltatásokat tartalmaz. A szolgáltatások ***kérésre*** valamennyi tagállamban igénybe vehetők.

Or. en

Módosítás 159
Evžen Tošenovský

Rendeletre irányuló javaslat
12 cikk – 3 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) az ***uniós intézmények, szervek és ügynökségek***.	b) Az ***e rendelet 17. cikkében említett harmadik országok***.

Or. en

Módosítás 160
Evžen Tošenovský

Rendeletre irányuló javaslat
12 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(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.	***4.*** A (3) bekezdés a) pontjában említett ***felhasználók kérésre igénybe vehetik*** az uniós kiberbiztonsági tartalék szolgáltatásait 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.

Or. en

Módosítás 161
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
12 cikk – 5 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(5) A Bizottság általános felelősséggel	***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.	tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság ***a NIS 2 koordinációs csoporttal egyeztetve és*** 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.

Or. en

Módosítás 162
Evžen Tošenovský

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 ***az ENISA-val együttműködésben*** 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.

Or. en

Módosítás 163
Evžen Tošenovský

Rendeletre irányuló javaslat
12 cikk – 6 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) A Bizottság hozzájárulási megállapodások révén részben vagy egészben az ENISA-t bízhatja meg az uniós kiberbiztonsági tartalék működtetésével és igazgatásával.	***törölve***

Or. en

Módosítás 164
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
12 cikk – 6 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) A Bizottság hozzájárulási megállapodások révén részben vagy egészben az ENISA-t ***bízhatja meg*** az uniós kiberbiztonsági tartalék működtetésével és igazgatásával.	***6.*** A Bizottság hozzájárulási megállapodások révén részben vagy egészben ***megbízza*** az ENISA-t az uniós kiberbiztonsági tartalék működtetésével és igazgatásával.

Or. en

Módosítás 165
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	***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***, beleértve a kiberbiztonsági munkaerő szükséges készségeit és kapacitását***. Az ENISA a Bizottsággal folytatott konzultációt

17. cikk alapján támogatásra jogosult harmadik országok szükségleteinek azonosítása érdekében. A Bizottság adott esetben konzultál a főképviselővel.

követően ***és a magánszektorral partnerségben*** 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.

Or. en

Módosítás 166
Evžen Tošenovský

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 harmadik országok szükségleteinek azonosítása érdekében. A Bizottság adott esetben konzultál a főképviselővel. ***Továbbá tájékoztatja a Tanácsot a harmadik országok szükségleteiről.***

Or. en

Módosítás 167
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
12 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) Annak érdekében, hogy támogassa	***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.	a Bizottságot az uniós kiberbiztonsági tartalék létrehozásában, az ENISA a tagállamokkal***, a Bizottsággal, az irányított biztonsági szolgáltatásokat nyújtó szolgáltatókkal és az ágazat képviselőivel*** 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.

Or. en

Módosítás 168
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
12 cikk – 8 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(8) A Bizottság ***végrehajtási jogi aktusok útján meghatározhatja*** az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusait és számát. E végrehajtási jogi aktusokat a 21. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***8.*** A Bizottság ***e rendelet 20a. cikkével összhangban felhatalmazáson alapuló jogi aktust fogadhat el, hogy meghatározza*** az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusait és számát. E végrehajtási jogi aktusokat a 21. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

Or. en

Módosítás 169
Evžen Tošenovský

Rendeletre irányuló javaslat
13 cikk – 5 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) ***megfelelő információk*** az érintett ***szervezetről*** és a kiberbiztonsági esemény lehetséges hatásairól, valamint a kért támogatás tervezett felhasználásáról, beleértve a becsült szükségletek megjelölését is;	a) az érintett ***szervezet típusa*** és a kiberbiztonsági esemény lehetséges hatásairól, valamint a kért támogatás tervezett felhasználásáról, beleértve a becsült szükségletek megjelölését is;

Or. en

Módosítás 170
Evžen Tošenovský

Rendeletre irányuló javaslat
13 cikk – 5 bekezdés – b pont

A Bizottság által javasolt szöveg	*Módosítás*
b) a (2) bekezdésben említett, a támogatás iránti kérelem tárgyát képező esemény hatásainak enyhítése érdekében hozott intézkedésekre vonatkozó információk;	b) a (2) bekezdésben említett, a támogatás iránti kérelem tárgyát képező esemény hatásainak enyhítése érdekében hozott intézkedésekre vonatkozó ***általános*** információk;

