EURÓPAI UNIÓ

AZ EURÓPAI PARLAMENT **A TANÁCS**

Brüsszel, 2024. december 19.
(OR. en)

2023/0109(COD)
LEX 2422

PE-CONS 94/1/24
REV 1

CYBER 208
TELECOM 218
CADREFIN 109
FIN 595
BUDGET 47
IND 328
JAI 1084
MI 633
DATAPROTECT 247
RELEX 881
CODEC 1588

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE A KIBERFENYEGETÉSEK ÉS -ESEMÉNYEK ÉSZLELÉSE, VALAMINT AZ AZOKRA VALÓ FELKÉSZÜLÉS ÉS REAGÁLÁS ÉRDEKÉBEN AZ UNIÓN BELÜLI SZOLIDARITÁS ÉS KÉPESSÉGEK MEGERŐSÍTÉSÉT CÉLZÓ INTÉZKEDÉSEK MEGHATÁROZÁSÁRÓL, ÉS AZ (EU) 2021/694 RENDELET MÓDOSÍTÁSÁRÓL (A KIBERSZOLIDARITÁSRÓL SZÓLÓ RENDELET)

AZ EURÓPAI PARLAMENT ÉS A TANÁCS
(EU) 2024/... RENDELETE

(2024. december 19.)

a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról, és az (EU) 2021/694 rendelet módosításáról
(a kiberszolidaritásról szóló rendelet)

AZ EURÓPAI PARLAMENT ÉS AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 173. cikke (3) bekezdésére és 322. cikke (1) bekezdésének a) pontjára,

tekintettel az Európai Bizottság javaslatára,

a jogalkotási aktus tervezete nemzeti parlamenteknek való megküldését követően,

tekintettel a Számvevőszék véleményére[1],

tekintettel az Európai Gazdasági és Szociális Bizottság véleményére[2],

tekintettel a Régiók Bizottságának véleményére[3],

rendes jogalkotási eljárás keretében[4],

---

1 2023. április 18-i vélemény (a Hivatalos Lapban még nem tették közzé).
2 HL C 349., 2023.9.29., 167. o.
3 HL C, C/2024/1049., 2024.02.9., ELI: https://eur-lex.europa.eu/eli/C/2024/1049/oj?locale=hu
4 Az Európai Parlament 2024. április 24-i álláspontja (a Hivatalos Lapban még nem tették közzé) és a Tanács 2024. december 2-i határozata.

mivel:

(1) A tagállami közigazgatási szervek, vállalkozások és polgárok folyamatosan növekvő, ágazatok közötti és határokon átnyúló összekapcsoltságának és egymástól való függésének fényében az információs és kommunikációs technológiák alkalmazása és az azoktól való függés alapvetően fontos tényezővé vált a gazdasági tevékenységek és a társadalom valamennyi ágazatában, ezzel egyidejűleg lehetséges sebezhetőségeket eredményezve.

(2) A kiberbiztonsági események nagyságrendje, gyakorisága és hatása egyre számottevőbb Unió-szerte és globális szinten is, ideértve az ellátási láncok ellen elkövetett, kiberkémkedést, zsarolóvírus 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 Unió kiberbiztonsági keretének fokozott felkészültségét követeli meg. Ez a veszély túlmutat Oroszország Ukrajna elleni agressziós háborúján, és tekintettel a jelenlegi geopolitikai feszültségekben közreműködő körök sokféleségére, valószínűleg nem fog alábbhagyni. Az ilyen események akadályozhatják a közszolgáltatások nyújtását, mivel a kibertámadások gyakran a helyi, regionális vagy nemzeti közszolgáltatások és infrastruktúrák ellen irányulnak, a helyi hatóságok pedig különösen kiszolgáltatottak, többek között korlátozott erőforrásaik miatt. Akadályozhatják továbbá a gazdasági tevékenységek folytatását, többek között a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban, jelentős pénzügyi veszteségeket okozhatnak, alááshatják a felhasználói bizalmat, jelentős károkat okozhatnak az uniós gazdaságnak és az Unió demokratikus rendszereinek, sőt egészségügyi vagy az emberi életet veszélyeztető következményekkel is járhatnak. Ezenkívül a kiberbiztonsági események kiszámíthatatlanok, mivel gyakran gyorsan alakulnak ki és eszkalálódnak, nem korlátozódnak egy adott földrajzi területre, hiszen több országot érintően egyidejűleg is előfordulhatnak vagy gyorsan terjedhetnek. Fontos a közszféra, a magánszektor, a tudományos élet, a civil társadalom és a média közötti szoros együttműködés.

(3) Az Európa jövőjéről szóló konferencia három különböző javaslatának megfelelően meg kell erősíteni az uniós ipar és szolgáltatás versenyhelyzetét a digitalizált gazdaságban, és támogatni kell digitális átalakulásukat a digitális egységes piacon a kiberbiztonság szintjének megerősítése révén. Növelni kell a polgárok, a vállalkozások – köztük a mikrovállalkozások, a kis- és középvállalkozások, valamint az induló innovatív vállalkozások, továbbá a kritikus infrastruktúrákat működtető szervezetek – ellenálló képességét a növekvő kiberfenyegetésekkel szemben, amelyek pusztító társadalmi és gazdasági hatásokkal járhatnak. Ezért olyan infrastruktúrákba és szolgáltatásokba, valamint a kiberbiztonsági készségek fejlesztéséhez szükséges képességek kiépítésébe történő beruházásokra van szükség, amelyek támogatják a kiberfenyegetések és -események gyorsabb észlelését és az azokra való gyorsabb reagálást. Emellett a tagállamoknak segítségre van szükségük ahhoz, hogy jobban felkészüljenek és hatékonyabban reagáljanak a jelentős és a nagyszabású kiberbiztonsági eseményekre, valamint az azokat követő helyreállítás megkezdéséhez. A meglévő struktúrákra építve és azokkal szoros együttműködésben az Uniónak növelnie kell kapacitásait ezeken a területeken, különösen a kiberfenyegetésekre és -eseményekre vonatkozó adatok gyűjtése és elemzése tekintetében.

(4) Az Unió már számos intézkedést hozott a kritikus infrastruktúrák és a kritikus szervezetek kockázatokkal szembeni sebezhetőségének csökkentése és fokozott ellenálló képességének érdekében, ezek közé tartozik különösen az (EU) 2019/881 európai parlamenti és tanácsi rendelet[5], az 2013/40/EU[6] és az (EU) 2022/2555[7] európai parlamenti és tanácsi irányelv és az (EU) 2017/1584 bizottsági ajánlás[8]. Ezen túlmenően a kritikus infrastruktúrák ellenálló képességének megerősítését célzó összehangolt uniós megközelítésről szóló, 2022. december 8-i tanácsi ajánlás felkéri a tagállamokat, hogy hozzanak intézkedéseket, továbbá hogy működjenek együtt egymással, a Bizottsággal és más érintett hatóságokkal, valamint az érintett szervezetekkel a belső piacon az alapvető szolgáltatások nyújtásához használt kritikus infrastruktúrák ellenálló képességének fokozása érdekében.

---

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

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

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

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

(5) A növekvő kiberbiztonsági kockázatok és az átfogóan komplex fenyegetettségi helyzet okán – amely egyértelműen azzal a kockázattal jár, hogy a biztonsági események gyorsan tovagyűrűzhetnek az egyik tagállamból a másikba, illetve valamely harmadik országból az Unióba – a kiberfenyegetések és -események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés, reagálás, valamint az azokat követő helyreállítás érdekében meg kell erősíteni az uniós szintű szolidaritást különösen a meglévő struktúrák képességeinek megerősítése révén. Továbbá, az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetések felkérték a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.

(6) A Bizottság és az Unió külügyi és biztonságpolitikai főképviselőjének az EU kibervédelmi politikájáról szóló, az Európai Parlamentnek és a Tanácsnak címzett, 2022. november 10-i közös közleménye bejelentette az uniós kiberszolidaritási kezdeményezést, amelynek céljai a biztonsági műveleti központok (a továbbiakban: SOC-k) alkotta uniós infrastruktúra kiépítésének előmozdítása révén a közös uniós észlelési, helyzetismereti és reagálási képességek megerősítése, a megbízható magánszolgáltatók szolgáltatásait igénybe vevő uniós szintű kiberbtartalék fokozatos kiépítésének támogatása, valamint a kritikus szervezetek uniós kockázatértékeléseken alapuló tesztelése a potenciális sebezhetőségek tekintetében.

(7) Unió-szerte meg kell erősíteni a kiberfenyegetések és -események észlelését és helyzetismeretét, valamint – a tagállamok és az Unió a jelentős és a nagyszabású kiberbiztonsági eseményekre való felkészültségét, azok megelőzését és az arra való reagálást szolgáló képességeinek javítása révén – meg kell erősíteni a szolidaritást is. Ezért létre kell hozni a kiberközpontok páneurópai hálózatát (a továbbiakban: Európai Kiberbiztonsági Riasztási Rendszer) az összehangolt észlelési és helyzetismereti képességek kiépítése érdekében, megerősítve az Unió fenyegetésészlelési és információmegosztási képességeit; létre kell hozni a kiberbiztonsági vészhelyzeti mechanizmust, amely kérésükre támogatja a tagállamokat a jelentős és a nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban, azok hatásainak mérséklésében és az azokat követő helyreállítás megkezdésében, valamint támogatja az egyéb felhasználókat a jelentős és a nagyszabású kiberbiztonsági eseményekre való reagálásban; és létre kell hozni az európai kiberbiztonsági események felülvizsgálati mechanizmusát konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából. Az e rendelet szerinti hozott intézkedéseket a tagállami hatáskörök kellő tiszteletben tartásával kell végrehajtani, és azoknak ki kell egészíteniük az (EU) 2022/2555 irányelv alapján létrehozott CSIRT-hálózat, az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (a továbbiakban: EU-CyCLONe) vagy az Együttműködési Csoport (a továbbiakban: Kiberbiztonsági Együttműködési Csoport) által végzett tevékenységeket, és nem kettőzhetik meg azokat. Ezek az intézkedések nem érintik az Európai Unió működéséről szóló szerződés (EUMSZ) 107. és 108. cikkét.

(8) E célkitűzések elérése érdekében bizonyos területeket érintően módosítani kell az (EU) 2021/694 európai parlamenti és tanácsi rendeletet[9]. Konkrétabban, e rendeletnek módosítania kell az (EU) 2021/694 rendeletet a tekintetben, hogy kiegészítse azt az Európai Kiberbiztonsági Riasztási Rendszerhez és a kiberbiztonsági vészhelyzeti mechanizmushoz kapcsolódó új operatív célkitűzésekkel, a Digitális Európa program 3. sz. egyedi célkitűzése szerint, amelynek célja a digitális egységes piac ellenálló képességének, integritásának és megbízhatóságának garantálása, a kibertámadások és -fenyegetések nyomon követésére és az azokra való reagálásra szolgáló képességek megerősítése, valamint a kiberbiztonsággal kapcsolatos, határokon átnyúló együttműködés és koordináció megerősítése. Az Európai Kiberbiztonsági Riasztási Rendszer fontos szerepet játszhat abban, hogy támogassa a tagállamokat a kiberfenyegetések előrejelzésében és az azokkal szembeni védekezésben, az uniós kiberbiztonsági tartalék pedig fontos szerepet játszhat a tagállamok, az uniós intézmények, szervek, hivatalok és ügynökségek, valamint a Digitális Európa programhoz társult harmadik országok támogatásában a jelentős, a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági események hatásainak kezelésében és mérséklésében. E hatások közé tartozhatnak jelentős anyagi vagy nem vagyoni károk, valamint súlyos közbiztonsági és biztonsági kockázatok. Tekintettel azokra a konkrét szerepekre, amelyeket az Európai Kiberbiztonsági Riasztási Rendszer és az uniós kiberbiztonsági tartalék játszhat, e rendeletnek módosítania kell az (EU) 2021/694 rendeletet az Unióban letelepedett, de harmadik országokból irányított jogalanyok részvétele tekintetében, amennyiben valós a kockázata annak, hogy a szükséges és elégséges eszköz, infrastruktúra és szolgáltatás, illetve technológia, szakértelem és kapacitás nem áll rendelkezésre az Unióban, és az ilyen szervezetek bevonásának előnyei meghaladják a biztonsági kockázatot. Meg kell határozni azokat a konkrét feltételeket, amelyek mellett pénzügyi támogatás nyújtható az Európai Kiberbiztonsági Riasztási Rendszert és az uniós kiberbiztonsági tartalékot végrehajtó intézkedésekhez, és meg kell határozni a kitűzött célok eléréséhez szükséges irányítási és koordinációs mechanizmusokat. Az (EU) 2021/694 rendelet egyéb módosításai ismertetik az új operatív célkitűzések keretében javasolt intézkedéseket, valamint az új operatív célkitűzések végrehajtásának nyomon követésére szolgáló mérhető mutatókat.

---

[9] Az Európai Parlament és a Tanács (EU) 2021/694 rendelete (2021. április 29.) a Digitális Európa program létrehozásáról és az (EU) 2015/2240 határozat hatályon kívül helyezéséről (HL L 166., 2021.5.11., 1. o.).

(9) A kiberfenyegetésekre és eseményekre adott uniós válasz megerősítése érdekében létfontosságú a nemzetközi szervezetekkel, valamint a megbízható, hasonlóan gondolkodó nemzetközi partnerekkel folytatott együttműködés. Ebben az összefüggésben a megbízható, hasonlóan gondolkodó nemzetközi partnerek alatt olyan országokat kell érteni, amelyek osztják azokat az elveket, amelyek az Unió létrehozását vezérelték, nevezetesen a demokrácia, a jogállamiság, az emberi jogok és alapvető szabadságok egyetemes és oszthatatlan volta, az emberi méltóság tiszteletben tartása, az egyenlőség és a szolidaritás elve, valamint az Egyesült Nemzetek Alapokmányában foglalt elvek és a nemzetközi jog tiszteletben tartása, és amelyek nem ássák alá az Unió vagy tagállamai alapvető biztonsági érdekeit. Ez az együttműködés az e rendelet szerint hozott intézkedések, különösen az Európai Kiberbiztonsági Riasztási Rendszer és az uniós kiberbiztonsági tartalék tekintetében is előnyös lehet. Az (EU) 2021/694 rendeletnek az Európai Kiberbiztonsági Riasztási Rendszer és az uniós kiberbiztonsági tartalék tekintetében elő kell írnia, hogy bizonyos rendelkezésre állási és biztonsági feltételek teljesülése esetén az Európai Kiberbiztonsági Riasztási Rendszerre és az uniós kiberbiztonsági tartalékra vonatkozó pályázatok – a biztonsági követelmények betartása mellett – nyitva legyenek harmadik országokból irányított jogalanyok előtt. A közbeszerzés ilyen módon történő megnyitásával kapcsolatos biztonsági kockázat értékelésekor fontos figyelembe venni azokat az elveket és értékeket, amelyek közösek az Unió és a hasonlóan gondolkodó nemzetközi partnerek között, amennyiben ezek az elvek és értékek az Unió alapvető biztonsági érdekeihez kapcsolódnak. Emellett, amikor az (EU) 2021/694 rendelet keretében ilyen biztonsági követelményeket mérlegelnek, több elemet is figyelembe lehet venni, például a szervezet szervezeti felépítését és döntéshozatali eljárását, az adatok és a minősített vagy érzékeny információk biztonságát, valamint annak biztosítását, hogy az intézkedés eredményeit a nem jogosult harmadik országok ne ellenőrizhessék és ne korlátozhassák.

(10) Az e rendelet szerinti intézkedések finanszírozásáról az (EU) 2021/694 rendelet rendelkezik, amely változatlanul a Digitális Európa program 3. sz. egyedi célkitűzésében foglalt intézkedések releváns alap-jogiaktusának számít. Az (EU) 2021/694 rendelettel összhangban a vonatkozó munkaprogramok határozzák meg az egyes intézkedések egyedi részvételi feltételeit.

(11) Erre a rendeletre az Európai Parlament és a Tanács által az EUMSZ 322. cikke alapján elfogadott horizontális költségvetési szabályok alkalmazandók. E szabályokat az (EU, Euratom) 2024/2509 európai parlamenti és tanácsi rendelet[10] állapítja meg, és e szabályok meghatározzák különösen az uniós költségvetés elkészítésére és végrehajtására vonatkozó eljárást, továbbá rendelkeznek a pénzügyi szereplők felelősségével kapcsolatos ellenőrzésekről. Az EUMSZ 322. cikke alapján elfogadott szabályok az uniós költségvetés védelmét szolgáló, az (EU, Euratom) 2020/2092 európai parlamenti és tanácsi rendeletben[11] meghatározott általános feltételrendszert is magukban foglalják.

---

[10] Az Európai Parlament és a Tanács (EU, Euratom) 2024/2509 rendelete (2024. szeptember 23.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról (HL L 2024/2509, 2024.9.26., 1. o., ELI: http://data.europa.eu/eli/reg/2024/2509/oj).