Or. en

Módosítás 171
Evžen Tošenovský

Rendeletre irányuló javaslat
13 cikk – 5 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) az érintett szervezet rendelkezésére álló egyéb támogatási formákra vonatkozó információk***, beleértve az eseményreagálási és az azonnali helyreállítási szolgáltatásokra vonatkozó szerződéses megállapodásokat, valamint az ilyen típusú kiberbiztonsági eseményekre potenciálisan kiterjedő biztosítási szerződéseket.***	c) az érintett szervezet rendelkezésére álló egyéb támogatási formákra vonatkozó információk

Or. en

Módosítás 172
Evžen Tošenovský

Rendeletre irányuló javaslat
13 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) A Bizottság végrehajtási jogi aktusok útján pontosíthatja az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályokat. E végrehajtási jogi aktusokat a 21. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***törölve***

Or. en

Módosítás 173
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
13 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) A Bizottság ***végrehajtási jogi aktusok útján pontosíthatja*** az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályokat. E végrehajtási jogi aktusokat a 21. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.	***7.*** A Bizottság ***e rendelet 20a. cikkével összhangban felhatalmazáson alapuló jogi aktusokat fogadhat el, amelyekben pontosítja*** az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályokat. E végrehajtási jogi aktusokat a 21. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

Or. en

Módosítás 174
Evžen Tošenovský

Rendeletre irányuló javaslat
14 cikk – 1 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmeket a Bizottság az ENISA közreműködésével ***vagy a 12. cikk (6) bekezdése szerinti hozzájárulási megállapodásokban meghatározottak szerint értékeli, és a választ haladéktalanul*** továbbítja a 12. cikk (3) bekezdésében említett felhasználóknak.	***1.*** Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmeket a Bizottság az ENISA közreműködésével ***értékeli, és határozatát indokolatlan késedelem nélkül, de legkésőbb 24 órán belül*** továbbítja a 12. cikk (3) bekezdésében említett felhasználóknak.

Or. en

Módosítás 175
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
14 cikk – 2 bekezdés – d pont

A Bizottság által javasolt szöveg	*Módosítás*
d) a kiberbiztonsági esemény lehetséges határokon átnyúló jellege és annak kockázata, hogy tovagyűrűzhet más tagállamokra vagy felhasználókra;	d) a kiberbiztonsági esemény ***kiterjedése,*** lehetséges határokon átnyúló jellege és annak kockázata, hogy tovagyűrűzhet más tagállamokra vagy felhasználókra;

Or. en

Módosítás 176
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
14 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Az uniós kiberbiztonsági tartalék szolgáltatásait a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi	***3.*** Az uniós kiberbiztonsági tartalék szolgáltatásait a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi

megállapodásokkal összhangban kell nyújtani. E megállapodásoknak tartalmazniuk kell felelősségre vonatkozó feltételeket is.	megállapodásokkal összhangban kell nyújtani. E megállapodásoknak tartalmazniuk kell felelősségre vonatkozó feltételeket is ***és a megállapodásban részes felek által az adott szolgáltatás nyújtásához szükségesnek ítélt egyéb rendelkezéseket***.

Or. en

Módosítás 177
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
14 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) Az uniós kiberbiztonsági tartalék szolgáltatásait a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi megállapodásokkal összhangban kell nyújtani. E megállapodásoknak tartalmazniuk kell felelősségre vonatkozó feltételeket is.	***3.*** Az uniós kiberbiztonsági tartalék szolgáltatásait ***a felhasználó jóváhagyása mellett és*** a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi megállapodásokkal összhangban kell nyújtani. E megállapodásoknak tartalmazniuk kell felelősségre vonatkozó feltételeket is.

Or. en

Módosítás 178
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
14 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A (3) bekezdésben említett ***megállapodások alapulhatnak*** az ENISA által a tagállamokkal folytatott konzultációt követően készített sablonokon.	***4.*** A (3) bekezdésben említett ***megállapodásoknak*** az ENISA által a tagállamokkal ***és a tartalék más felhasználóival*** folytatott konzultációt követően készített sablonokon ***kell alapulniuk***.

Or. en

Módosítás 179
Evžen Tošenovský

Rendeletre irányuló javaslat
14 cikk – 5 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(5) A Bizottság és az ENISA nem visel szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott károkért.	***törölve***

Or. en

Módosítás 180
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
14 cikk – 5 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(5) A Bizottság és az ENISA nem visel szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott károkért.	***5.*** A Bizottság és az ENISA nem visel szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott károkért***, kivéve a szolgáltató kérelmének értékelése során elkövetett gondatlanság eseteit, vagy azokban az esetekben, amikor a Bizottság vagy az ENISA felhasználók, és a károkért felelősek***.

Or. en

Módosítás 181
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat

14 cikk – 5 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(5) A Bizottság és az ENISA nem visel szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott károkért.	***5.*** A Bizottság és az ENISA nem visel szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott károkért***, kivéve azokat az eseteket, amikor a Bizottság vagy az ENISA a 14. cikk (3) bekezdése szerint a Tartalék felhasználói***.

Or. en

Módosítás 182
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
14 cikk – 6 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) A támogatási intézkedés befejezését követő egy hónapon belül a felhasználók összefoglaló jelentést nyújtanak be a Bizottságnak és az ENISA-nak a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról. Amennyiben a felhasználó a 17. cikkben meghatározott harmadik országból származik, a szóban forgó jelentést meg kell osztani a főképviselővel.	***6.*** A támogatási intézkedés befejezését követő egy hónapon belül a felhasználók összefoglaló jelentést nyújtanak be a Bizottságnak és az ENISA-nak a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról. Amennyiben a felhasználó a 17. cikkben meghatározott harmadik országból származik, a szóban forgó jelentést meg kell osztani a főképviselővel. ***A jelentésnek tiszteletben kell tartania az érzékeny vagy minősített adatok védelmére vonatkozó uniós és nemzeti jogszabályokat.***

Or. en

Módosítás 183
Evžen Tošenovský

Rendeletre irányuló javaslat
14 cikk – 6 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) A támogatási intézkedés befejezését követő egy hónapon belül a felhasználók összefoglaló jelentést nyújtanak be a Bizottságnak ***és az ENISA-nak*** a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról. Amennyiben a felhasználó a 17. cikkben meghatározott harmadik országból származik, a szóban forgó jelentést meg kell osztani a főképviselővel.	***6.*** A támogatási intézkedés befejezését követő egy hónapon belül a felhasználók összefoglaló jelentést nyújtanak be a Bizottságnak***, az ENISA-nak, számítógép-biztonsági eseményekre reagáló csoportok hálózatának, és adott esetben az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának*** a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról. Amennyiben a felhasználó a 17. cikkben meghatározott harmadik országból származik, a szóban forgó jelentést meg kell osztani a főképviselővel.

Or. en

Módosítás 184
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
14 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(7) A Bizottság rendszeresen jelentést tesz a Kiberbiztonsági Együttműködési Csoportnak a támogatás felhasználásáról és eredményeiről.	***7.*** A Bizottság rendszeresen jelentést tesz a Kiberbiztonsági Együttműködési Csoportnak a támogatás felhasználásáról és eredményeiről. ***A bizalmas információkat az érzékeny vagy minősített adatok védelmére vonatkozó uniós vagy nemzeti jogszabályokkal összhangban védenie kell.***

Or. en

Módosítás 185
Evžen Tošenovský

Rendeletre irányuló javaslat
14 cikk – 7 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*

(7) A Bizottság ***rendszeresen*** jelentést tesz a Kiberbiztonsági Együttműködési Csoportnak a támogatás felhasználásáról és eredményeiről.	***7.*** A Bizottság ***évente legalább kétszer*** jelentést tesz a Kiberbiztonsági Együttműködési Csoportnak a támogatás felhasználásáról és eredményeiről.

Or. en

Módosítás 186
Evžen Tošenovský

Rendeletre irányuló javaslat
15 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Koordináció a válságkezelési ***mechanizmusokkal***	***A kiberbiztonsági szükséghelyzeti mechanizmus és*** a válságkezelési ***mechanizmusok összehangolása***

Or. en

Módosítás 187
Evžen Tošenovský

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 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.***	***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 nyújtott segítséget.

Or. en

Módosítás 188
Evžen Tošenovský

Rendeletre irányuló javaslat
16 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Megbízható szolgáltatók	***Az irányított biztonsági szolgáltatásokat nyújtó,*** megbízható szolgáltatók

Or. en

Módosítás 189
Johan Nissinen

Rendeletre irányuló javaslat
16 cikk – 1 bekezdés – bevezető rész

A Bizottság által javasolt szöveg	*Módosítás*
(1) Az uniós kiberbiztonsági tartalék létrehozását célzó közbeszerzési eljárások során az ajánlatkérő szerv az (EU, Euratom) 2018/1046 rendeletben meghatározott elvekkel és a következő elvekkel összhangban jár el:	***1.*** Az uniós kiberbiztonsági tartalék létrehozását célzó közbeszerzési eljárások során az ajánlatkérő szerv ***a tagállamok nemzetbiztonsággal kapcsolatos elsődleges felelősségének sérelme nélkül,*** az (EU, Euratom) 2018/1046 rendeletben meghatározott elvekkel és a következő elvekkel összhangban jár el:

Or. en

Módosítás 190
Evžen Tošenovský

Rendeletre irányuló javaslat
16 cikk – 1 bekezdés – a pont

A Bizottság által javasolt szöveg	*Módosítás*
a) biztosítja, hogy az uniós kiberbiztonsági tartalék olyan szolgáltatásokat foglaljon magában, amelyek valamennyi tagállamban igénybe vehetők, figyelembe véve különösen az	a) biztosítja, hogy az uniós kiberbiztonsági tartalék olyan szolgáltatásokat foglaljon magában, amelyek ***e rendelet 17. cikkével összhangban*** valamennyi tagállamban ***és***

ilyen szolgáltatások nyújtására vonatkozó nemzeti követelményeket, beleértve a tanúsítást, illetve az akkreditációt is;	***harmadik országban*** igénybe vehetők, figyelembe véve különösen az ilyen szolgáltatások nyújtására vonatkozó nemzeti követelményeket, beleértve a tanúsítást, illetve az akkreditációt is;

Or. en

Módosítás 191
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
16 cikk – 1 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) biztosítja, hogy az uniós kiberbiztonsági tartalék uniós hozzáadott értéket képviseljen azáltal, hogy hozzájárul az (EU) 2021/694 rendelet 3. cikkében meghatározott célkitűzésekhez, így többek között előmozdítsa a kiberbiztonsági készségek fejlesztését az EU-ban.	c) biztosítja, hogy az uniós kiberbiztonsági tartalék uniós hozzáadott értéket képviseljen azáltal, hogy hozzájárul az (EU) 2021/694 rendelet 3. cikkében meghatározott célkitűzésekhez, így többek között előmozdítsa a kiberbiztonsági készségek fejlesztését az EU-ban***, megerősítve az Unió rezilienciáját és szuverenitását, valamint javítva az Unió versenyképességét***.

Or. en

Módosítás 192
Evžen Tošenovský

Rendeletre irányuló javaslat
16 cikk – 1 bekezdés – c pont

A Bizottság által javasolt szöveg	*Módosítás*
c) biztosítja, hogy az uniós kiberbiztonsági tartalék ***uniós hozzáadott értéket képviseljen azáltal, hogy*** hozzájárul az (EU) 2021/694 rendelet 3. cikkében meghatározott célkitűzésekhez, így többek között előmozdítsa a kiberbiztonsági készségek fejlesztését az EU-ban.	c) biztosítja, hogy az uniós kiberbiztonsági tartalék hozzájárul az (EU) 2021/694 rendelet 3. cikkében meghatározott célkitűzésekhez, így többek között előmozdítsa a kiberbiztonsági készségek fejlesztését az EU-ban.

Or. en

Módosítás 193
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***legújabb*** műszaki berendezésekkel, beleértve a hardvereket és szoftvereket is***, és adott esetben meg kell felelnie a(z) XX/XXXX rendeletben (a kiberrezilienciáról szóló jogszabály) meghatározott követelményeknek***;

Or. en

Módosítás 194
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

A Bizottság által javasolt szöveg	*Módosítás*
	fa) a szolgáltatónak bizonyítania kell, hogy döntéshozatali és irányítási struktúrái mentesek az Unió rendszerszintű riválisainak minősülő államok kormányainak jogtalan befolyásától;

Or. en

Módosítás 195
Evžen Tošenovský

Rendeletre irányuló javaslat

16 cikk – 2 bekezdés – h pont

A Bizottság által javasolt szöveg	*Módosítás*
h) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást rövid időn belül nyújtsa abban a tagállamban, illetve azokban a tagállamokban**,** ahol a szolgáltatást biztosítani tudja;	h) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást rövid időn belül nyújtsa abban a tagállamban, illetve azokban a tagállamokban ***vagy harmadik országokban*** ahol a szolgáltatást biztosítani tudja;

Or. en

Módosítás 196
Evžen Tošenovský

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – i pont

A Bizottság által javasolt szöveg	*Módosítás*
i) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást azon tagállam(ok) helyi nyelvén nyújtsa, ahol a szolgáltatást nyújtani tudja;	i) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást azon tagállam(ok) ***vagy harmadik országok*** helyi nyelvén nyújtsa, ahol a szolgáltatást nyújtani tudja***, vagy az uniós intézmények egyik munkanyelvén***;

Or. en

Módosítás 197
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – j pont

A Bizottság által javasolt szöveg	*Módosítás*
j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó uniós tanúsítási rendszer, a szolgáltatónak az említett rendszerrel összhangban ***kell*** tanúsítást szereznie.	j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó uniós tanúsítási rendszer, a szolgáltatónak ***a rendszer elfogadásától számított két éven belül*** az említett rendszerrel összhangban tanúsítást ***kell*** szereznie.