[11] Az Európai Parlament és a Tanács (EU, Euratom) 2020/2092 rendelete (2020. december 16.) az uniós költségvetés védelmét szolgáló általános feltételrendszerről (HL L 433. I, 2020.12.22., 1. o., ELI: http://data.europa.eu/eli/reg/2020/2092/oj?locale=hu).

(12) Bár a megelőzési és felkészültségi intézkedések elengedhetetlenek ahhoz, hogy az Unió ellenállóbbá váljon a jelentős kiberbiztonsági eseményekkel, a nagyszabású kiberbiztonsági eseményekkel és a nagyszabásúval egyenértékű kiberbiztonsági eseményekkel való szembenézés terén, az ilyen események előfordulása, időzítése és nagyságrendje jellegénél fogva kiszámíthatatlan. A megfelelő reagálás biztosításához szükséges pénzügyi források évről évre jelentősen eltérhetnek, és azokat azonnal rendelkezésre kell bocsátani. Ezért a kiszámíthatóság költségvetési elvének az új igényekre való gyors reagálás szükségességével való összeegyeztetéséhez a munkaprogramok pénzügyi végrehajtásának kiigazítására van szükség. Következésképpen helyénvaló engedélyezni a fel nem használt előirányzatoknak a csak a következő évre és csak az uniós kiberbiztonsági tartalékra és a kölcsönös segítségnyújtást támogató intézkedésekre történő átvitelét, az (EU, Euratom) 2024/2509 rendelet 12. cikkének (4) bekezdése szerint engedélyezett előirányzatok átvitelén felül.

(13) A kiberfenyegetések 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. A kiberfenyegetések azonosítására, mérséklésére és megelőzésére irányuló proaktív megközelítés magában foglalja a fejlett észlelési képességek kapacitásának növelését. Az Európai Kiberbiztonsági Riasztási Rendszernek több, határokon átnyúló kiberközpontból kell állnia, amelyek mindegyike három vagy több nemzeti kiberközpontot tömörít. Ennek az infrastruktúrának a nemzeti és uniós kiberbiztonsági érdekeket és igényeket kell szolgálnia, felhasználva a legkorszerűbb technológiát a releváns és adott esetben anonimizált adatok és információk fejlett gyűjtéséhez és elemzési eszközökhöz az összehangolt kiberészlelési és -kezelési képességek megerősítéséhez, valamint a valós idejű helyzetismeret biztosításához. Ennek az infrastruktúrának a kiberhelyzet javítását kell szolgálnia az adatok és információk észlelésének, összesítésének és elemzésének fokozása révén a kiberfenyegetések és -események megelőzése céljából, és ezáltal ki kell egészítenie és támogatnia kell az uniós kiberválság-kezelésért felelős uniós szervezeteket és hálózatokat, különösen az EU-CyCLONe-t.

(14) Az Európai Kiberbiztonsági Riasztási Rendszerben való részvétel önkéntes a tagállamok számára. Minden tagállamnak ki kell jelölnie egyetlen nemzeti szintű szervezetet, amelynek feladata a kiberfenyegetés-észlelési tevékenységek összehangolása az adott tagállamban. Ezeknek a nemzeti kiberközpontoknak nemzeti szinten referenciapontként és átjáróként kell szolgálniuk az Európai Kiberbiztonsági Riasztási Rendszerben való részvételhez, és biztosítaniuk kell, hogy az állami és magánszervezetektől származó, kiberfenyegetettséggel kapcsolatos információkat nemzeti szinten hatékonyan és egységesen osszák meg és gyűjtsék össze. A nemzeti kiberközpontok megerősíthetik a köz- és magánszervezetek közötti együttműködést és információmegosztást, és támogathatják a releváns adatoknak és információknak az érintett ágazati és ágazatközi közösségekkel, többek között az érintett ágazati információmegosztó és -elemző központokkal (a továbbiakban: ISAC) való cseréjét. Az állami és magánszervezetek közötti szoros és összehangolt együttműködés központi szerepet játszik az Unió kiberellenálló képességének megerősítésében. Ez az együttműködéskülönösen értékes a kiberfenyegetettség felderítés megosztásának összefüggésében az aktív kibervédelem javítása érdekében. Ezen együttműködés és információmegosztás részeként a nemzeti kiberközpontok konkrét információkat kérhetnek és kaphatnak. E nemzeti kiberközpontokat ez a rendelet nem kötelezi és nem is hatalmazza fel az ilyen megkeresések érvényesítésére. Adott esetben, valamint az uniós és a nemzeti joggal összhangban a kért vagy kapott információk magukban foglalhatják az adott tagállamon belül kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetektől – például irányított biztonsági szolgáltatóktól – származó telemetriai, érzékelő- és naplózási adatokat annak érdekében, hogy a potenciális kiberfenyegetések és -események korábbi szakaszban történő gyors észlelése javuljon, ezáltal javítva a helyzetismeretet. Ha a nemzeti kiberközpont nem az érintett tagállam által az (EU) 2022/2555 irányelv 8. cikkének (1) bekezdése szerint kijelölt vagy létrehozott illetékes hatóság, alapvető fontosságú, hogy együttműködjön az említett illetékes hatósággal az ilyen adatkérések és -fogadások tekintetében.

(15) Az Európai Kiberbiztonsági Riasztási Rendszer részeként számos határokon átnyúló kiberközpontot kell létrehozni. A határokon átnyúló fenyegetések észlelése, valamint az információmegosztás és -kezelés előnyeinek teljes körű kiaknázása érdekében ezeknek a határokon átnyúló kiberközpontoknak legalább három tagállam nemzeti kiberközpontjából kell állniuk. A határokon átnyúló kiberközpontok általános célkitűzése a kiberfenyegetések elemzésére, megelőzésére és észlelésére szolgáló kapacitások megerősítése, valamint a magas színvonalú kiberfenyegetettség felderítés előállításának támogatása kell, hogy legyen, elsősorban releváns és adott esetben anonimizált információk megbízható és biztonságos környezetben, a különböző – köz- vagy magánforrásokból származó – adatok megosztása, a legkorszerűbb eszközök megosztása és közös használata, valamint az észlelési, elemzési és megelőzési képességek megbízható és biztonságos környezetben történő közös fejlesztése révén. A határokon átnyúló kiberközpontoknak új, kiegészítő kapacitást kell biztosítaniuk a meglévő SOC-okra és CSIRT-ekre és más érintett szereplőkre, többek között a CSIRT-ek hálózatára építve és azokat kiegészítve.

(16) Az (EU) 2021/887 európai parlamenti és tanácsi rendelettel[12] létrehozott Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) által a nemzeti kiberközpont létrehozására vagy kapacitásainak fejlesztésére irányuló részvételi szándék kifejezésére való felhívást követően kiválasztott tagállamnak az ECCC-vel közösen kell beszereznie a releváns eszközöket, infrastruktúrákat vagy szolgáltatásokat. Az ilyen tagállamoknak jogosultaknak kell lenniük arra, hogy támogatásban részesüljenek az eszközök, infrastruktúrák vagy szolgáltatások működtetéséhez. Az ECCC által a részvételi szándék kifejezésére való felhívást követően határokon átnyúló kiberközpont létrehozására vagy kapacitásainak fejlesztésére kiválasztott, legalább három tagállamból álló üzemeltetési konzorciumnak az ECCC-vel közösen kell beszereznie a releváns eszközöket, infrastruktúrát vagy szolgáltatásokat. Az üzemeltetési konzorciumnak jogosultnak kell lennie arra, hogy támogatásban részesüljön az eszközök, infrastruktúra vagy szolgáltatások működtetéséhez. A vonatkozó eszközök, infrastruktúra vagy szolgáltatások beszerzésére irányuló közbeszerzési eljárást az ECCC-nek és az adott részvételi szándék kifejezésére való felhívást követően kiválasztott tagállamok érintett ajánlatkérő szerveinek közösen kell lefolytatniuk. Az ilyen beszerzésnek meg kell felelnie az (EU, Euratom) 2024/2509 rendelet 168. cikke (2) bekezdésének és az ECCC pénzügyi szabályzatának. A magánszervezetek ezért nem lehetnek jogosultak arra, hogy részt vegyenek a részvételi szándék kifejezésére való felhívásokban, hogy az ECCC-vel közösen vásároljanak eszközöket, infrastruktúrákat vagy szolgáltatásokat, és nem kaphatnak támogatást ezen eszközök, infrastruktúrák vagy szolgáltatások működtetéséhez. A tagállamok számára azonban lehetővé kell tenni, hogy az uniós és a nemzeti joggal összhangban más, általuk megfelelőnek ítélt módon bevonják a magánszervezeteket nemzeti kiberközpontjaik és határokon átnyúló kiberközpontjaik létrehozásába, fejlesztésébe és működtetésébe. A magánszervezetek az (EU) 2021/887 rendelet szerint uniós finanszírozásra is jogosultak lehetnek a nemzeti kiberközpontok támogatása céljából.

---

[12] Az Európai Parlament és a Tanács (EU) 2021/887 rendelete (2021. május 20.) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról (HL L 202., 2021.6.8., 1. o.), ELI: http://data.europa.eu/eli/reg/2021/887/oj).

(17) Az Unión belüli kiberfenyegetések észlelésének és helyzetismeretének javítása érdekében a nemzeti kiberközpont létrehozására vagy képességeinek fejlesztésére irányuló részvételi szándék kifejezésére való felhívást követően kiválasztott tagállamoknak kötelezettséget kell vállalniuk arra, hogy pályáznak a határokon átnyúló kiberközpontban való részvételre. Amennyiben egy tagállam az eszközök, infrastruktúrák vagy szolgáltatások beszerzésének vagy a vissza nem térítendő támogatás igénybevételének időpontjától számított két éven belül – attól függően, hogy melyik következik be előbb – nem vesz részt egy határokon átnyúló kiberközpontban, nem lehet jogosult arra, hogy részt vegyen a nemzeti kiberközpont képességeinek fejlesztését célzó további, az Európai Kiberbiztonsági Riasztási Rendszer keretében hozott uniós támogatási intézkedésekben. Ilyen esetekben a tagállamok szervezetei továbbra is részt vehetnek a Digitális Európa program vagy más uniós finanszírozási programok keretében más témákra vonatkozó pályázati felhívásokban, ideértve a kiberészlelési és információmegosztási kapacitásokra vonatkozó felhívásokat is, feltéve, hogy ezek a szervezetek megfelelnek a programokban meghatározott támogathatósági kritériumoknak.

(18) A CSIRT-ek az (EU) 2022/2555 irányelvvel összhangban a CSIRT-ek hálózatában folytatnak információcserét. Az Európai Kiberbiztonsági Riasztási Rendszernek olyan új képességet kell képeznie, amely kiegészíti a CSIRT-ek hálózatát azáltal, hogy hozzájárul egy olyan uniós helyzetismeret kialakításához, amely lehetővé teszi a CSIRT-ek hálózata képességeinek megerősítését. A határokon átnyúló kiberközpontoknak szoros koordinációt és együttműködést kell folytatniuk a CSIRT-ek hálózatával. Úgy kell eljárniuk, hogy összegyűjtik az adatokat, és megosztják a köz- és magánszervezetektől származó kiberfenyegetésekre vonatkozó releváns és adott esetben anonimizált információkat, szakértői elemzések, valamint közösen beszerzett infrastruktúrák és legkorszerűbb eszközök révén növelik az ilyen adatok és információk értékét, továbbá hozzájárulnak az Unió technológiai szuverenitásához, nyitott stratégiai autonómiájához, versenyképességéhez és ellenálló képességéhez, valamint az uniós képességek fejlesztéséhez.

(19) A határokon átnyúló kiberközpontoknak olyan központi pontként kell működniük, amely lehetővé teszi a releváns adatok és kiberfenyegetettség felderítés kiterjedt gyűjtését, és a fenyegetettségre vonatkozó információk különféle érdekelt felek, mint például hálózatbiztonsági vészhelyzeteket elhárító csoportok (a továbbiakban: CERT), CSIRT-ek, ISAC-ok és a kritikus infrastruktúrák üzemeltetői közötti széles körű terjesztését. Az üzemeltetési konzorcium tagjainak a konzorciumi megállapodásban meg kell határozniuk az érintett, határokon átnyúló kiberközpont résztvevői között megosztandó releváns információkat. A határokon átnyúló kiberközpont résztvevői közötti információcsere kiterjedhet például a hálózatokból és érzékelőkből származó adatokra, a kiberfenyegetettségi információk hírcsatornáira, a fertőzöttségi mutatókra, valamint a kiberbiztonsági eseményekre, kiberfenyegetésekre, majdnem bekövetkezett eseményekre, sebezhetőségekre, technikákra és eljárásokra, kontradiktórius taktikákra, a fenyegetettségi szereplőkre vonatkozó konkrét információkra, kiberbiztonsági riasztásokra és a kibertámadások észlelésére szolgáló kiberbiztonsági eszközök konfigurációjára vonatkozó ajánlásokra. Emellett a határokon átnyúló kiberközpontoknak együttműködési megállapodásokat kell kötniük egymással is. Ezeknek az együttműködési megállapodásoknak különösen az információmegosztás elveit és az interoperabilitást kell meghatározniuk. Az interoperabilitásra vonatkozó záradékaiknak – különösen az információmegosztás formátumainak és protokoljainak – az (EU) 2019/881 rendelettel létrehozott Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által kiadott iránymutatásokon kell alapulniuk, és ezért azokat kiindulópontként kell tekinteniük. Ezeket az iránymutatásokat mielőbb ki kell adni annak biztosítása érdekében, hogy a határokon átnyúló kiberközpontok már korai szakaszban figyelembe vehessék azokat. Figyelembe kell venniük a nemzetközi szabványokat és a bevált gyakorlatokat és a határokon átnyúló kiberközpontok jelenlegi működését.

(20) A határokon átnyúló kiberközpontoknak és a CSIRT-ek hálózatának szorosan együtt kell működnie a szinergiák és a tevékenységek egymást kiegészítő jellegének biztosítása érdekében. E célból meg kell állapodniuk az együttműködésre és a releváns információk megosztására vonatkozó eljárási szabályokról. Ez magában foglalhatja a kiberfenyegetésekre és a jelentős kiberbiztonsági eseményekre vonatkozó releváns információk megosztását, valamint annak biztosítását, hogy a határokon átnyúló kiberközpontokban használt legkorszerűbb eszközökkel, különösen a mesterséges intelligenciával és az adatelemzési technológiával kapcsolatos tapasztalatokat megosszák a CSIRT-ek hálózatával.

(21) Az érintett hatóságok közösen kialakított helyzetismerete elengedhetetlen előfeltétele a jelentős és a 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. Az (EU) 2022/2555 irányelv a CSIRT-ek hálózatát is létrehozta a valamennyi tagállam közötti gyors és hatékony operatív együttműködés előmozdítása érdekében. A helyzetismeret biztosítása és a szolidaritás megerősítése érdekében azokban a helyzetekben, amikor a határokon átnyúló kiberközpontok egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről szereznek információt, releváns információkat kell szolgáltatniuk a CSIRT-ek hálózatának, és korai előrejelzésként tájékoztatniuk kell az EU-CyCLONe-t. A helyzettől függően a megosztandó információk közé tartozhatnak különösen a technikai információk, a támadó vagy potenciális támadó jellegére és szándékaira vonatkozó információk, valamint a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos magasabb szintű, nem technikai jellegű információk. Ebben az összefüggésben kellő figyelmet kell fordítani a szükséges ismeret elvére és a megosztott információk potenciálisan érzékeny jellegére. Az (EU) 2022/2555 irányelv ismételten hangsúlyozza a Bizottságnak az 1313/2013/EU európai parlamenti és tanácsi határozattal[13] létrehozott uniós polgári védelmi mechanizmussal (a továbbiakban: UCPM) kapcsolatos felelősségét is, valamint hogy a Bizottság felelőssége, hogy elemző jelentéseket készítsen az (EU) 2018/1993 tanácsi végrehajtási határozat[14] szerinti uniós politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR-mechanizmus) számára.

---

13 Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o., ELI: http://data.europa.eu/eli/dec/2013/1313/oj).

14 A Tanács (EU) 2018/1993 végrehajtási határozata (2018. december 11.) az uniós politikai szintű integrált válságelhárítási mechanizmusról (HL L 320., 2018.12.17., 28. o., ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).

Amikor a határokon átnyúló kiberközpontok megosztják az EU-CyCLONe-nal és a CSIRT-ek hálózatával a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos releváns információkat és korai figyelmeztetéseket, elengedhetetlen, hogy ezeket az információkat ezeken a hálózatokon keresztül megosszák a tagállami hatóságokkal és a Bizottsággal. E tekintetben az (EU) 2022/2555 irányelv előírja, hogy az EU-CyCLONe célja a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelésének támogatása, valamint a releváns információk tagállamok és az Unió intézményei, szervei, hivatalai és ügynökségei közötti rendszeres cseréjének biztosítása. Az EU-CyCLONe feladatai közé tartozik az ilyen eseményekre és válságokra vonatkozó közös helyzetismeret kialakítása. Rendkívül fontos, hogy az EU-CyCLONe e céllal és feladataival összhangban biztosítsa, hogy az ilyen információkat haladéktalanul eljuttassák az érintett tagállamok képviselőinek és a Bizottságnak. E célból alapvető fontosságú, hogy az EU-CyCLONe eljárási szabályzata megfelelő rendelkezéseket tartalmazzon.