Or. en

Módosítás 198
Evžen Tošenovský

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – j pont

A Bizottság által javasolt szöveg	*Módosítás*
j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó ***uniós*** tanúsítási rendszer, a szolgáltatónak az említett rendszerrel összhangban kell tanúsítást szereznie.	j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó ***európai kiberbiztonsági*** tanúsítási rendszer, a szolgáltatónak az említett rendszerrel összhangban kell tanúsítást szereznie.

Or. en

Módosítás 199
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
16 cikk – 2 bekezdés – j pont

A Bizottság által javasolt szöveg	*Módosítás*
j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó uniós tanúsítási rendszer, a szolgáltatónak az említett rendszerrel összhangban ***kell*** tanúsítást szereznie.	j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó uniós tanúsítási rendszer, a szolgáltatónak az említett rendszerrel összhangban ***két éven belül*** tanúsítást ***kell*** szereznie.

Or. en

Indokolás

A Bizottság javaslata szerint az e rendeletben felsorolt műszaki követelményeket egy tanúsítási rendszer váltja fel. Ez a módosítás több időt biztosít a vállalkozások, különösen a kkv-k számára az említett rendszerre való átállásra, és ösztönzi az egyenlőbb versenyfeltételeket az egész Unióban. Addig az időpontig be kell tartaniuk e rendelet műszaki követelményeit.

Módosítás 200

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

A Bizottság által javasolt szöveg	*Módosítás*
	ja) a szolgáltatónak képesnek kell lennie arra, hogy szolgáltatásait a szélesebb körű szerződéstől különválassza, hogy a felhasználó másik szolgáltatóra válthasson;

Or. en

Módosítás 201
Evžen Tošenovský

Rendeletre irányuló javaslat
17 cikk – 6 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(6) A Bizottság egyeztet a főképviselővel a beérkezett kérelmekről és az uniós kiberbiztonsági tartalékból harmadik országoknak nyújtott támogatás végrehajtásáról.	***6.*** A Bizottság ***indokolatlan késedelem nélkül értesíti a Tanácsot, és*** egyeztet a főképviselővel a beérkezett kérelmekről és az uniós kiberbiztonsági tartalékból harmadik országoknak nyújtott támogatás végrehajtásáról.

Or. en

Módosítás 202
Evžen Tošenovský

Rendeletre irányuló javaslat
18 cikk

A Bizottság által javasolt szöveg	*Módosítás*
18. cikk	***törölve***
A kiberbiztonsági események felülvizsgálati mechanizmusa	
(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 főképviselővel.

(2) Az (1) bekezdésben említett eseményértékelési jelentés elkészítése érdekében az ENISA együttműködik valamennyi érdekelt féllel, beleértve a tagállamok, a Bizottság és más érintett uniós intézmények, szervek és ügynökségek, valamint az irányított biztonsági szolgáltatók képviselőit és a kiberbiztonsági szolgáltatások felhasználóit. Az ENISA adott esetben együttműködik a jelentős vagy nagyszabású kiberbiztonsági események által érintett szervezetekkel is. Az eseményértékelés alátámasztása érdekében az ENISA más típusú érdekelt felekkel is konzultálhat. A konzultációba bevont képviselőknek jelezniük kell bármilyen esetleges összeférhetetlenséget.

(3) A jelentésnek ki kell terjednie az adott jelentős vagy nagyszabású kiberbiztonsági esemény felülvizsgálatára és elemzésére, beleértve a fő okokat, a sebezhetőségeket és a levont tanulságokat. A bizalmas információkat az érzékeny vagy minősített adatok védelmére vonatkozó uniós vagy nemzeti jogszabályokkal összhangban védenie kell.

(4) A jelentés adott esetben ajánlásokat fogalmaz meg az Unió kiberbiztonsági helyzetének javítása érdekében.

(5) Ha lehetséges, a jelentés egy változatát nyilvánosan hozzáférhetővé kell tenni. Ez a változat csak nyilvános információkat tartalmazhat.

Or. en

Módosítás 203
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
18 cikk – 2 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(2) Az (1) bekezdésben említett eseményértékelési jelentés elkészítése érdekében az ENISA együttműködik valamennyi érdekelt féllel, beleértve a tagállamok, a Bizottság és más érintett uniós intézmények, szervek és ügynökségek, valamint az irányított biztonsági szolgáltatók képviselőit és a kiberbiztonsági szolgáltatások felhasználóit. Az ENISA adott esetben együttműködik a jelentős vagy nagyszabású kiberbiztonsági események által érintett szervezetekkel is. Az eseményértékelés alátámasztása érdekében az ENISA más típusú érdekelt felekkel is konzultálhat. A konzultációba bevont képviselőknek jelezniük kell bármilyen esetleges összeférhetetlenséget.	***2.*** Az (1) bekezdésben említett eseményértékelési jelentés elkészítése érdekében az ENISA együttműködik valamennyi érdekelt féllel***, és visszajelzést gyűjt azoktól***, beleértve a tagállamok, a Bizottság és más érintett uniós intézmények, szervek és ügynökségek, valamint az irányított biztonsági szolgáltatók képviselőit és a kiberbiztonsági szolgáltatások felhasználóit. Az ENISA adott esetben együttműködik a jelentős vagy nagyszabású kiberbiztonsági események által érintett szervezetekkel is. Az eseményértékelés alátámasztása érdekében az ENISA más típusú érdekelt felekkel is konzultálhat. A konzultációba bevont képviselőknek jelezniük kell bármilyen esetleges összeférhetetlenséget.

Or. en

Módosítás 204
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Rendeletre irányuló javaslat
18 cikk – 3 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(3) A jelentésnek ki kell terjednie az adott jelentős vagy nagyszabású kiberbiztonsági esemény felülvizsgálatára és elemzésére, beleértve a fő okokat, a sebezhetőségeket és a levont tanulságokat.	***3.*** A jelentésnek ki kell terjednie az adott jelentős vagy nagyszabású kiberbiztonsági esemény felülvizsgálatára és elemzésére, beleértve a fő okokat, a sebezhetőségeket és a levont tanulságokat.

A bizalmas információkat az érzékeny vagy minősített adatok védelmére vonatkozó uniós vagy nemzeti jogszabályokkal összhangban védenie kell.	A bizalmas információkat az érzékeny vagy minősített adatok védelmére vonatkozó uniós vagy nemzeti jogszabályokkal összhangban védenie kell. ***Nem tartalmazhat semmilyen részletet az aktívan kihasznált sebezhetőségekről, amelyek továbbra is orvosolatlanok.***

Or. en

Módosítás 205
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
18 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A jelentés adott esetben ajánlásokat fogalmaz meg az Unió kiberbiztonsági helyzetének javítása érdekében***.***	***4.*** A jelentés adott esetben ***konkrét*** ajánlásokat fogalmaz meg **–** ***többek között valamennyi érdekelt fél számára –*** az Unió kiberbiztonsági helyzetének javítása érdekében***;***

Or. en

Módosítás 206
Johan Nissinen

Rendeletre irányuló javaslat
18 cikk – 4 bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
(4) A jelentés adott esetben ajánlásokat fogalmaz meg az Unió kiberbiztonsági helyzetének javítása érdekében.	***4.*** A jelentés adott esetben ***jogilag nem kötelező erejű önkéntes*** ajánlásokat fogalmaz meg az Unió kiberbiztonsági helyzetének javítása érdekében.

Or. en

Módosítás 207
Evžen Tošenovský

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

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 ***számítógép-biztonsági eseményekre reagáló csoportok (CSIRT), az információmegosztó és -elemző központok (ISAC) és a*** biztonsági műveleti központok ***(SOC)*** fejlesztését, telepítését és működtetését, amelyek hozzájárulnak az Unión belüli helyzetismerethez és az Unió kiberfenyegetettségi információszerző képességeinek megerősítéséhez;

Or. en

Módosítás 208
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
19 cikk – 1 bekezdés – 3 pont
Az (EU) 2021/694 rendelet
14. cikk (2) bekezdés

A Bizottság által javasolt szöveg	*Módosítás*
A program a költségvetési rendeletben megállapított bármely formában nyújthat finanszírozást, többek között különösen közbeszerzés mint elsődleges forma vagy vissza nem térítendő támogatások és pénzdíjak útján.	A program a költségvetési rendeletben megállapított bármely formában nyújthat finanszírozást, többek között különösen közbeszerzés mint elsődleges forma vagy vissza nem térítendő támogatások és pénzdíjak útján. ***Az ENISA további forrásokat kap a(z) XX/XXX rendeletben (kiberbiztonsági szolidaritásról szóló jogszabály) meghatározott további feladatai ellátásához. E kiegészítő finanszírozás nem veszélyeztetheti a program célkitűzéseinek elérését.***

Or. en

Módosítás 209
Evžen Tošenovský

Rendeletre irányuló javaslat
19 cikk – 1 bekezdés – 5 pont
Az (EU) 2021/694 rendelet
19 cikk