(22) Az Európai Kiberbiztonsági Riasztási Rendszerben részt vevő szervezeteknek gondoskodniuk kell az egymás közötti magas szintű interoperabilitásról, beleértve adott esetben az adatformátumokat, a taxonómiát, az adatkezelésre és az adatelemzésre szolgáló eszközöket. Gondoskodniuk kell továbbá a biztonságos kommunikációs csatornákról, az alkalmazási réteg minimális biztonsági szintjéről, a helyzetismereti jelzőrendszerről és a mutatókról. A közös taxonómia elfogadása és az észlelt kiberfenyegetések és -kockázatok okait leíró helyzetjelentés-minta kidolgozása során figyelembe kell venni az (EU) 2022/2555 irányelv végrehajtásával összefüggésben már elvégzett munkát.

(23) Annak érdekében, hogy a különböző forrásokból származó, kiberfenyegetésekkel kapcsolatos adat- és információcserére széles körben és megbízható környezetben kerülhessen sor, az Európai Kiberbiztonsági Riasztási Rendszerben részt vevő szervezeteket a legkorszerűbb, rendkívül biztonságos eszközökkel, berendezésekkel és infrastruktúrákkal kell felszerelni, valamint 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.

(24) A releváns adatok és információk gyűjtése, elemzése, megosztása és cseréje révén az Európai Kiberbiztonsági Riasztási Rendszernek meg kell erősítenie az Unió technológiai szuverenitását és nyitott stratégiai autonómiáját a kiberbiztonság, a versenyképesség és az ellenálló képesség területén. A kiváló minőségű rendszerezett adatok összevonása hozzájárulhat a fejlett mesterségesintelligencia- és adatelemzési technológiák fejlesztéséhez is. Az emberi felügyelet és e célból a képzett munkaerő továbbra is elengedhetetlen a jó minőségű adatok hatékony összegyűjtéséhez.

(25) Jóllehet az Európai Kiberbiztonsági Riasztási Rendszer polgári projekt, a kibervédelmi közösség számára is előnyt jelenthetnek a kritikus infrastruktúrák védelmére kifejlesztett, erősebb polgári észlelési és helyzetismereti képességek.

(26) Az Európai Kiberbiztonsági Riasztási Rendszer résztvevői közötti információmegosztásnak meg kell felelnie a meglévő jogi követelményeknek, különösen az uniós és nemzeti adatvédelmi jognak, valamint az információcserére irányadó uniós versenyjogi szabályoknak. Amennyiben személyes adatok kezelésére is szükség van, az információ címzettjének olyan technikai és szervezeti intézkedéseket kell végrehajtania, amelyek védik az érintettek jogait és szabadságait, és amint az adatok a megjelölt célból már nem szükségesek, meg kell azokat semmisítenie, majd tájékoztatnia kell az adatokat rendelkezésre bocsátó szervezetet arról, hogy az adatokat megsemmisítették.

(27) A titoktartás és az információbiztonság megőrzése kiemelkedő fontosságú e rendelet mindhárom pillére szempontjából, legyen szó akár az Európai Kiberbiztonsági Riasztási Rendszer keretében történő információmegosztás és -csere ösztönzéséről, a kiberbiztonsági szükséghelyzeti mechanizmus keretében támogatást igénylő szervezetek érdekeinek védelméről, akár annak biztosításáról, hogy az európai kiberbiztonsági események felülvizsgálati mechanizmusa keretében tett bejelentésekből hasznos tanulságokat vonhassanak le anélkül, hogy negatív hatást gyakorolnának az események által érintett szervezetekre. A tagállamok és a szervezetek e mechanizmusokban való részvétele az összetevőik közötti bizalmi viszonytól függ. Amennyiben az információk az uniós vagy nemzeti szabályok értelmében bizalmasak, az e rendelet szerinti információmegosztást vagy -cserét a megosztás vagy csere céljára vonatkozó és azzal arányos mértékre kell korlátozni. Ennek az információmegosztásnak vagy -cserének meg kell őriznie ezen információk bizalmas jellegét is, beleértve az érintett szervezetek biztonsági és kereskedelmi érdekeinek védelmét is. Az e rendelet szerinti információmegosztás vagy -csere történhet titoktartási megállapodások vagy az információterjesztésre vonatkozó iránymutatás, például a jelzőlámpa-protokoll (a továbbiakban: TLP) alkalmazásával. A TLP-t olyan eszközként kell értelmezni, amely arra szolgál, hogy tájékoztatást nyújtson az információk további terjesztésének korlátairól. Szinte valamennyi CSIRT-ben és egyes ISAC-kban használják. Ezen általános követelmények mellett az Európai Kiberbiztonsági Riasztási Rendszer tekintetében az üzemeltetési konzorciumokra vonatkozó megállapodásoknak konkrét szabályokat kell megállapítaniuk az érintett, határokon átnyúló kiberközponton belüli információmegosztás feltételeire vonatkozóan. Ezek a megállapodások különösen azt írhatják elő, hogy az információmegosztás kizárólag az uniós és a nemzeti joggal összhangban történjen.

(28) Az uniós kiberbiztonsági tartalék bevezetése tekintetében egyedi titoktartási szabályokra van szükség. A támogatás igénylésére, értékelésére és nyújtására válsághelyzetben, valamint az érzékeny ágazatokban működő szervezetek tekintetében kerül sor. Az uniós kiberbiztonsági tartalék hatékony működéséhez elengedhetetlen, hogy a felhasználók és a szervezetek képesek legyenek haladéktalanul megosztani és hozzáférést biztosítani minden olyan információhoz, amely ahhoz szükséges, hogy az egyes szervezetek részt tudjanak venni a kérelmek értékelésében és a támogatás kiépítésében. Ennek megfelelően e rendeletnek elő kell írnia, hogy minden ilyen információt csak akkor lehet felhasználni vagy megosztani, ha az az uniós kiberbiztonsági tartalék működéséhez szükséges, és hogy az uniós és a nemzeti jog szerint bizalmas vagy minősített információkat kizárólag az említett jognak megfelelően szabad felhasználni és megosztani. Emellett a felhasználók számára mindig lehetővé kell tenni, hogy adott esetben információmegosztási protokollokat, például TLP-t használjanak a korlátozások további meghatározására. Bár a felhasználók mérlegelési jogkörrel rendelkeznek e tekintetben, fontos, hogy e korlátozások alkalmazásakor figyelembe vegyék a lehetséges következményeket, különösen a kért szolgáltatások késedelmes értékelése vagy nyújtása tekintetében. A hatékony uniós kiberbiztonsági tartalék létrehozása érdekében fontos, hogy az ajánlatkérő szerv a kérelem benyújtása előtt tisztázza ezeket a következményeket a felhasználó számára. Ezek a biztosítékok az uniós kiberbiztonsági tartalék szolgáltatásainak igénylésére és nyújtására korlátozódnak, és nem érintik a más összefüggésben, például az uniós kiberbiztonsági tartalék keretén belüli beszerzésekkel kapcsolatos információcserét.

(29) Tekintettel arra, hogy a tagállamokat érintő események egyre nagyobb kockázatot jelentenek és egyre gyakoribbak, létre kell hozni egy válsághelyzetek kezelését célzó támogatási eszközt, nevezetesen a kiberbiztonsági vészhelyzeti mechanizmust, amely javítja az Unió jelentős, nagyszabású és nagyszabásúval egyenértékű kiberbiztonsági eseményekkel szembeni ellenálló képességet, és a felkészültséghez, az eseményekre történő reagáláshoz és az alapvető szolgáltatások helyreállításának megkezdéséhez nyújtott vészhelyzeti pénzügyi támogatás révén kiegészíti a tagállamok intézkedéseit. Mivel a biztonsági eseményt követő teljes helyreállítás az esemény által érintett szervezet működésének az esemény előtti állapotba való helyreállítására irányuló átfogó folyamat, amely hosszú és költséges lehet, az uniós kiberbiztonsági tartalékból származó támogatást a helyreállítási folyamat kezdeti szakaszára kell korlátozni, ami a rendszerek alapvető funkcióinak helyreállításához vezet. A kiberbiztonsági vészhelyzeti mechanizmusnak 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 az események és válsághelyzetek megelőzése, valamint az azokra való felkészülés és reagálás elsősorban a tagállamok feladata, a kiberbiztonsági vészhelyzeti mechanizmus az Európai Unióról szóló szerződés (EUSZ) 3. cikkének (3) bekezdésével összhangban előmozdítja a tagállamok közötti szolidaritást.

(30) A jelentős és a nagyszabású kiberbiztonsági eseményekre való reagálás alkalmával és azokat követő helyreállítás megkezdése során a kiberbiztonsági vészhelyzeti mechanizmusnak a tagállami intézkedéseket és erőforrásokat, valamint a rendelkezésre álló egyéb támogatási lehetőségeket – például az ENISA által a megbízatásával összhangban nyújtott szolgáltatásokat, a CSIRT-ek hálózata nyújtotta összehangolt reagálást és segítséget, az EU-CyCLONe mérséklési támogatását, valamint a tagállamok közötti, többek között az EUSZ 42. cikkének (7) bekezdésével összefüggésben és a (KKBP) 2017/2315 tanácsi határozattal[15] létrehozott állandó strukturált együttműködés (PESCO) kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportjaikeretében nyújtott kölcsönös segítségnyújtást – kiegészítve kell támogatnia a tagállamokat. A mechanizmusnak az igényekre reagálva biztosítania kell, hogy Unió-szerte és a Digitális Európa programhoz társult harmadik országokban speciális eszközök álljanak rendelkezésre, amelyek támogatják az ilyen eseményekre való felkészültséget, reagálást, és az azokat követő helyreállítást.

[15] A Tanács (KKBP) 2017/2315 határozata (2017. december 11.) az állandó strukturált együttműködés (PESCO) létrehozásáról és a részt vevő tagállamok jegyzékének meghatározásáról (HL L 331., 2017.12.14., 57. o., ELI: http://data.europa.eu/eli/dec/2017/2315/2023-05-23).

(31) Ez a rendelet nem érinti a válságreagálás uniós szintű koordinálására szolgáló eljárásokat és kereteket, különösen az (EU) 2022/2555 irányelvet, az 1313/2013/EU európai parlamenti és tanácsi határozattal[16] létrehozott uniós polgári védelmi mechanizmust, az IPCR-mechanizmust és az (EU) 2017/1584 bizottsági ajánlást[17]. A kiberbiztonsági szükséghelyzeti mechanizmus keretében nyújtott támogatás kiegészítheti a közös kül- és biztonságpolitika, valamint a közös biztonság- és védelempolitika keretében – többek között a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportokon keresztül – nyújtott támogatást, figyelembe véve a kiberbiztonsági szükséghelyzeti mechanizmus polgári jellegét. A kiberbiztonsági szükséghelyzeti mechanizmus keretében nyújtott támogatás kiegészítheti az EUSZ 42. cikkének (7) bekezdésével összefüggésben végrehajtott intézkedéseket, beleértve az egyik tagállam által egy másik tagállamnak nyújtott támogatást, vagy részét képezheti az Unió és a tagállamok közötti, vagy az EUMSZ 222. cikkében említett helyzetekben végrehajtott közös reagálásnak. E rendelet végrehajtását adott esetben össze kell hangolni a kiberdiplomáciai eszköztár szerinti intézkedések végrehajtásával is.

---

16 Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (HL L 347., 2013.12.20., 924. o.).

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

(32) 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, a tagállamok, az ENISA és adott esetben az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont 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.

(33) Az (EU) 2022/2555 irányelv előírja a tagállamok számára, hogy jelöljenek ki vagy hozzanak létre egy vagy több, kiberválságok kezelésével foglalkozó hatóságot, és biztosítsák, hogy azok megfelelő forrásokkal rendelkezzenek a rájuk ruházott feladatok hatékony és eredményes ellátásához. Előírja továbbá a tagállamok számára, hogy meghatározzák azon képességeket, eszközöket és eljárásokat, amelyek válság esetén alkalmazhatók, valamint hogy fogadjanak el nemzeti szintű nagyszabású kiberbiztonsági esemény- és válságelhárítási tervet, amelyben meghatározzák a nagyszabású kiberbiztonsági események és válsághelyzetek kezelésének célkitűzéseit és szabályait. A tagállamoknak továbbá létre kell hozniuk egy vagy több CSIRT-et, amelyek feladata a biztonsági események egy jól meghatározott folyamat szerinti kezelése, amely kiterjed legalább az említett irányelv hatálya alá tartozó ágazatokra, alágazatokra és szervezettípusokra, és biztosítaniuk kell, hogy hogy minden CSIRT megfelelő erőforrásokkal rendelkezzen feladatai hatékony ellátásához. Ez a rendelet nem érinti a Bizottság szerepét annak biztosításában, hogy a tagállamok megfeleljenek az (EU) 2022/2555 irányelvben foglalt kötelezettségeknek. A kiberbiztonsági szükséghelyzeti mechanizmusnak segítséget kell nyújtania a felkészültség megerősítését és a biztonsági eseményekre való reagálást célzó intézkedésekhez a jelentős és nagyszabású kiberbiztonsági események hatásának mérséklése, a helyreállítás megkezdésének támogatása vagy a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetek által nyújtott szolgáltatások alapvető funkcióinak helyreállítása érdekében.

(34) A következetes megközelítés előmozdítása, valamint az Unió és belső piaca biztonságának megerősítése érdekében a készültségi intézkedések részeként támogatást kell nyújtani az (EU) 2022/2555 irányelv alapján azonosított, kiemelten kritikus ágazatokban működő szervezetek kiberbiztonságának összehangolt teszteléséhez és értékeléséhez, többek között gyakorlat és képzés révén. E célból a Bizottságnak az ENISA-val, a Kiberbiztonsági Együttműködési Csoporttal és az EU-CyCLONe-val folytatott konzultációt követően rendszeresen azonosítania kell azokat az érintett ágazatokat vagy alágazatokat, amelyek jogosultak az uniós szintű összehangolt készültségi teszteléshez nyújtott pénzügyi támogatásra. Az ágazatokat vagy alágazatokat az (EU) 2022/2555 irányelv I. mellékletében felsorolt kiemelten kritikus ágazatok közül kell kiválasztani. Az összehangolt készültségi tesztelésnek közös kockázati forgatókönyveken és módszereken kell alapulnia.

Az ágazatok kiválasztása és a kockázati forgatókönyvek kidolgozása során figyelembe kell venni a vonatkozó uniós szintű kockázatértékeléseket és kockázati forgatókönyveket, többek között a párhuzamosságok elkerülésének igényét, például az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a Bizottsághoz, az Unió külügyi és biztonságpolitikai főképviselőjéhez (a továbbiakban: a főképviselő) és a Kiberbiztonsági Együttműködési Csoporthoz intézett felkérés szerinti, az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – többek között az EU-CyCLONe-nal – koordinációban elvégzendő kockázatértékelést és kidolgozandó kiberbiztonsági szempontú kockázati forgatókönyvet, és a távközlési hálózatokra és infrastruktúrákra vonatkozóan a nevers-i közös miniszteri felhívás nyomán a Kiberbiztonsági Együttműködési Csoport által, a Bizottság és az ENISA támogatásával, az (EU) 2018/1971 európai parlamenti és tanácsi rendelettel[18] létrehozott Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben elvégzendő kockázatértékelést, az (EU) 2022/2555 irányelv[19] 22. cikke alapján elvégzendő összehangolt kockázatértékeléseket, valamint az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben előírt digitális működési reziliencia tesztelését. Az ágazatok kiválasztása során figyelembe kell venni a kritikus infrastruktúra ellenálló képességének megerősítésére szolgáló koordinált megközelítésről szóló tanácsi ajánlást is.

---

[18] Az Európai Parlament és a Tanács (EU) 2018/1971 rendelete (2018. december 11.) az Európai Elektronikus Hírközlési Szabályozók Testületének (BEREC) és a BEREC Működését Segítő Ügynökségnek (BEREC Hivatal) a létrehozásáról, az (EU) 2015/2120 rendelet módosításáról, valamint az 1211/2009/EK rendelet hatályon kívül helyezéséről (HL L 321., 2018.12.17., 1. o.).

[19] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról (HL L 333., 2022.12.27., 1. o.).

(35) Emellett a kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell nyújtania más készültségi intézkedésekhez, és támogatnia kell a felkészültséget más olyan ágazatokban, amelyekre nem terjed ki a kiemelten kritikus és egyéb kritikus ágazatokban működő szervezetek összehangolt készültségi tesztelése. Az említett intézkedések különböző típusú nemzeti szintű készültségi tevékenységet foglalhatnak magukban.