A Bizottság által javasolt szöveg	*Módosítás*
A vissza nem térítendő támogatásként nyújtott támogatást az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont a költségvetési rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti az XXXX rendelet 4. cikkében említett ***nemzeti biztonsági műveleti központoknak és az XXXX rendelet 5. cikkében említett üzemeltetési konzorciumnak***.	A vissza nem térítendő támogatásként nyújtott támogatást az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont a költségvetési rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti az XXXX rendelet 4. cikkében említett ***számítógép-biztonsági eseményekre reagáló csoportoknak, az információmegosztó és -elemző központoknak***.

Or. en

Módosítás 210
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
20 cikk – cím

A Bizottság által javasolt szöveg	*Módosítás*
Értékelés	Értékelés ***és felülvizsgálat***

Or. en

Módosítás 211
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 [***két*** évvel e rendelet alkalmazásának kezdőnapját követően]-ig***, majd azt követően kétévente értékeli az e rendeletben meghatározott intézkedések működését, és*** jelentést nyújt be az Európai Parlamentnek és a Tanácsnak. ***Az értékelés különösen a következőkre terjed ki:*** ***a) a tagállamok részvétele az európai kiberpajzsban, beleértve a rendelet részeként létrehozott nemzeti és határokon átnyúló biztonsági műveleti központok száma és az információcsere hatékonysága;*** ***b) e rendelet hozzájárulása az Unió rezilienciájának és szuverenitásának megerősítéséhez, az érintett ágazatok – köztük a kkv-k – versenyképességének javításához, valamint a kiberbiztonsági készségek fejlesztéséhez az EU-ban;*** ***c) a kiberbiztonsági tartalék felhasználása, beleértve azt is, hogy a tartalék hatályát ki kell-e terjeszteni a biztonsági eseményekre való felkészülési szolgáltatásokra vagy a megbízható szolgáltatókkal és a kiberbiztonsági tartalék potenciális felhasználóival közös gyakorlatokra a tartalék szükség szerinti hatékony működésének biztosítása érdekében;*** ***d) e rendelet hozzájárulása a kiberbiztonsági ágazatban dolgozó munkaerő azon készségeinek és kompetenciáinak fejlesztéséhez és javításához, amelyek az Unió kiberbiztonsági fenyegetések és események észlelésére, megelőzésére, az azokra való reagálásra és az azokat követő helyreállításra irányuló képességének megerősítéséhez szükségesek;*** ***e) e rendelet hozzájárulása a legkorszerűbb technológiák Unión belüli bevezetéséhez és fejlesztéséhez;***

E jelentés alapján a Bizottság adott esetben jogalkotási javaslatot nyújt be a Parlamentnek és a Tanácsnak e rendelet módosítása céljából.

Or. en

Módosítás 212
Evžen Tošenovský

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 [négy évvel e rendelet alkalmazásának kezdőnapját követően]-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet értékeléséről és felülvizsgálatáról. ***A jelentéshez szükség esetén jogalkotási javaslatot mellékel.***

Or. en

Módosítás 213
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

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

A Bizottság által javasolt szöveg	*Módosítás*
	A Bizottság minden évben, a következő évre vonatkozó költségvetési tervezet előterjesztésekor részletes értékelést nyújt be az ENISA e rendelet szerinti, valamint [a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről szóló javaslatban] és más uniós jogszabályokban meghatározott feladatairól, és részletesen felsorolja az e feladatok ellátásához szükséges pénzügyi és emberi erőforrásokat.

Or. en

Módosítás 214
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Rendeletre irányuló javaslat
20 a cikk (új)

A Bizottság által javasolt szöveg	*Módosítás*
	20a. cikk
	A felhatalmazás gyakorlása
	1. A felhatalmazáson alapuló jogi aktusok elfogadására vonatkozóan a Bizottság részére adott felhatalmazás feltételeit ez a cikk határozza meg.
	2. A Bizottságnak a 12. cikk (8) bekezdésében és a 13. cikk (7) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól ...-tól/-től [az alap jogalkotási aktus hatálybalépésének időpontja vagy a társjogalkotók által megállapított bármely más időpont] kezdődő hatállyal. A Bizottság legkésőbb kilenc hónappal az ötéves időtartam letelte előtt jelentést készít a felhatalmazásról. A felhatalmazás hallgatólagosan meghosszabbodik a korábbival megegyező időtartamra, amennyiben az Európai Parlament vagy a Tanács nem ellenzi a meghosszabbítást legkésőbb három hónappal minden egyes időtartam letelte előtt.
	3. Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 12. cikk (8) bekezdésében és a 13. cikk (7) bekezdésében említett felhatalmazást. A visszavonásról szóló határozat megszünteti az abban meghatározott felhatalmazást. A határozat az Európai Unió Hivatalos Lapjában való kihirdetését követő napon, vagy a benne megjelölt későbbi időpontban lép hatályba. A határozat nem érinti a már hatályban lévő, felhatalmazáson alapuló jogi aktusok érvényességét.