(36) Amennyiben a tagállamok a készültségi intézkedések támogatására vissza nem térítendő támogatásban részesülnek, a kiemelten kritikus ágazatokban működő szervezetek önkéntes alapon részt vehetnek ezekben az intézkedésekben. Bevált gyakorlat, hogy az ilyen intézkedéseket követően a részt vevő szervezetek helyreállítási tervet dolgoznak ki az ebből eredő konkrét intézkedésekre vonatkozó ajánlások végrehajtására, hogy a lehető legteljesebb mértékben kihasználhassák a készültségi intézkedés előnyeit. Bár fontos, hogy a tagállamok az intézkedések részeként kérjék, hogy a részt vevő szervezetek dolgozzanak ki és hajtsanak végre ilyen helyreállítási terveket, e rendelet nem kötelezi és nem is hatalmazza fel a tagállamokat az ilyen kérelmek érvényesítésére. Az ilyen kérelmek nem érintik a szervezetekre és az illetékes hatóságok felügyeleti hatáskörére vonatkozó, az (EU) 2022/2555 irányelvvel összhangban meghatározott követelményeket.

(37) A kiberbiztonsági vészhelyzeti mechanizmusnak emellett támogatást kell nyújtania a jelentős, a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági események hatásának mérséklését, a helyreállítás megkezdésének támogatását és az alapvető szolgáltatások működésének helyreállítását célzó, kiberbiztonsági eseményekre való reagálással kapcsolatos intézkedésekhez. Adott esetben ki kell egészítenie az uniós polgári védelmi mechanizmust, biztosítva a kiberbiztonsági események polgárokra gyakorolt hatásaira való reagálás átfogó megközelítését.

(38) A kiberbiztonsági szükséghelyzeti mechanizmusnak támogatnia kell az egyik tagállam által egy másik, jelentős vagy nagyszabású kiberbiztonsági esemény által érintett tagállamnak – beleértve az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének f) pontjában említett CSIRT-eket is – biztosított technikai segítségnyújtást. Az ilyen segítséget nyújtó tagállamok számára lehetővé kell tenni, hogy kérelmeket nyújtsanak be a szakértői csoportok kölcsönös segítségnyújtás keretében történő kiküldésével kapcsolatos költségek fedezésére. Az elszámolható költségek közé tartozhatnak a kiberbiztonsági szakértők utazási, szállás- és napidíjköltségei.

(39) Tekintettel arra, hogy a magánvállalkozások alapvető szerepet játszanak a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági események észlelésében, az azokra való felkészültségben és reagálásban, fontos elismerni az ilyen vállalkozásokkal folytatott önkéntes pro bono együttműködés értékét, amelynek keretében a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági események és válságok esetén díjazás nélkül kínálnak szolgáltatásokat. Az ENISA az EU-CyCLONe-nal együttműködve nyomon követhetné az ilyen pro bono kezdeményezések alakulását, és előmozdíthatná, hogy azok megfeleljenek az e rendelet értelmében a megbízható irányított biztonsági szolgáltatókra alkalmazandó kritériumoknak, többek között a magánvállalkozások megbízhatóságával, tapasztalataival, valamint az érzékeny információk biztonságos kezelésének képességével kapcsolatban.

(40) A kiberbiztonsági vészhelyzeti mechanizmus részeként fokozatosan létre kell hozni egy uniós kiberbiztonsági tartalékot, amely megbízható irányított biztonsági szolgáltatók szolgáltatásaiból áll a tagállamokat, az uniós intézményeket, szerveket, hivatalokat és ügynökségeket vagy a Digitális Európa program társult harmadik országait érintő jelentős, nagyszabású vagy nagyszabásúval egyenértékű kiberbiztonsági események esetén a reagálás támogatása és a helyreállítási intézkedések megkezdése céljából. Az uniós kiberbiztonsági tartalék keretében biztosítani kell a szolgáltatások rendelkezésre állását és készenlétét. Ezért annak magában kell foglalnia az előzetesen vállalt szolgáltatásokat, beleértve például a készenlétben lévő és rövid időn belül bevethető kapacitásokat. Az uniós kiberbiztonsági tartalék szolgáltatásai a nemzeti hatóságokat hivatottak támogatni abban, hogy saját nemzeti szintű intézkedéseik kiegészítéseként segítséget nyújtsanak a kiemelten kritikus vagy egyéb kritikus ágazatokban működő érintett szervezeteknek. Az uniós kiberbiztonsági tartalék szolgáltatásai hasonló feltételek mellett az uniós intézményeknek, szerveknek, hivataloknak és ügynökségeknek is támogatást nyújthatnak. Az uniós kiberbiztonsági tartalék hozzájárulhat az uniós ipar és szolgáltatások – többek között a mikrovállalkozások, valamint a kis- és középvállalkozások, továbbá az induló innovatív vállalkozások – versenyképességének megerősítéséhez is az Unióban, többek között a kutatási és innovációs beruházások ösztönzése révén. Az uniós kiberbiztonsági tartalékhoz kapcsolódó szolgáltatások beszerzése során fontos figyelembe venni az ENISA Európai Kiberbiztonsági Készségek Keretét. Amikor a felhasználók támogatást kérnek az uniós kiberbiztonsági tartalékból, kérelmükbe bele kell foglalniuk az érintett szervezetre és a lehetséges hatásokra vonatkozó megfelelő információkat, az uniós kiberbiztonsági tartalékból igényelt szolgáltatásra vonatkozó információkat, és az érintett szervezetnek nemzeti szinten nyújtott támogatást, amelyet figyelembe kell venni a kérelmező kérelmének értékelésekor. Az érintett szervezet rendelkezésére álló egyéb támogatási formákkal való kiegészítő jelleg biztosítása érdekében a kérelemnek – amennyiben rendelkezésre áll – tartalmaznia kell a biztonsági eseményekre való reagálásra és az azokat követő helyreállítást megkezdő szolgáltatásokra vonatkozó meglévő szerződéses megállapodásokra, valamint az ilyen típusú eseményekre potenciálisan kiterjedő biztosítási szerződésekre vonatkozó információkat is.

(41) Az uniós finanszírozás hatékony felhasználásának biztosítása érdekében az e uniós kiberbiztonsági tartalékból lőzetesen lekötött szolgáltatásoknak a vonatkozó szerződéssel összhangban biztonsági események megelőzésével és elhárításával kapcsolatos felkészültségi szolgáltatásokká átalakíthatónak kell lenniük abban az esetben, ha ezeket az előzetesen lekötött szolgáltatásokat az előzetes kötelezettségvállalás ideje alatt nem használják fel biztonsági eseményekre való reagálásra. Ezeknek a szolgáltatásoknak ki kell egészíteniük, és nem szabad megkettőzniük az ECCC által irányítandó készültségi intézkedéseket.

(42) A tagállamok kiberválságkezelő hatóságai és CSIRT-jei, vagy a CERT-EU által az uniós intézmények, szervek, hivatalok és ügynökségek nevében benyújtott, az uniós kiberbiztonsági tartalékból származó támogatás iránti kérelmeket az ajánlatkérő szervnek kell értékelnie. Azokban az esetekben, amikor az ENISA-t bízták meg az uniós kiberbiztonsági tartalék igazgatásával és működtetésével, az ENISA minősül az ajánlatkérő szervnek. A Digitális Európa programhoz társult harmadik országok támogatás iránti kérelmeit a Bizottságnak kell értékelnie. A támogatási kérelmek benyújtásának és értékelésének megkönnyítése érdekében az ENISA biztonságos platformot hozhat létre.

(43) Amennyiben több párhuzamos megkeresés érkezik, ezeket a kérelmeket az e rendeletben meghatározott kritériumokkal összhangban kell rangsorolni. E rendelet általános célkitűzéseinek fényében e kritériumoknak ki kell terjedniük az esemény nagyságrendjére és súlyosságára, az érintett szervezet típusára, az eseménynek az érintett tagállamokra és felhasználókra gyakorolt lehetséges hatására, a lehetséges határokon átnyúló jellegére és a továbbgyűrűző hatások kockázatára, valamint a felhasználó által a reagálás és a helyreállítás megkezdésének elősegítése érdekében már meghozott intézkedésekre. Ugyanezen célkitűzések fényében, valamint tekintettel arra, hogy a tagállami felhasználók kéréseinek célja kizárólag a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetek támogatása Unió-szerte, helyénvaló nagyobb prioritást biztosítani a tagállami felhasználók kérelmeinek, amennyiben ezek a kritériumok két vagy több kérelem egyenlőként való értékelését eredményezik. Ez nem érinti a tagállamok azon kötelezettségeit, hogy a vonatkozó üzemeltetési megállapodások alapján intézkedéseket hozzanak az uniós intézmények, szervek, hivatalok és ügynökségek védelme és támogatása érdekében.

(44) A Bizottságnak általános felelősséget kell vállalnia az uniós kiberbiztonsági tartalék végrehajtásáért. Tekintettel az ENISA által a kiberbiztonsági támogatási intézkedéssel kapcsolatban szerzett széles körű tapasztalatokra, az ENISA a legalkalmasabb ügynökség az uniós kiberbiztonsági tartalék végrehajtására. Ezért a Bizottságnak – részben vagy amennyiben a Bizottság megfelelőnek ítéli, teljes egészében – az ENISA-t kell megbíznia az uniós kiberbiztonsági tartalék működtetésével és igazgatásával. A megbízást az (EU, Euratom) 2024/2509 rendelet szerinti alkalmazandó szabályokkal összhangban kell végrehajtani, és különösen a hozzájárulási megállapodás aláírására vonatkozó feltételek teljesülésétől kell függővé tenni. Az uniós kiberbiztonsági tartalék működtetésének és igazgatásának nem az ENISA-ra bízott vonatkozásait a Bizottságnak közvetlenül kell irányítania, többek között a hozzájárulási megállapodás aláírása előtt.

(45) A tagállamoknak kulcsszerepet kell játszaniuk az uniós kiberbiztonsági tartalék létrehozásában, bevezetésében és a bevezetését követően is. Mivel az (EU) 2021/694 rendelet az uniós kiberbiztonsági tartalékot végrehajtó intézkedések releváns alapjogiaktusa, az uniós kiberbiztonsági tartalék keretében végrehajtott intézkedésekről az (EU) 2021/694 rendelet 24. cikkében említett munkaprogramokban kell rendelkezni. Az említett cikk (6) bekezdése szerint a Bizottságnak végrehajtási jogi aktusok útján kell elfogadnia ezeket a munkaprogramokat, a vizsgálóbizottsági eljárásnak megfelelően. Ezenkívül a Bizottságnak a Kiberbiztonsági Együttműködési Csoporttal együttműködve meg kell határoznia az uniós kiberbiztonsági tartalék prioritásait és alakulását.

(46) Az uniós kiberbiztonsági tartalék keretében létrehozott szerződések nem érinthetik a vállalkozások közötti kapcsolatot, valamint az érintett szervezet vagy a felhasználók és a szolgáltató közötti meglévő kötelezettségeket.

(47) Az uniós kiberbiztonsági tartalék keretében szolgáltatásokat nyújtó magánszolgáltatók kiválasztása céljából meg kell határozni az e szolgáltatók kiválasztására irányuló ajánlati felhívásban szereplő minimum szempontokat és követelményeket, biztosítva, hogy a tagállami hatóságok és a kiemelten kritikus vagy egyéb kritikus ágazatokban működő szervezetek igényei teljesüljenek. A tagállamok sajátos igényeinek kielégítése érdekében az ajánlatkérő szervnek az uniós kiberbiztonsági tartalékhoz kapcsolódó szolgáltatások beszerzése során adott esetben az e rendeletben meghatározottakon felül további kiválasztási szempontokat és követelményeket kell kidolgoznia. Fontos ösztönözni a regionális és helyi szinten aktív kisebb szolgáltatók részvételét.

(48) Az uniós kiberbiztonsági tartalékba bekerülő szolgáltatók kiválasztásakor az ajánlatkérő szervnek törekednie kell annak biztosítására, hogy az uniós kiberbiztonsági tartalék egészében véve olyan szolgáltatókat tartalmazzon, amelyek képesek megfelelni a felhasználók nyelvi igényeinek. E célból az ajánlatkérő szervnek az ajánlattételi dokumentáció elkészítése előtt meg kell vizsgálnia, hogy az uniós kiberbiztonsági tartalék potenciális felhasználóinak vannak-e különleges nyelvi igényei annak érdekében, hogy az uniós kiberbiztonsági tartalék támogatási szolgáltatásait az uniós intézmények vagy valamely tagállam egy vagy több hivatalos nyelvén lehessen nyújtani, amelyet a felhasználó vagy az érintett szervezet valószínűleg megért. Abban az esetben, ha egy felhasználó egynél több nyelvet kér az uniós kiberbiztonsági tartaléktámogatási szolgáltatások nyújtásához, és a szolgáltatásokat ezeken a nyelveken szerezték be az adott felhasználó számára, a felhasználó számára lehetővé kell tenni, hogy az uniós kiberbiztonsági tartaléktámogatás iránti kérelemben meghatározza, hogy e nyelvek közül melyiken kell a szolgáltatást nyújtani a kérelem alapjául szolgáló konkrét kiberbiztonsági eseménnyel kapcsolatban.

(49) Az uniós kiberbiztonsági tartalék létrehozásának támogatása érdekében fontos, hogy a Bizottság felkérje az ENISA-t, hogy a kiberbiztonsági vészhelyzeti mechanizmus hatálya alá tartozó területeken az irányított biztonsági szolgáltatásokra vonatkozóan készítsen az (EU) 2019/881 rendelet szerinti kiberbiztonsági tanúsítási rendszerre irányuló javaslatot.

(50) E rendelet azon célkitűzéseinek támogatása érdekében, amelyek a közös helyzetismeret előmozdítására, az Unió ellenálló képességének fokozására és a jelentős és a nagyszabású kiberbiztonsági eseményekre való hatékony reagálás lehetővé tételére irányulnak, a Bizottságnak vagy az EU-CyCLONe-nak képesnek kell lennie arra, hogy felkérje az ENISA-t – a CSIRT-ek hálózatának támogatásával és az érintett tagállamok jóváhagyásával – a kiberfenyegetések, az ismert kihasználható sebezhetőségek és a kockázatcsökkentő intézkedések felülvizsgálatára és értékelésére egy adott jelentős vagy nagyszabású kiberbiztonsági esemény tekintetében. A biztonsági esemény felülvizsgálatának és értékelésének befejezését követően az ENISA-nak az érintett tagállammal, az érintett érdekelt felekkel, többek között a magánszektor, a Bizottság és más érintett uniós intézmények, szervek, hivatalok és ügynökségek képviselőivel együttműködésben eseményértékelési jelentést kell készítenie. A – többek között a magánszektorbeli – érdekelt felekkel folytatott együttműködésre építve a konkrét kiberbiztonsági eseményekkel kapcsolatos eseményértékelési jelentésnek arra kell irányulnia, hogy bekövetkezte után értékelje az esemény okait, hatásait és az azzal kapcsolatos mérséklési intézkedéseket. Különös figyelmet kell fordítani az e rendeletben előírt legmagasabb szintű szakmai feddhetetlenség, pártatlanság és szükséges technikai szakértelem feltételeinek megfelelő irányított biztonsági szolgáltatók által megosztott információkra és tapasztalatokra. A jelentést be kell nyújtani az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak, és azt be kell építeni mind azok, mind az ENISA munkájába. Amennyiben az esemény egy a Digitális Európa programhoz társult harmadik országgal kapcsolatos, a Bizottságnak a jelentést el kell juttatnia a főképviselőhöz is.

(51) Figyelembe véve a kibertámadások kiszámíthatatlan jellegét és azt, hogy azok gyakran nem korlátozódnak egy adott földrajzi területre, és így a tovagyűrűzés magas kockázatát hordozzák magukban, a szomszédos országok ellenálló képességének és a jelentős és a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való hatékony reagálási képességüknek a megerősítése hozzájárul az Unió – és különösen annak belső piaca és ipara – egészének védelméhez. Ezek a tevékenységek még inkább hozzájárulhatnak az uniós kiberdiplomáciához. Ezért a Digitális Európa programhoz társult harmadik országok a területük egészén vagy egy részén támogatást kérhetnek az uniós kiberbiztonsági tartalékból, amennyiben erről az a megállapodás rendelkezik, amelyen keresztül a harmadik ország a Digitális Európa programhoz társult. A Digitális Európa programhoz társult harmadik országok a vonatkozó partnerségek és finanszírozási eszközök keretében részesülnek az Unió nyújtotta finanszírozásból. A támogatásnak ki kell terjednie a jelentős vagy a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálás és az azokat követő helyreállítás megkezdésének területén nyújtott szolgáltatásokra.

(52) Az e rendeletben az uniós kiberbiztonsági tartalékra és a megbízható irányított biztonsági szolgáltatókra vonatkozóan meghatározott feltételeket alkalmazni kell a Digitális Európa programhoz társult harmadik országoknak nyújtott támogatásokra. A Digitális Európa programhoz társult harmadik országok számára lehetővé kell tenni, hogy kérelmezzék a támogatást az uniós kiberbiztonsági tartalékból, ha a célzott szervezetek, amelyek számára támogatást kérnek az uniós kiberbiztonsági tartalékból, kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetek, és ha az észlelt események jelentős működési zavarokhoz vezetnek vagy tovagyűrűző hatásokkal járhatnak az Unióban. A Digitális Európa programhoz társult harmadik országok csak akkor jogosultak támogatásra, ha az a megállapodás, amelyen keresztül a programhoz társultak, kifejezetten rendelkezik ilyen támogatásról. Ezen túlmenően az ilyen harmadik országok csak akkor támogathatók, ha három kritérium teljesül. Először is, a harmadik országnak teljes mértékben meg kell felelnie az említett megállapodás vonatkozó feltételeinek. Másodszor, tekintettel az uniós kiberbiztonsági tartalék kiegészítő jellegére, a harmadik országnak előzetesen megfelelő lépéseket kell megtennie a jelentős vagy a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való felkészülés érdekében. Harmadszor, az uniós kiberbiztonsági tartalékból nyújtott támogatásnak összhangban kell lennie az adott országgal kapcsolatos uniós politikával és a vele fenntartott általános kapcsolatokkal, valamint az Unió egyéb biztonsági politikáival. Az ezen harmadik kritériumnak való megfelelés értékelése keretében a Bizottságnak konzultálnia kell a főképviselővel az ilyen támogatás nyújtásának a közös kül- és biztonságpolitikával való összehangolásáról.

(53) A Digitális Európa programhoz társult harmadik országoknak nyújtott támogatás hatással lehet a harmadik országokkal fenntartott kapcsolatokra és az Unió biztonságpolitikájára, többek között a közös kül- és biztonságpolitika, valamint a közös biztonság- és védelempolitika összefüggésében. Ennek megfelelően helyénvaló, hogy a Tanács végrehajtási hatásköröket kapjon az ilyen támogatás nyújtására rendelkezésre álló időszak engedélyezésére és meghatározására. A Tanácsnak a Bizottság javaslata alapján kell eljárnia, kellően figyelembe véve a három kritérium Bizottság általi értékelését. Ugyanennek kell vonatkoznia a megújításokra és az ilyen jogi aktusok módosítására vagy hatályon kívül helyezésére irányuló javaslatokra is. Amennyiben a Tanács kivételes körülmények között úgy ítéli meg, hogy a harmadik kritérium tekintetében a körülményekben jelentős változás következett be, a Tanács számára lehetővé kell tenni, hogy egy végrehajtási jogi aktus módosítása vagy hatályon kívül helyezése érdekében saját kezdeményezésére járjon el, a Bizottság javaslatának megvárása nélkül. Az ilyen jelentős változások valószínűleg sürgős fellépést tesznek szükségessé, különösen jelentős következményekkel járnak a harmadik országokkal fenntartott kapcsolatokra nézve, és nem igényelnek részletes értékelést a Bizottság részéről. Ezen túlmenően a Bizottságnak együtt kell működnie a főképviselővel a Digitális Európa programhoz társult harmadik országok támogatás iránti kérelmeinek, és az ilyen harmadik országoknak nyújtott támogatás végrehajtásának tekintetében. A Bizottságnak figyelembe kell vennie az ENISA ezen kérelmekkel és támogatással kapcsolatos véleményét is. A Bizottságnak tájékoztatnia kell a Tanácsot a kérelmek értékelésének eredményéről, beleértve az e tekintetben tett releváns megfontolásokat és a kiépített szolgáltatásokat.

(54) A Kiberkészségek Akadémiájáról szóló, 2023. április 18-i bizottsági közlemény elismerte a képzett szakemberek hiányát. Az említett készségekre e rendelet célkitűzéseinek elérése érdekében van szükség. Az Uniónak sürgősen szüksége van olyan szakemberekre, akik rendelkeznek a kibertámadások megelőzéséhez, észleléséhez és az azoktól való elrettentéshez, valamint az Unió – többek között a legkritikusabb infrastruktúrái – ilyen támadásokkal szembeni védelméhez és ellenálló képességének biztosításához szükséges készségekkel és kompetenciákkal. E célból fontos ösztönözni az érdekelt felek – köztük a magánszektor, a tudományos körök és a közszféra – közötti együttműködést. Ugyanilyen fontos, hogy az Unió valamennyi területén szinergiák jöjjenek létre az oktatásba és képzésbe való beruházás tekintetében, hogy előmozdítsák az agyelszívás elkerülését célzó biztosítékok, valamint az azt célzó biztosítékok létrehozását, hogy a készséghiány egyes régiókban ne mélyüljön tovább más régiókhoz képest. Sürgősen meg kell szüntetni a kiberbiztonsági készséghiányt, különös tekintettel a kiberbiztonsági munkaerőn belül a nemek közötti különbségek csökkentésére a nők jelenlétének és részvételének a digitális kormányzás kialakításában való előmozdítása érdekében.

(55) A digitális egységes piac innovációjának fellendítése érdekében fontos a kiberbiztonság területén a kutatás és az innováció megerősítése, ezzel hozzájárulva a tagállamok ellenálló képességének és az Unió nyitott stratégiai autonómiájának növeléséhez, amelyek e rendelet célkitűzései. A szinergiák elengedhetetlenek a különböző érdekelt felek – köztük a magánszektor, a civil társadalom és a tudományos élet – közötti együttműködés és koordináció megerősítéséhez.

(56) E rendeletnek figyelembe kell vennie az Európai Parlament, a Tanács és a Bizottság 2022. január 26-i, „Európai Nyilatkozat a digitális jogokról és a digitális évtized alapelveiről” című közös nyilatkozatában foglalt, az Unió demokráciáinak, az emberek, a vállalkozások és a közintézmények érdekeinek a kiberbiztonsági kockázatokkal és a kiberbűnözéssel – többek között adatvédelmi incidensekkel, valamint a személyazonosság-lopással vagy -manipulációval – szembeni védelméhez kapcsolódó kötelezettségvállalást.

(57) E rendelet egyes nem alapvető rendelkezéseinek kiegészítése érdekében a Bizottságot fel kell hatalmazni arra, hogy az EUMSZ 290. cikkének megfelelően jogi aktusokat fogadjon el az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának meghatározása céljából. Különösen fontos, hogy a Bizottság az előkészítő munkája során megfelelő konzultációkat folytasson, többek között szakértői szinten is, és hogy e konzultációkra a jogalkotás minőségének javításáról szóló, 2016. április 13-i intézményközi megállapodásban[20] megállapított elvekkel összhangban kerüljön sor. Így különösen a felhatalmazáson alapuló jogi aktusok előkészítésében való egyenlő részvétel biztosítása érdekében az Európai Parlament és a Tanács a tagállamok szakértőivel egyidejűleg kap kézhez minden dokumentumot, és szakértőik rendszeresen részt vehetnek a Bizottság felhatalmazáson alapuló jogi aktusok előkészítésével foglalkozó szakértői csoportjainak ülésein.

[20] HL L 123., 2016.5.12., 1. o., ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj?locale=hu.

(58) E rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak elosztására vonatkozó részletes eljárási szabályok további meghatározása céljából. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek[21] megfelelően kell gyakorolni.

(59) Az Unió éves költségvetésére vonatkozó, a Szerződések szerinti szabályok sérelme nélkül a Bizottságnak az ENISA költségvetés-tervezési és személyzeti igényeinek értékelésekor figyelembe kell vennie az e rendeletből eredő kötelezettségeket.

(60) A Bizottságnak rendszeresen értékelnie kell az e rendeletben meghatározott intézkedéseket. Az első ilyen értékelést az e rendelet hatálybalépésének napjától számított első 2 évben, majd azt követően legalább négyévente kell elvégezni, figyelembe véve az EUMSZ 312. cikke alapján létrehozott többéves pénzügyi keret felülvizsgálatának időzítését. A Bizottságnak jelentést kell benyújtania az Európai Parlamentnek és a Tanácsnak az elért eredményekről. A különböző szükséges elemek, köztük az Európai Kiberbiztonsági Riasztási Rendszeren belül megosztott információk körének értékelése érdekében a Bizottságnak kizárólag könnyen hozzáférhető vagy önkéntesen rendelkezésre bocsátott információkra kell támaszkodnia. Figyelembe véve a geopolitikai fejleményeket, valamint az e rendeletben meghatározott intézkedések 2027 utáni folytonosságának és továbbfejlesztésének biztosítása érdekében fontos, hogy a Bizottság értékelje, hogy szükséges-e megfelelő költségvetést elkülöníteni a 2028–2034 közötti időszakra vonatkozó többéves pénzügyi keretben.

---

[21] Az Európai Parlament és a Tanács 182/2011/EU rendelete (2011. február 16.) a Bizottság végrehajtási hatásköreinek gyakorlására vonatkozó tagállami ellenőrzési mechanizmusok szabályainak és általános elveinek megállapításáról (HL L 55., 2011.2.28., 13. o., ELI: http://data.europa.eu/eli/reg/2011/182/oj?locale=hu).

(61) Mivel a rendelet céljait, nevezetesen az uniós ipar és szolgáltatások versenyhelyzetének a digitális gazdaságban történő megerősítését, és a kiberbiztonság területén az Unió technológiai szuverenitásához és nyílt stratégiai autonómiájához való hozzájárulást a tagállamok nem tudják kielégítően megvalósítani, az Unió szintjén azonban az intézkedés terjedelme és hatása miatt e célok jobban megvalósíthatók, az Unió intézkedéseket hozhat a szubszidiaritásnak az Európai Unióról szóló szerződés 5. cikkében foglalt elvével összhangban. Az arányosságnak az említett cikkben foglalt elvével összhangban ez a rendelet nem lépi túl az e célok eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

I. fejezet
Általános rendelkezések

1. cikk

Tárgy és célkitűzések

(1) E rendelet intézkedéseket állapít meg a kiberfenyegetések és -események észlelésére, valamint az azokra való felkészülésre és reagálásra irányuló uniós képességek megerősítésére, különösen a következők létrehozása révén:

a) a kiberközpontok páneurópai hálózata (a továbbiakban: Európai Kiberbiztonsági Riasztási Rendszer) az összehangolt észlelési és közös helyzetismereti képességek kiépítése és javítása érdekében;

b) a kiberbiztonsági vészhelyzeti mechanizmus, amelynek célja, hogy támogassa a tagállamokat a jelentős és a nagyszabású kiberbiztonsági eseményekre való felkészülésben, az azokra való reagálásban, azok hatásainak mérséklésében és az azokat követő helyreállítás megkezdésében, valamint támogassa az egyéb felhasználókat a jelentős és a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálásban;

c) a kiberbiztonsági események európai felülvizsgálati mechanizmusa, a jelentős vagy a nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából.

(2) E rendelet általános célkitűzései az uniós ipar és szolgáltatások – többek között a mikrovállalkozások, valamint a kis- és középvállalkozások, továbbá az induló innovatív vállalkozások – versenyhelyzeténekmegerősítése a digitális gazdaságban, valamint az Unió technológiai szuverenitásához és nyitott stratégiai autonómiájához való hozzájárulás a kiberbiztonság területén, többek között a digitális egységes piacon belüli innováció fellendítése révén. Ezeket a célkitűzéseket a szolidaritás uniós szintű erősítése, a kiberbiztonsági ökoszisztéma megerősítése, a tagállamok kiberellenálló képességének fokozása, valamint a munkaerő kiberbiztonsággal kapcsolatos készségeinek, know-how-jának, képességeinek és kompetenciáinak fejlesztése révén valósítja meg.

(3) A (2) bekezdésben említett általános célkitűzéseket a következő egyedi célkitűzések teljesítése révén kell megvalósítani:

a) a közös összehangolt uniós észlelési kapacitások és a kiberfenyegetésekkel és -eseményekkel kapcsolatos közös helyzetismeret megerősítése;

b) a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetek felkészültségének megerősítése Unió-szerte, valamint a szolidaritás megerősítése a jelentős, a nagyszabású vagy a nagyszabásúval egyenértékű kiberbiztonsági események kezelésére szolgáló összehangolt készültségi tesztelés, valamint fokozott reagálási és helyreállítási kapacitások kidolgozása révén, beleértve annak lehetőségét is, hogy a kiberbiztonsági eseményekre való uniós reagálási támogatást a Digitális Európa programhoz társult harmadik országok rendelkezésére bocsássák;

c) az Unió ellenálló képességének fokozása és az eseményekre történő hatékony reagáláshoz való hozzájárulás a jelentős vagy a nagyszabású kiberbiztonsági események felülvizsgálata és értékelése révén, beleértve a levont tanulságokat és adott esetben az ajánlásokat is.

(4) Az e rendelet szerinti intézkedéseket a tagállamok hatásköreinek kellő tiszteletben tartásával kell végrehajtani, és azoknak ki kell egészíteniük a CSIRT-ek hálózata, az EU-CyCLONe és a Kiberbiztonsági Együttműködési Csoport által végzett tevékenységeket.

(5) Ez a rendelet nem érinti a tagállamok alapvető állami funkcióit, többek között az állam területi integritásának biztosítását, a közrend fenntartását és a nemzetbiztonság garantálását. Így különösen, a nemzetbiztonság az egyes tagállamok kizárólagos felelőssége marad.

(6) Az uniós vagy nemzeti szabályok értelmében bizalmas információk e rendelet szerinti megosztásának és cseréjének az adott megosztás vagy csere célja szempontjából releváns és azzal arányos mértékre kell korlátozódnia. Az információk ilyen megosztása vagy cseréje során meg kell őrizni az információk bizalmas jellegét, és védeni kell az érintett szervezetek biztonsági és kereskedelmi érdekeit. Ez nem foglalja magában olyan információk szolgáltatását, amelyek közlése ellentétes lenne a tagállamok alapvető nemzetbiztonsági, közbiztonsági vagy védelmi érdekeivel.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

1. „határokon átnyúló kiberközpont”: írásbeli konzorciummegállapodással létrehozott, több országra kiterjedő platform, amely összehangolt hálózati struktúrába tömöríti legalább három tagállam nemzeti kiberközpontjait, és amelynek célja a kiberfenyegetések nyomon követésének, észlelésének és elemzésének javítása az események megelőzése és a kiberfenyegetettség felderítés előállításának támogatása érdekében, különösen releváns és adott esetben anonimizált adatok és információk cseréje, valamint a legkorszerűbb eszközök megosztása és valamely megbízható környezetben a kiberészlelési, -elemzési, valamint -megelőzési és -védelmi képességek közös fejlesztése révén;

2. „üzemeltetési konzorcium”: olyan részt vevő tagállamokból álló konzorcium, amelyek megállapodtak, hogy határokon átnyúló kiberközpontot hoznak létre, és hozzájárulnak az azt szolgáló eszközök, infrastruktúra vagy szolgáltatások beszerzéséhez, valamint a határokon átnyúló kiberközpont működtetéséhez;

3. „CSIRT”: az (EU) 2022/2555 irányelv 10. cikke alapján kijelölt vagy létrehozott CSIRT;

4. „szervezet”: az (EU) 2022/2555 irányelv 6. cikkének 38. pontjában meghatározottak szerinti szervezet;

5. „kiemelten kritikus ágazatokban működő szervezetek”: az (EU) 2022/2555 irányelv I. mellékletében felsorolt szervezettípusok;

6. „egyéb kritikus ágazatokban működő szervezetek”: az (EU) 2022/2555 irányelv II. mellékletében felsorolt szervezettípusok;

7. „kockázat”: az (EU) 2022/2555 rendelet 6. cikkének 9. pontjában meghatározottak szerinti kockázat;

8. „kiberfenyegetés”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározottak szerinti kiberfenyegetés;

9. „esemény”: az (EU) 2022/2555 irányelv 6. cikkének 6. pontjában meghatározottak szerinti esemény;

10. „jelentős kiberbiztonsági esemény”: az (EU) 2022/2555 irányelv 23. cikkének (3) bekezdésében meghatározott kritériumoknak megfelelő esemény;

11. „súlyos biztonsági esemény”: az (EU, Euratom) 2023/2841 európai parlamenti és tanácsi rendelet[22] 3. cikkének 8. pontjában meghatározottak szerinti súlyos biztonsági esemény;

12. „nagyszabású kiberbiztonsági esemény”: az (EU) 2022/2555 irányelv 6. cikkének 7. pontjában meghatározottak szerinti nagyszabású kiberbiztonsági esemény;

---

[22] Az Európai Parlament és a Tanács (EU, Euratom) 2023/2841 rendelete (2023. december 13.) az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról (HL L., 2023/2841, 2023.12.18., ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

13. „nagyszabásúval egyenértékű kiberbiztonsági esemény”: az uniós intézmények, szervek, hivatalok és ügynökségek esetében súlyos biztonsági esemény, a Digitális Európa programhoz társult harmadik országok esetében pedig olyan szintű zavart okozó esemény, amely meghaladja a Digitális Európa programhoz társult érintett harmadik ország reagálási képességét;

14. „a Digitális Európa programhoz társult harmadik ország”: olyan harmadik ország, amely az Unióval kötött, az (EU) 2021/694 rendelet 10. cikke alapján a Digitális Európa programban való részvételét lehetővé tevő megállapodásban részes fél;

15. „ajánlatkérő szerv”: a Bizottság vagy – amennyiben az uniós kiberbiztonsági tartalék működtetésével és igazgatásával a 14. cikk (5) bekezdése értelmében az ENISA-t bízták meg – az ENISA;

16. „irányított biztonsági szolgáltató”: az (EU) 2022/2555 irányelv 6. cikkének 40. pontjában meghatározottak szerinti irányított biztonsági szolgáltató;

17. „megbízható irányított biztonsági szolgáltatók”: e rendelet 17. cikkével összhangban az uniós kiberbiztonsági tartalékba való felvételre kiválasztott irányított biztonsági szolgáltatók.