4. A felhatalmazáson alapuló jogi aktus elfogadása előtt a Bizottság a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban foglalt elveknek megfelelően konzultál az egyes tagállamok által kijelölt szakértőkkel.

5. A Bizottság a felhatalmazáson alapuló jogi aktus elfogadását követően haladéktalanul és egyidejűleg értesíti arról az Európai Parlamentet és a Tanácsot.

6. A 12. cikk (8) bekezdése és a 13. cikk (7) bekezdése értelmében elfogadott, felhatalmazáson alapuló jogi aktus csak akkor lép hatályba, ha az Európai Parlamentnek és a Tanácsnak a jogi aktusról való értesítését követő két hónapon belül sem az Európai Parlament, sem a Tanács nem emelt ellene kifogást, illetve, ha az említett időtartam lejártát megelőzően mind az Európai Parlament, mind a Tanács arról tájékoztatta a Bizottságot, hogy nem fog kifogást emelni. Ez az időtartam az Európai Parlament vagy a Tanács kezdeményezésére [két hónappal] meghosszabbodik.

Or. en

Módosítás 215
Evžen Tošenovský

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 1 pont
Az (EU) 2021/694 rendelet
I melléklet – „3 egyedi célkitűzés – Kiberbiztonság és bizalom” fejezet

A Bizottság által javasolt szöveg	*Módosítás*
1. A tagállamokkal közös beruházások fejlett kiberbiztonsági berendezésekbe, infrastruktúrákba és know-how-ba, amelyek alapvető fontosságúak a kritikus infrastruktúrák és általában a digitális egységes piac védelméhez. Az ilyen közös beruházások körébe tartozhatnak a	1. A tagállamokkal közös beruházások fejlett kiberbiztonsági berendezésekbe, infrastruktúrákba és know-how-ba, amelyek alapvető fontosságúak a kritikus infrastruktúrák és általában a digitális egységes piac védelméhez. Az ilyen közös beruházások körébe tartozhatnak a

kvantum-létesítményekbe és a kiberbiztonságot szolgáló adatforrásokba, a kibertérbeli helyzetismeretbe – beleértve az Európai Kiberpajzsot alkotó nemzeti ***biztonsági műveleti központokat és a határokon átnyúló*** biztonsági műveleti központokat –, valamint egyéb olyan eszközökbe történő befektetések, amelyeket az állami és magánszektor rendelkezésére kell bocsátani egész Európában.	kvantum-létesítményekbe és a kiberbiztonságot szolgáló adatforrásokba, a kibertérbeli helyzetismeretbe – beleértve az Európai Kiberpajzsot alkotó nemzeti ***számítógép-biztonsági eseményekre reagáló csoportokat és a*** biztonsági műveleti központokat –, valamint egyéb olyan eszközökbe történő befektetések, amelyeket az állami és magánszektor rendelkezésére kell bocsátani egész Európában.

Or. en

Módosítás 216
Evžen Tošenovský

Rendeletre irányuló javaslat
I melléklet – 1 bekezdés – 1 pont
Az (EU) 2021/694 rendelet
I melléklet – „3 egyedi célkitűzés – Kiberbiztonság és bizalom” fejezet

A Bizottság által javasolt szöveg	*Módosítás*
5. A tagállamok közötti szolidaritás előmozdítása a jelentős kiberbiztonsági eseményekre való felkészülés és reagálás terén a kiberbiztonsági szolgáltatások határokon átnyúló bevezetése révén, beleértve a hatóságok közötti kölcsönös segítségnyújtás támogatását és a ***megbízható kiberbiztonsági*** szolgáltatókból álló uniós szintű tartalék létrehozását.	5. A tagállamok közötti szolidaritás előmozdítása a jelentős kiberbiztonsági eseményekre való felkészülés és reagálás terén a kiberbiztonsági szolgáltatások határokon átnyúló bevezetése révén, beleértve a hatóságok közötti kölcsönös segítségnyújtás támogatását és a ***irányított biztonsági szolgáltatásokat nyújtó, megbízható*** szolgáltatókból álló uniós szintű tartalék létrehozását.***;***

Or. en