II. fejezet
Az Európai Kiberbiztonsági Riasztási Rendszer

3. cikk

Az Európai Kiberbiztonsági Riasztási Rendszer létrehozása

(1) Létrejön az Európai Kiberbiztonsági Riasztási Rendszer, amely önkéntes alapon csatlakozó nemzeti kiberközpontokból és határokon átnyúló kiberközpontokból álló páneurópai infrastruktúra-hálózat, hogy támogassa az Unió fejlett képességeinek fejlesztését a kiberfenyegetésekkel kapcsolatos észlelési, elemzési és adatkezelési képességek javítása, valamint az Unión belüli események megelőzése érdekében.

(2) Az Európai Kiberbiztonsági Riasztási Rendszer:

a) hozzájárul a kiberfenyegetések elleni jobb védekezéshez és az azokra való reagáláshoz azáltal, hogy támogatja az érintett szervezeteket, illetve együttműködik azokkal, különösen a CSIRT-ekkel, a CSIRT-ek hálózatával, az EU-CyCLONe-vel és az (EU) 2022/2555 irányelv 8. cikkének (1) bekezdése alapján kijelölt vagy létrehozott illetékes hatóságokkal, és megerősíti azok képességeit;

b) a határokon átnyúló kiberközpontokon belül összegyűjti a különböző forrásokból származó kiberfenyegetésekre és -eseményekre vonatkozó releváns adatokat és információkat, és a határokon átnyúló kiberközpontokon keresztül megosztja az elemzett vagy összesített információkat, adott esetben a CSIRT-ek hálózatával;

c) magas színvonalú, hasznosítható információkat és kiberfenyegetettség felderítést gyűjt és támogatja ezek előállítását a legkorszerűbb eszközök és fejlett technológiák alkalmazásával, és megosztja ezeket az információkat és a kiberfenyegetettség felderítést;

d) hozzájárul a kiberfenyegetések összehangolt észlelésének és a közös helyzetismeretnek az egész Unióban történő javításához, valamint a riasztások kiadásához, többek között adott esetben a szervezeteknek szóló konkrét ajánlások révén;

e) szolgáltatásokat és tevékenységeket nyújt az Unió kiberbiztonsági közössége számára, többek között hozzájárul a fejlett eszközök és technológiák, így a mesterséges intelligencia és az adatelemzést szolgáló eszközök fejlesztéséhez.

(3) Az Európai Kiberbiztonsági Riasztási Rendszert végrehajtó intézkedéseket a Digitális Európa programból nyújtott finanszírozással kell támogatni, és az (EU) 2021/694 rendelettel, különösen annak 3. egyedi célkitűzésével összhangban kell végrehajtani.

4. cikk

Nemzeti kiberközpontok

(1) Amennyiben egy tagállam úgy dönt, hogy részt vesz az Európai Kiberbiztonsági Riasztási Rendszerben, e rendelet alkalmazásában nemzeti kiberközpontot jelöl ki vagy adott esetben hoz létre.

(2) A nemzeti kiberközpont egy, a tagállam fennhatósága alatt működő egyetlen szervezet. Lehet CSIRT, vagy adott esetben egy kiberválságok kezelésével foglalkozó nemzeti hatóság vagy az (EU) 2022/2555 irányelv 8. cikkének (1) bekezdése alapján kijelölt vagy létrehozott egyéb illetékes hatóság, vagy más szervezet. A nemzeti kiberközpontnak:

a) képesnek kell lennie arra, hogy nemzeti szintű referenciapontként és átjáróként szolgáljon más állami és magánszervezetek számára a kiberfenyegetésekre és -eseményekre vonatkozó információk gyűjtése és elemzése céljából, valamint hogy hozzájáruljon valamely, az 5. cikkben említett, határokon átnyúló kiberközponthoz; és

b) képesnek kell lennie a kiberfenyegetések és -események szempontjából releváns adatok és információk – például a fenyegetettség felderítés – észlelésére, összesítésére és elemzésére, különösen a legkorszerűbb technológiák alkalmazásával, az események megelőzése céljából.

(3) Az e cikk (2) bekezdésében említett funkciók részeként a nemzeti kiberközpontok együttműködhetnek a magánszektorbeli szervezetekkel – többek között az (EU) 2022/2555 irányelv 3. cikkében említett alapvető és fontos szervezetek ágazati és ágazatközi közösségeivel – a kiberfenyegetések és -események észlelése és megelőzése céljából releváns adatok és információk cseréje érdekében. Adott esetben, valamint az uniós és a nemzeti joggal összhangban a nemzeti kiberközpontok által kért vagy kapott információk telemetriai, szenzor- és naplózási adatokat is tartalmazhatnak.

(4) Valamely, a 9. cikk (1) bekezdése alapján kiválasztott tagállam vállalja, hogy kérelmezi nemzeti kiberközpontja részvételét egy határokon átnyúló kiberközpontban.

5. cikk

Határokon átnyúló kiberközpontok

(1) Amennyiben legalább három tagállam elkötelezett annak biztosítása mellett, hogy nemzeti kiberközpontjaik együttműködjenek kiberészlelési és fenyegetésmonitoring tevékenységeik összehangolása érdekében, e tagállamok e rendelet alkalmazásában üzemeltetési konzorciumot hozhatnak létre.

(2) Az üzemeltetési konzorcium legalább három részt vevő tagállamból áll, amelyek megállapodtak abban, hogy a (4) bekezdéssel összhangban létrehoznak egy határokon átnyúló kiberközpontot, és hozzájárulnak az azt szolgáló eszközök, infrastruktúra vagy szolgáltatások beszerzéséhez és az említett kiberközpont működéséhez.

(3) Amennyiben az üzemeltetési konzorciumot a 9. cikk (3) bekezdésével összhangban választják ki, annak tagjai írásbeli konzorciumi megállapodást kötnek, amely:

a) meghatározza a 9. cikk (3) bekezdésében említett üzemeltetési és használati megállapodás végrehajtásának belső szabályait;

b) létrehozza az üzemeltetési konzorcium határokon átnyúló kiberközpontját; és

c) tartalmazza a 6. cikk (1) és (2) bekezdésében előírt konkrét rendelkezéseket.

(4) A határokon átnyúló kiberközpont a (3) bekezdésben említett írásbeli konzorciumi megállapodással létrehozott, több országra kiterjedő platform. Összehangolt hálózati struktúrában egyesíti az üzemeltetési konzorcium tagállamainak nemzeti kiberközpontjait. Úgy kell kialakítani, hogy javítsa a kiberfenyegetések nyomon követését, észlelését és elemzését, megelőzze az eseményeket és támogassa a kiberfenyegetettség felderítés előállítását, különösen a releváns és adott esetben anonimizált adatok és információk cseréje, valamint a legkorszerűbb eszközök megosztása, valamint a kiberészlelési, -elemzési, valamint -megelőzési és -védelmi képességek megbízható környezetben történő közös fejlesztése révén.

(5) A határokon átnyúló kiberközpont jogi képviseletét a megfelelő üzemeltetési konzorcium koordinátorként eljáró tagja, vagy az üzemeltetési konzorcium látja el, amennyiben az jogi személyiséggel rendelkezik. A határokon átnyúló kiberközpont e rendeletnek és az üzemeltetési és használati megállapodásnak való megfeleléséért viselt felelősséget a (3) bekezdésben említett írásbeli konzorciumi megállapodásban kell elosztani.

(6) A tagállamok az üzemeltetési konzorcium tagjainak beleegyezésével csatlakozhatnak egy meglévő üzemeltetési konzorciumhoz. A (3) bekezdésben említett írásbeli konzorciumi megállapodást, valamint az üzemeltetési és használati megállapodást ennek megfelelően módosítani kell. Ez nem érinti az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak (a továbbiakban: ECCC) az említett üzemeltetési konzorciummal már közösen beszerzett eszközök, infrastruktúrák vagy szolgáltatások feletti tulajdonjogát.

6. cikk

Együttműködés és információmegosztás a határokon átnyúló kiberközpontokon belül és azok között

(1) Az üzemeltetési konzorcium tagjai biztosítják, hogy nemzeti kiberközpontjaik egymás között a határokon átnyúló kiberközponton belül – az 5. cikk (3) bekezdésében említett írésbeli konzorciumi megállapodással összhangban – releváns, adott esetben anonimizált információkat osszanak meg, így 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:

a) előmozdítja és fokozza a kiberfenyegetések észlelését, és megerősíti a CSIRT-ek hálózatának a biztonsági események megelőzésére és az azokra való reagálásra, illetve azok hatásainak mérséklésére irányuló képességeit;

b) növeli a kiberbiztonság szintjét, például azáltal, hogy felhívja a figyelmet a kiberfenyegetésekre, korlátozza vagy gátolja az ilyen fenyegetések terjedési képességét, támogatja a védelmi képességek széles skáláját, a sebezhetőség elhárítását és nyilvánosságra hozatalát, a fenyegetésészlelési, -korlátozási és -megelőzési technikákat, a mérséklési stratégiákat, az elhárítási és helyreállítási szakaszt, vagy előmozdítja az állami szervek és magánszervezetek közötti együttműködésen alapuló, kiberfenyegetésekkel kapcsolatos kutatásokat.

(2) Az 5. cikk (3) bekezdésében említett írásbeli konzorciumi megállapodásban meg kell állapítani a következőket:

a) az (1) bekezdésben említett információknak az üzemeltetési konzorcium tagjai közötti megosztására vonatkozó kötelezettségvállalás, valamint az említett információk megosztásának feltételei;

b) egy irányítási keret, amely tisztázza és ösztönzi az (1) bekezdésben említett releváns és adott esetben anonimizált információk valamennyi résztvevő általi megosztását;

c) a fejlett eszközök és technológiák, így mesterséges intelligencia és adatelemzést szolgáló eszközök fejlesztéséhez való hozzájárulásra vonatkozó célértékek.

Az írásbeli konzorciumi megállapodás előírhatja, hogy az (1) bekezdésben említett információkat az uniós és a nemzeti joggal összhangban kell megosztani.

(3) A határokon átnyúló kiberközpontok együttműködési megállapodásokat kötnek egymással, amelyekben meghatározzák a határokon átnyúló kiberközpontok közötti interoperabilitás és információmegosztás elveit. A határokon átnyúló kiberközpontok tájékoztatják a Bizottságot a megkötött együttműködési megállapodásokról.

(4) A határokon átnyúló kiberközpontok közötti, az (1) bekezdésben említett információmegosztást magas szintű interoperabilitással kell biztosítani. Az ilyen interoperabilitás támogatása érdekében az ENISA – a Bizottsággal szorosan konzultálva – indokolatlan késedelem nélkül, és mindenféleképpen ... [e rendelet hatálybalépésének napjától számított 12 hónappal]-ig, interoperabilitási iránymutatásokat bocsát ki, amelyekben meghatározza különösen az információmegosztás formátumait és protokolljait, figyelembe véve a nemzetközi szabványokat és bevált gyakorlatokat, valamint a létrehozott, határokon átnyúló kiberközpontok működését. A határokon átnyúló kiberközpontok együttműködési megállapodásaiban előírt interoperabilitási követelményeknek az ENISA által kiadott iránymutatásokon kell alapulniuk.

7. cikk

Együttműködés és információmegosztás az uniós szintű hálózatokkal

(1) A határokon átnyúló kiberközpontoknak és a CSIRT-hálózatnak szorosan együtt kell működniük, különösen az információk megosztása céljából. E célból megállapodnak az együttműködésre és a releváns információk megosztására vonatkozó eljárási szabályokról, valamint – a (2) bekezdés sérelme nélkül – a megosztandó információk típusairól.

(2) Amennyiben a határokon átnyúló kiberközpontok információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a közös helyzetismeret céljából biztosítják, hogy a releváns információkat és a korai figyelmeztetéseket az EU-CyCLONe-n és a CSIRT-ek-hálózatán keresztül indokolatlan késedelem nélkül eljuttassák a tagállami hatóságoknak és a Bizottságnak.

8. cikk

Biztonság

(1) Az európai kiberbiztonsági riasztási rendszerben részt vevő tagállamok biztosítják az európai kiberbiztonsági riasztási rendszer magas szintű kiberbiztonságát, beleértve a titoktartást és az adatbiztonságot, valamint az európai kiberbiztonsági riasztási rendszer fizikai biztonságát, valamint biztosítják, hogy a hálózatot megfelelő irányítás és ellenőrzés révén megvédjék a fenyegetésektől, továbbá biztosítják a hálózat és a rendszerek – többek között a hálózaton keresztül megosztott adatok és információk – biztonságát is.

(2) Az Európai Kiberbiztonsági Riasztási Rendszerben részt vevő tagállamok biztosítják, hogy a 6. cikk (1) bekezdésében említett információknak az Európai Kiberbiztonsági Riasztási Rendszeren belüli, valamely tagállam hatóságától vagy szervétől eltérő szervezettel való megosztása ne érintse hátrányosan az Unió vagy a tagállamok biztonsági érdekeit.

9. cikk

Az Európai Kiberbiztonsági Riasztási Rendszer finanszírozása

(1) Az Európai Kiberbiztonsági Riasztási Rendszerben részt venni kívánó tagállamoknak szóló, részvételi szándék kifejezésére való felhívást követően az ECCC kiválasztja a tagállamokat, hogy az ECCC-vel részt vegyenek az eszközök, az infrastruktúra vagy a szolgáltatások közös beszerzésében, a 4. cikk (1) bekezdése szerint kijelölt vagy létrehozott nemzeti kiberközpontok létrehozása, vagy képességeinek javítása érdekében. Az ECCC vissza nem térítendő támogatást ítélhet oda a kiválasztott tagállamoknak ezen eszközök, infrastruktúrák vagy szolgáltatások működésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök, infrastruktúrák vagy szolgáltatások beszerzési költségeinek legfeljebb 50 %-át és a működési költségek legfeljebb 50 %-át fedezi. A fennmaradó költségeket a kiválasztott tagállamok fedezik. Az eszközök, infrastruktúrák vagy szolgáltatások beszerzésére irányuló eljárás megindítása előtt az ECCC és a kiválasztott tagállamok az eszközök, infrastruktúrák vagy szolgáltatások használatát szabályozó üzemeltetési és használati megállapodást kötnek.

(2) Ha egy tagállam nemzeti kiberközpontja az eszközök, infrastruktúrák vagy szolgáltatások beszerzésének vagy vissza nem térítendő támogatásban való részesülésének időpontjától számított két éven belül – attól függően, hogy melyik következik be korábban – nem vesz részt egy határokon átnyúló kiberközpontban, a tagállam mindaddig nem jogosult további uniós támogatásra e fejezet alapján, amíg nem csatlakozott egy határokon átnyúló kiberközponthoz.

(3) Az ECCC részvételi szándék kifejezésére való felhívást követően választja ki azt az üzemeltetési konzorciumot, amely részt vesz az eszközök, infrastruktúrák vagy szolgáltatások ECCC-vel közös beszerzésében. Az ECCC vissza nem térítendő támogatást ítélhet oda az üzemeltetési konzorciumnak az eszközök, infrastruktúrák vagy szolgáltatások működésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök, infrastruktúrák vagy szolgáltatások beszerzési költségeinek legfeljebb 75 %-át és a működési költségek legfeljebb 50 %-át fedezi. A fennmaradó költségeket az üzemeltetési konzorcium fedezi. Az eszközök, infrastruktúrák vagy szolgáltatások beszerzésére irányuló eljárás megindítása előtt az ECCC és az üzemeltetési konzorcium az eszközök, infrastruktúrák vagy szolgáltatások használatát szabályozó üzemeltetési és használati megállapodást köt.

(4) Az ECCC legalább kétévente feltérképezi a nemzeti kiberközpontok és a határokon átnyúló kiberközpontok létrehozásához vagy képességeinek fejlesztéséhez szükséges és megfelelő minőségű eszközöket, infrastruktúrákat vagy szolgáltatásokat, valamint azok rendelkezésre állását, többek között a tagállamokban letelepedett vagy letelepedettnek tekintett és a tagállamok vagy a tagállamok állampolgárai által ellenőrzött jogalanyok részéről. A feltérképezés előkészítése során az ECCC konzultál a CSIRT-es hálózatával, mindegyik határokon átnyúló kiberközponttal, az ENISA-val és a Bizottsággal.

III. fejezet
Kiberbiztonsági vészhelyzeti mechanizmus

10. cikk

A kiberbiztonsági vészhelyzeti mechanizmus létrehozása

(1) Létrejön egy kiberbiztonsági vészhelyzeti mechanizmus, amelynek célja az Unió kiberfenyegetésekkel szembeni ellenálló képessége javításának támogatása, valamint a szolidaritás szellemében a jelentős, a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági események rövid távú hatásaira való felkészülés és e hatások mérséklése.

(2) A tagállamok esetében a kiberbiztonsági vészhelyzeti mechanizmus szerinti intézkedéseket kérésre kell biztosítani, és azoknak ki kell egészíteniük az eseményekre való felkészülésre, az azokra való reagálásra és az azokat követő helyreállításra irányuló tagállami erőfeszítéseket és intézkedéseket.

(3) A kiberbiztonsági vészhelyzeti mechanizmust végrehajtó intézkedéseket a Digitális Európa programból nyújtott finanszírozással kell támogatni, és az (EU) 2021/694 rendelettel, különösen annak 3. egyedi célkitűzésével összhangban kell végrehajtani.

(4) A kiberbiztonsági vészhelyzeti mechanizmus keretében végrehajtott intézkedéseket elsősorban az ECCC-n keresztül kell végrehajtani az (EU) 2021/887 rendelettel összhangban. Az e rendelet 11. cikkének b) pontjában említett uniós kiberbiztonsági tartalékot végrehajtó intézkedéseket azonban a Bizottságnak és az ENISA-nak kell végrehajtania.

11. cikk

Intézkedéstípusok

A kiberbiztonsági vészhelyzeti mechanizmus a következő intézkedéstípusokat támogatja:

a) készültségi intézkedések, nevezetesen:

i. a 12. cikkben meghatározottak szerint Unió-szerte a kiemelten kritikus ágazatokban működő szervezetek összehangolt készültségi tesztelése;

ii. a 13. cikkben meghatározottak szerint a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetekre vonatkozó egyéb készültségi intézkedések;

b) a jelentős, a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálást és az azokat követő helyreállítást megkezdő intézkedések, amelyeket a 14. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő, megbízható irányított biztonsági szolgáltatók biztosítanak;

c) a 18. cikkben említett kölcsönös segítségnyújtást támogató intézkedések.

12. cikk

A szervezetek összehangolt készültségi tesztelése

(1) A kiberbiztonsági vészhelyzeti mechanizmus támogatja a kiemelten kritikus ágazatokban működő szervezetek önkéntes összehangolt készültségi tesztelését.

(2) Az összehangolt készültségi tesztelés magában foglalhat készültségi tevékenységeket, például behatolási tesztelést és fenyegetésértékelést.

(3) Az e cikk szerinti készültségi intézkedések támogatását elsősorban vissza nem térítendő támogatások formájában és az (EU) 2021/694 rendelet 24. cikkében említett vonatkozó munkaprogramokban előírt feltételek mellett kell nyújtani a tagállamok számára.

(4) A szervezetek e rendelet 10. cikke a) pontjának i. alpontjában említett összehangolt készültségi tesztelésének Unió-szerte történő támogatása céljából a Bizottság a Kiberbiztonsági Együttműködési Csoporttal, az EU-CyCLONe-vel és az ENISA-val folytatott konzultációt követően azonosítja az (EU) 2022/2555 irányelv I. mellékletében felsorolt kiemelten kritikus ágazatokon belüli érintett ágazatokat vagy alágazatokat, amelyekre vonatkozóan támogatás odaítélésére vonatkozó pályázati felhívás bocsátható ki. A tagállamok önkéntes alapon vesznek részt az említett pályázatokon.

(5) A (4) bekezdésben említett ágazatok vagy alágazatok azonosítása során a Bizottság figyelembe veszi az uniós szintű össszehangolt kockázatértékeléseket és rezilienciateszteléseket, valamint azok eredményeit.

(6) A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az Unió külügyi és biztonságpolitikai főképviselőjével (a továbbiakban: a főképviselő) és az ENISA-val, valamint megbízatásának keretein belül az EU-CyCLONe-nal együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki a 11. cikk a) pontjának i. alpontjában említett összehangolt készültségi teszteléshez, valamint adott esetben az említett cikk a) pontjának ii. alpontjában említett egyéb készültségi intézkedésekhez.

(7) Amennyiben egy kiemelten kritikus ágazatban működő szervezet önkéntesen vesz részt összehangolt készültségi tesztelésben, és ez a tesztelés olyan konkrét intézkedésekre vonatkozó ajánlásokat eredményez, amelyeket a résztvevő szervezet belefoglalhat a helyreállítási tervbe, az összehangolt készültségi tesztelésért felelős tagállami hatóságnak adott esetben felül kell vizsgálnia az említett intézkedések részt vevő szervezetek általi nyomon követését a felkészültség megerősítése érdekében.

13. cikk

Egyéb készültségi intézkedések

(1) A kiberbiztonsági vészhelyzeti mechanizmus támogatja a 12. cikk hatálya alá nem tartozó készültségi intézkedéseket. Ezeknek a készültségi intézkedéseknek magukban kell foglalniuk a 12. cikk szerinti összehangolt készültségi tesztelés szempontjából nem azonosított ágazatokban működő szervezetekre vonatkozó készültségi intézkedéseket. Ezek az intézkedések támogathatják a sebezhetőség nyomon követését, a kockázatok nyomon követését, a gyakorlatokat és a képzéseket.

(2) Az e cikk szerinti készültségi intézkedésekhez nyújtott támogatást kérésre és elsősorban vissza nem térítendő támogatások formájában, valamint az (EU) 2021/694 rendelet 24. cikkében említett vonatkozó munkaprogramokban előírt feltételek mellett kell nyújtani a tagállamok számára.

14. cikk

Az uniós kiberbiztonsági tartalék létrehozása

(1) Létre kell hozni az uniós kiberbiztonsági tartalékot annak érdekében, hogy a jelentős, a nagyszabású vagy a nagyszabásúval egyenértékű kiberbiztonsági események alkalmával a (3) bekezdésben említett felhasználók kérésre segítséget kapjanak a reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállítás megkezdéséhez.

(2) Az uniós kiberbiztonsági tartalék a 17. cikk (2) bekezdésében meghatározott kritériumoknak megfelelően kiválasztott, megbízható irányított biztonsági szolgáltatók reagálási szolgáltatásaiból áll össze. Az uniós kiberbiztonsági tartalék előzetes kötelezettségvállalás keretében rendelkezésre bocsátott szolgáltatásokat tartalmazhat. A megbízható irányított biztonsági szolgáltató előzetesen rendelkezésre bocsátott szolgáltatásait – amikor ezeket az előzetesen rendelkezésre bocsátott szolgáltatásokat az előzetes kötelezettségvállalás keretében történő rendelkezésre bocsátás ideje alatt nem használják fel eseményekre való reagálásra – az események megelőzésével és az azokra való reagálással kapcsolatos felkészültségi szolgáltatásokká alakíthatóvá kell tenni. Az uniós kiberbiztonsági tartalék kérésre felhasználható valamennyi tagállamban, uniós intézményben, szervben, hivatalban és ügynökségben, valamint a 19. cikk (1) bekezdésében említett, a Digitális Európa programhoz társult harmadik országokban.

(3) Az uniós kiberbiztonsági tartalék által nyújtott szolgáltatások felhasználói az alábbiak:

a) a tagállamok az (EU) 2022/2555 irányelv 9. cikkének (1) és (2) bekezdésében említett kiberválságok kezelésével foglalkozó hatóságai és az említett irányelv 10. cikkében említett CSIRT-ek;

b) a CERT-EU, az (EU, Euratom) 2023/2841 rendelet 13. cikkének megfelelően;

c) a Digitális Európa programhoz társult harmadik országok illetékes hatóságai, például a számítógép-biztonsági eseményekre reagáló csoportok és a kiberválságok kezelésével foglalkozó hatóságok a 19. cikk (8) bekezdésével összhangban.

(4) A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság a Kiberbiztonsági Együttműködési 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. Ezeket a prioritásokat kétévente felül kell vizsgálni és adott esetben ellenőrizni kell. A Bizottság tájékoztatja az Európai Parlamentet és a Tanácsot ezekről a prioritásokról és azok felülvizsgálatáról.

(5) Az e cikk (4) bekezdésében említett, az uniós kiberbiztonsági tartalék végrehajtására vonatkozó átfogó bizottsági felelősség sérelme nélkül és az (EU, Euratom) 2024/2509 rendelet 2. cikkének 19. pontjában meghatározottak szerinti hozzájárulási megállapodás függvényében a Bizottság az uniós kiberbiztonsági tartalék működtetésével és igazgatásával részben vagy egészben az ENISA-t bízza meg. Az ENISA-ra nem bízott szempontok továbbra is a Bizottság közvetlen irányítása alá tartoznak.

(6) Az ENISA legalább kétévente feltérképezi az e cikk (3) bekezdésének a) és b) pontjában említett felhasználók számára szükséges szolgáltatásokat. A feltérképezésnek magában kell foglalnia az ilyen szolgáltatások elérhetőségét is, beleértve a tagállamokban letelepedett vagy letelepedettnek tekintett és a tagállamok vagy a tagállamok állampolgárai által ellenőrzött jogalanyok részéről. E rendelkezésre állás feltérképezése során az ENISA értékeli az uniós kiberbiztonsági munkaerőnek az uniós kiberbiztonsági tartalék célkitűzései szempontjából releváns készségeit és kapacitását. A feltérképezés során az ENISA konzultál a Kiberbiztonsági Együttműködési Csoporttal, az EU-CyCLONe-nal, a Bizottsággal és adott esetben az (EU, Euratom) 2023/2841 rendelet 10. cikkével létrehozott Intézményközi Kiberbiztonsági Testülettel (a továbbiakban: az IICB). A szolgáltatások rendelkezésre állásának feltérképezése során az ENISA-nak konzultálnia kell a kiberbiztonsági ágazat érintett érdekelt feleivel, beleértve az irányított biztonsági szolgáltatókat is. Az ENISA hasonló feltérképezést készít, miután tájékoztatta a Tanácsot, valamint konzultált az EU-CyCLONe-nal, a Bizottsággal és adott esetben a főképviselővel, hogy azonosítsa az e cikk (3) bekezdésének c) pontjában említett felhasználók igényeit.

(7) A Bizottság felhatalmazást kap arra, hogy a 23. cikknek megfelelően felhatalmazáson alapuló jogi aktusokat fogadjon el abból a célból, hogy kiegészítse ezt a rendeletet az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának meghatározása révén. E felhatalmazáson alapuló jogi aktusok előkészítése során a Bizottság figyelembe veszi az e cikk (6) bekezdésében említett feltérképezést, valamint megoszthatja a tanácsokat és együttműködhet a Kiberbiztonsági Együttműködési Csoporttal és az ENISA-val.

15. cikk

Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmek

(1) A 14. cikk (3) bekezdésében említett felhasználók szolgáltatásokat kérhetnek az uniós kiberbiztonsági tartalékból a jelentős, a nagyszabású vagy a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálás és az azokat követő helyreállítás megkezdésének támogatása érdekében.

(2) Ahhoz, hogy az uniós kiberbiztonsági tartalékból támogatásban részesüljenek, a 14. cikk (3) bekezdésében említett felhasználók minden megfelelő intézkedést megtesznek azon esemény hatásainak mérséklése érdekében, amelyre a támogatást kérik, beleértve adott esetben a közvetlen technikai segítségnyújtást, valamint az eseményre való reagálást segítő egyéb források nyújtását, valamint a helyreállítási erőfeszítéseket.

(3) A támogatási kérelmeket a következő módon kell továbbítani az ajánlatkérő szervnek:

a) az e rendelet 14. cikke (3) bekezdésének a) pontjában említett felhasználók esetében az (EU) 2022/2555 irányelv 8. cikkének (3) bekezdése szerint kijelölt vagy létrehozott egyedüli kapcsolattartó ponton keresztül;

b) a 14. cikk (3) bekezdésének b) pontjában említett felhasználó esetében a felhasználó által;

c) a 14. cikk (3) bekezdésének c) pontjában említett felhasználók esetében a 19. cikk (9) bekezdésében említett egyedüli kapcsolattartó ponton keresztül.

(4) A 14. cikk (3) bekezdésének a) pontjában említett felhasználók kérelmei esetében a tagállamok tájékoztatják a CSIRT-ek hálózatát és adott esetben az EU-CyCLONe-t felhasználóiknak az e cikk szerinti eseményekre való reagáláshoz és helyreállítás megkezdéséhez támogatást igénylő kérelmeiről.

(5) Az eseményekre való reagáláshoz és a helyreállítás megkezdéséhez támogatást igénylő kérelmek a következőket tartalmazzák:

a) megfelelő információk az érintett szervezetről és az eseménynek a következőkre gyakorolt lehetséges hatásairól:

i. a 14. cikk (3) bekezdésének a) pontjában említett felhasználók esetében az érintett tagállamok és felhasználók, beleértve a más tagállamba való továbbgyűrűzés kockázatát is;

ii. a 14. cikk (3) bekezdésének b) pontjában említett felhasználó esetében az érintett uniós intézmények, szervek, hivatalok vagy ügynökségek;

iii. a 14. cikk (3) bekezdésének c) pontjában említett felhasználók esetében az érintett, a Digitális Európa programhoz társult országok;

b) a kért szolgáltatásra vonatkozó információk a kért támogatás tervezett felhasználásával együtt, beleértve a becsült igények megjelölését is;

c) a (2) bekezdésben említett, a támogatás iránti kérelem tárgyát képező esemény hatásainak mérséklése érdekében hozott intézkedésekre vonatkozó megfelelő információk;

d) adott esetben az érintett szervezet rendelkezésére álló egyéb támogatási formákra vonatkozó, rendelkezésre álló információk.

(6) Az ENISA a Bizottsággal és az EU-CyCLONe-nal együttműködve mintát dolgoz ki az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmek benyújtásának megkönnyítésére.

(7) A Bizottság végrehajtási jogi aktusok útján részletesen meghatározhatja az arra vonatkozó részletes eljárási szabályokat, hogy az uniós kiberbiztonsági tartalék támogató szolgáltatásait hogyan kell kérni és azokra hogyan kell reagálni az e cikk, a 16. cikk (1) bekezdése és a 19. cikk (10) bekezdése értelmében, beleértve a kérelmek benyújtására és a válaszok adására, valamint a 16. cikk (9) bekezdésében említett jelentések mintáira vonatkozó szabályokat. Ezeket a végrehajtási jogi aktusokat a 25. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

16. cikk

Az uniós kiberbiztonsági tartalékból nyújtott támogatás végrehajtása

(1) A 14. cikk (3) bekezdésének a) és b) pontjában említett felhasználók kérelmei esetében az ajánlatkérő szerv értékeli az uniós kiberbiztonsági tartalékból származó támogatás iránti kérelmeket. A támogatás hatékonyságának biztosítása érdekében a 14. cikk (3) bekezdésének a) és b) pontjában említett felhasználóknak haladéktalanul, de legkésőbb a kérelem benyújtásától számított 48 órán belül választ kell küldeni. Az ajánlatkérő szerv tájékoztatja a Tanácsot és a Bizottságot a folyamat eredményeiről.

(2) Az uniós kiberbiztonsági tartalék szolgáltatásainak kérelmezése és nyújtása során megosztott információk tekintetében az e rendelet alkalmazásában részt vevő valamennyi fél:

a) ezen információk felhasználását és megosztását az e rendelet szerinti kötelezettségei vagy funkciói teljesítéséhez szükséges mértékre korlátozza;

b) az uniós és a nemzeti jog alapján bizalmas vagy minősített információkat kizárólag az említett jognak megfelelően használhat fel és oszthat meg; és

c) biztosítja az eredményes, hatékony és biztonságos információcserét, adott esetben a vonatkozó információmegosztási protokollok, köztük a TLP-protokoll használata és tiszteletben tartása révén.

(3) A 16. cikk (1) bekezdése és a 19. cikk (10) bekezdése szerinti egyedi kérelmek elbírálása során az ajánlatkérő szerv vagy adott esetben a Bizottság először azt értékeli, hogy teljesülnek-e a 15. cikk (1) és (2) bekezdésében említett kritériumok. Amennyiben igen, értékeli a támogatás megfelelő időtartamát és jellegét, figyelembe véve az 1. cikk (3) bekezdésének b) pontjában említett célkitűzést és adott esetben a következő kritériumokat:

a) az esemény nagyságrendje és súlyossága;

b) az érintett szervezet típusa, e tekintetben nagyobb prioritást élveznek az (EU) 2022/2555 irányelv 3. cikkének (1) bekezdésében említett alapvető szervezeteket érintő események;

c) az eseménynek az érintett tagállamokra, uniós intézményekre, szervekre, hivatalokra vagy ügynökségekre, vagy a Digitális Európa Programhoz társult harmadik országokra gyakorolt lehetséges hatása;

d) a kiberbiztonsági esemény lehetséges határokon átnyúló jellege és annak kockázata, hogy tovagyűrűzhet más tagállamokra, uniós intézményekre, szervekre, hivatalokra vagy ügynökségekre, vagy a Digitális Európa Programhoz társult harmadik országokra;

e) a felhasználó által a reagálás támogatása érdekében hozott intézkedések és a helyreállítás megkezdésére irányuló erőfeszítések a 15. cikk (2) bekezdésében említettek szerint.

(4) A kérelmek rangsorolása érdekében a 14. cikk (3) bekezdésében említett felhasználóktól érkező párhuzamos kérelmek esetében figyelembe kell venni az e cikk (3) bekezdésében említett kritériumokat, adott esetben a tagállamok és az uniós intézmények, szervek, hivatalok és ügynökségek közötti lojális együttműködés elvének sérelme nélkül. Amennyiben az említett kritériumok alapján két vagy több kérelem egyenlőnek minősül, nagyobb prioritást kell biztosítani a tagállami felhasználók kérelmeinek. Amennyiben a 14. cikk (5) bekezdése szerint az uniós kiberbiztonsági tartalék működtetésével és igazgatásával részben vagy egészben az ENISA-t bízták meg, az ENISA és a Bizottság szorosan együttműködik a kérelmek e bekezdéssel összhangban történő rangsorolása érdekében.

(5) Az uniós kiberbiztonsági tartalék szolgáltatásait a megbízható irányított biztonsági szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi megállapodásokkal összhangban kell nyújtani. Ezek a szolgáltatások a megbízható irányított biztonsági szolgáltató, a felhasználó és az érintett szervezet közötti egyedi megállapodásokkal összhangban nyújthatók. Az e bekezdésben említett valamennyi megállapodásnak tartalmaznia kell többek között a felelősségre vonatkozó feltételeket.

(6) Az (5) bekezdésben említett megállapodásoknak az ENISA által a tagállamokkal és adott esetben az uniós kiberbiztonsági tartalék egyéb felhasználóival folytatott konzultációt követően készített mintákon kell alapulniuk.

(7) A Bizottság, az ENISA és az uniós kiberbiztonsági tartalék felhasználói nem viselnek szerződéses felelősséget az uniós kiberbiztonsági tartalék végrehajtása keretében nyújtott szolgáltatások nyomán harmadik feleknek okozott kárért.

(8) A felhasználók az uniós kiberbiztonsági tartalék 15. cikk (1) bekezdése szerinti kérésre nyújtott szolgáltatásait kizárólag a jelentős, a nagyszabású vagy a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálás támogatása és az azokat követő helyreállítás megkezdése céljából vehetik igénybe. Ezeket a szolgáltatásokat csak a következők tekintetében vehetik igénybe:

a) a 14. cikk (3) bekezdésének a) pontjában említett felhasználók esetében a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezetek, a 14. cikk (3) bekezdésének c) pontjában említett felhasználók esetében pedig az egyenértékű szervezetek; és

b) a 14. cikk (3) bekezdésének b) pontjában említett felhasználó esetében az uniós intézmények, szervek, hivatalok és ügynökségek.

(9) Valamely támogatás végét követő két hónapon belül a támogatást kapott felhasználók összefoglaló jelentést bocsátanak rendelkezésre a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról, a következőknek:

a) a 14. cikk (3) bekezdésének a) pontjában említett felhasználók esetében a Bizottságnak, az ENISA-nak, a CSIRT-ek hálózatának és az EU-CyCLONe-nak;

b) a 14. cikk (3) bekezdésének b) pontjában említett felhasználó esetében a Bizottságnak, az ENISA-nak és az IICB-nek;

c) a 14. cikk (3) bekezdésének c) pontjában említett felhasználók esetében a Bizottságnak.

A Bizottság az e bekezdés első albekezdésének c) pontja szerint a 14. cikk (3) bekezdésében említett felhasználóktól kapott összefoglaló jelentést továbbítja a Tanácsnak és a főképviselőnek.

(10) Amennyiben e rendelet 14. cikkének (5) bekezdése szerint az uniós kiberbiztonsági tartalék működtetésével és igazgatásával részben vagy egészben az ENISA-t bízták meg, az ENISA e tekintetben rendszeresen jelentést tesz a Bizottságnak és konzultál azzal. Ezzel összefüggésben az ENISA haladéktalanul elküldi a Bizottságnak az e rendelet 14. cikke (3) bekezdésének c) pontjában említett felhasználóktól kapott kérelmeket, valamint – amennyiben az e cikk szerinti rangsorolás céljából szükséges – az e rendelet 14. cikke (3) bekezdésének a) vagy b) pontjában említett felhasználóktól kapott kérelmeket. Az e bekezdésben foglalt kötelezettségek nem érintik az (EU) 2019/881 rendelet 14. cikkét.

(11) A 14. cikk (3) bekezdésének a) és b) pontjában említett felhasználók esetében az ajánlatkérő szerv rendszeresen, de legalább évente kétszer jelentést tesz a Kiberbiztonsági Együttműködési Csoportnak a támogatás felhasználásáról és eredményeiről.

(12) A 14. cikk (3) bekezdésének c) pontjában említett felhasználók esetében a Bizottság rendszeresen, de legalább évente kétszer jelentést tesz a Tanácsnak, és tájékoztatja a főképviselőt a támogatás felhasználásáról és eredményeiről.

17. cikk

Megbízható irányított biztonsági szolgáltatók

(1) Az uniós kiberbiztonsági tartalék létrehozását célzó közbeszerzési eljárások során az ajánlatkérő szerv az (EU, Euratom) 2024/2509 rendeletben meghatározott elvekkel és a következő elvekkel összhangban jár el:

a) biztosítja, hogy az uniós kiberbiztonsági tartalékba tartozó szolgáltatások összességükben olyan jellegűek legyenek, hogy az uniós kiberbiztonsági tartalék olyan szolgáltatásokat foglaljon magában, amelyek valamennyi tagállamban igénybe vehetők, figyelembe véve különösen az ilyen szolgáltatások nyújtására vonatkozó nemzeti követelményeket, például a nyelvekre, a tanúsításra vagy az akkreditációra vonatkozóan;

b) biztosítja az Unió és tagállamai alapvető biztonsági érdekeinek védelmét;

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 Unióban.

(2) Az uniós kiberbiztonsági tartalékhoz kapcsolódó szolgáltatások beszerzése során az ajánlatkérő szervnek a következő kritériumokat és követelményeket kell belefoglalnia a közbeszerzési dokumentumokba:

a) a szolgáltatónak bizonyítania kell, hogy személyzete a saját területén a legmagasabb szintű szakmai feddhetetlenséggel, függetlenséggel, felelősséggel és az adott területén a tevékenységek elvégzéséhez szükséges műszaki szakértelemmel rendelkezik, továbbá biztosítania kell a szakértelem állandóságát és folytonosságát, valamint a szükséges technikai erőforrásokat;

b) a szolgáltatónak, valamint az érintett leányvállalatoknak és alvállalkozóknak meg kell felelniük a minősített adatok védelmére vonatkozó alkalmazandó szabályoknak, és megfelelő intézkedésekkel kell rendelkezniük – beleértve adott esetben az egymás közötti megállapodásokat is – a szolgáltatással kapcsolatos bizalmas információk, különösen a bizonyítékok, megállapítások és jelentések védelme érdekében;

c) a szolgáltatónak elegendő bizonyítékot kell szolgáltatnia arra vonatkozóan, hogy irányítási struktúrája átlátható, és valószínűleg nem veszélyezteti pártatlanságát és szolgáltatásai minőségét, és nem okoz összeférhetetlenséget;

d) a szolgáltatónak megfelelő biztonsági tanúsítvánnyal kell rendelkeznie, legalább azon személyek tekintetében, akiket a szolgáltatásnyújtásban alkalmazni kíván, amennyiben azt valamely tagállam megköveteli;

e) a szolgáltatónak megfelelő biztonsági szintű informatikai rendszerekkel kell rendelkeznie;

f) a szolgáltatónak rendelkeznie kell a kért szolgáltatáshoz szükséges hardverrel és szoftverrel, amely nem tartalmazhat ismert kihasználható sebezhetőségeket, tartalmazza a legújabb biztonsági frissítéseket, és minden esetben meg kell felelnie az (EU) 2024/... európai parlamenti és tanácsi rendelet[23+] alkalmazandó rendelkezéseinek;

g) a szolgáltatónak bizonyítékot kell szolgáltatnia arra vonatkozóan, hogy tapasztalattal rendelkezik az érintett nemzeti hatóságoknak, illetve a kiemelten kritikus ágazatokban vagy egyéb kritikus ágazatokban működő szervezeteknek nyújtott hasonló szolgáltatások terén;

h) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást rövid időn belül nyújtsa azokban a tagállamokban, ahol a szolgáltatást biztosítani tudja;

i) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást az uniós intézmények vagy valamely tagállam egy vagy több hivatalos nyelvén nyújtsa, amennyiben a tagállamok vagy a 14. cikk (3) bekezdésének b) és c) pontjában említett felhasználók ezt igénylik, amennyiben a szolgáltató a szolgáltatást nyújtani tudja;

j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó európai kiberbiztonsági tanúsítási rendszer, a szolgáltatónak a rendszer alkalmazása megkezdésének napját követő 2 éven belül az említett rendszerrel összhangban tanúsítást kell szereznie;

---

23 Az Európai Parlament és a Tanács (EU) 2024/… rendelete (...) (HL L..., ELI:...).

\+ HL: Kérjük, illesszék be a szövegbe a PE-CONS 100/23 (2022/0272(COD)) dokumentumban szereplő rendelet számát, és illesszék be a lábjegyzetbe az említett rendelet számát, dátumát, HL-hivatkozását és ELI-hivatkozását.

k) a szolgáltatónak az ajánlatban fel kell tüntetnie minden olyan fel nem használt, eseményekre való reagálással kapcsolatos szolgáltatás átalakítási feltételeit, amely az eseményre való reagáláshoz szorosan kapcsolódó felkészültségi szolgáltatássá, például gyakorlattá vagy képzéssé alakítható át.

(3) Az uniós kiberbiztonsági tartalékhoz kapcsolódó szolgáltatások beszerzése céljából az ajánlatkérő szerv adott esetben a tagállamokkal szoros együttműködésben a (2) bekezdésben említetteken felül további kritériumokat és követelményeket is kidolgozhat.

18. cikk

A kölcsönös segítségnyújtást támogató intézkedések

(1) A kiberbiztonsági vészhelyzeti mechanizmus támogatást nyújt az egyik tagállam által egy másik, jelentős vagy nagyszabású kiberbiztonsági esemény által érintett tagállamnak történő technikai segítségnyújtáshoz, beleértve az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének f) pontjában említett eseteket is.

(2) Az e cikk (1) bekezdésében említett kölcsönös technikai segítségnyújtáshoz nyújtott támogatást vissza nem térítendő támogatás formájában és az (EU) 2021/694 rendelet 24. cikkében említett vonatkozó munkaprogramokban előírt feltételek mellett kell nyújtani.

19. cikk

A Digitális Európa programhoz társult harmadik országok számára nyújtott támogatás

(1) A Digitális Európa programhoz társult harmadik ország támogatást kérhet az uniós kiberbiztonsági tartalékból, amennyiben az a megállapodás, amelyen keresztül e harmadik ország a Digitális Európa programhoz társult, az uniós kiberbiztonsági tartalékban való részvételt ír elő. Az említett megállapodásnak olyan rendelkezéseket kell tartalmaznia, amelyek előírják a Digitális Európa programhoz társult érintett harmadik ország számára az e cikk (2) és (9) bekezdésében meghatározott kötelezettségek teljesítését. Egy harmadik országnak az uniós kiberbiztonsági tartalékban való részvétele céljából egy harmadik ország Digitális Európa programhoz való részleges társulása magában foglalhat az (EU) 2021/694 rendelet 6. cikke (1) bekezdésének g) pontjában említett operatív célkitűzésre korlátozódó társulást.

(2) Az (1) bekezdésben említett megállapodás megkötésétől számított 3 hónapon belül, de minden esetben mielőtt a Digitális Európa programhoz társult harmadik ország bármilyen támogatást kapna az uniós kiberbiztonsági tartalékból, tájékoztatja a Bizottságot a kiberellenálló és kockázatkezelési képességeiről, beleértve legalább a jelentős, a nagyszabású vagy a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való felkészülés érdekében hozott nemzeti intézkedésekre vonatkozó információkat, valamint a felelős nemzeti szervezetekre – köztük a számítógép-biztonsági eseményekre reagáló csoportokra vagy azokkal egyenértékű szervezetekre –, azok képességeire és a hozzájuk rendelt erőforrásokra vonatkozó információkat. A Digitális Európa programhoz társult harmadik ország rendszeresen, de legalább évente egyszer naprakésszé teszi ezeket az információkat. A Bizottság a (11) bekezdés alkalmazásának megkönnyítése céljából eljuttatja ezeket az információkat a főképviselőnek és az ENISA-nak.

(3) A Bizottság rendszeresen, de legalább évente egyszer értékeli a következő kritériumokat az (1) bekezdésben említett valamennyi, a Digitális Európa programhoz társult harmadik ország tekintetében:

a) az adott ország megfelel-e az (1) bekezdésben említett megállapodás feltételeinek, amennyiben ezek a feltételek az uniós kiberbiztonsági tartalékban való részvételre vonatkoznak;

b) a (2) bekezdésben említett információk alapján az adott ország megfelelő lépéseket tett-e a jelentős és a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való felkészülés érdekében; és

c) a támogatás nyújtása összhangban van-e az adott országgal kapcsolatos uniós politikával és a vele fenntartott általános kapcsolatokkal, és összhangban van-e más uniós biztonsági politikákkal.

A Bizottság az első albekezdésben említett értékelés során konzultál a főképviselővel az említett albekezdés c) pontjában említett kritérium tekintetében.

Amennyiben a Bizottság arra a következtetésre jut, hogy egy a Digitális Európa programhoz társult harmadik ország teljesíti az első albekezdésben említett valamennyi feltételt, a Bizottság javaslatot nyújt be a Tanácsnak, hogy a (4) bekezdéssel összhangban végrehajtási jogi aktust fogadjon el, amelyben engedélyezi az uniós kiberbiztonsági tartalékból az adott országnak nyújtott támogatást.

(4) A Tanács elfogadhatja a (3) bekezdésben említett végrehajtási jogi aktusokat. Ezek a végrehajtási jogi aktusok legfeljebb egy évig alkalmazandók. E végrehajtási jogi aktusok megújíthatók. E végrehajtási jogi aktusok tartalmazhatnak egy legalább 75 napos felső határt, azon napok számára vonatkozóan, amelyekre egyetlen kérelem alapján támogatás nyújtható.

E cikk alkalmazásában a Tanács késlekedés nélkül jár el, és főszabály szerint a (3) bekezdés harmadik albekezdése szerinti vonatkozó bizottsági javaslat elfogadásától számított nyolc héten belül elfogadja az e bekezdésben említett végrehajtási jogi aktusokat.

(5) A Tanács a Bizottság javaslata alapján eljárva bármikor módosíthatja vagy hatályon kívül helyezheti a (4) bekezdés szerint elfogadott végrehajtási jogi aktust.

Amennyiben a Tanács úgy ítéli meg, hogy a (3) bekezdésharmadik albekezdésének c) pontjában említett kritérium tekintetében jelentős változás következett be, a Tanács egy vagy több tagállam kellően indokolt kezdeményezésére módosíthatja vagy hatályon kívül helyezheti a (4) bekezdés szerint elfogadott végrehajtási jogi aktust.

(6) E cikk szerinti végrehajtási hatásköreinek gyakorlása során a Tanács alkalmazza a (3) bekezdés első albekezdésében említett kritériumokat, és megmagyarázza az említett kritériumokra vonatkozó értékelését. A Tanács különösen abban az esetben, ha az (5) bekezdés második albekezdése alapján saját kezdeményezésére jár el, magyarázatot ad az említett albekezdésben említett jelentős változásra.

(7) Egy a Digitális Európa programhoz társult harmadik ország számára az uniós kiberbiztonsági tartalékból nyújtott támogatásnak meg kell felelnie az (1) bekezdésben említett megállapodásban meghatározott egyedi feltételeknek.

(8) Az uniós kiberbiztonsági tartalék szolgáltatásainak igénybevételére jogosult, a Digitális Európa programhoz társult harmadik ország felhasználói közé tartoznak az illetékes hatóságok, például a számítógép-biztonsági eseményekre reagáló csoportok vagy az azokkal egyenértékű szervezetek és a kiberválságok kezelésével foglalkozó hatóságok.

(9) Az uniós kiberbiztonsági tartalékból támogatásra jogosult minden egyes, a Digitális Európa programhoz társult harmadik ország kijelöl egy hatóságot, amely e rendelet alkalmazásában egyedüli kapcsolattartó pontként jár el.

(10) Az e cikk szerinti, az uniós kiberbiztonsági tartalékból származó támogatás iránti kérelmeket a Bizottság értékeli. Az ajánlatkérő szerv csak akkor és addig nyújthat támogatást harmadik országnak, ha és amíg az adott ország tekintetében az e cikk (4) bekezdése szerint elfogadott, ilyen támogatást engedélyező tanácsi végrehajtási jogi aktus hatályban van. A választ indokolatlan késedelem nélkül továbbítani kell a 14. cikk (3) bekezdésének c) pontjában említett felhasználóknak.

(11) Az e cikk szerinti támogatás iránti kérelem kézhezvételét követően a Bizottság haladéktalanul tájékoztatja a Tanácsot. A Bizottság folyamatosan tájékoztatja a Tanácsot a kérelem értékeléséről. A Bizottság emellett együttműködik a főképviselővel a beérkezett kérelmekkel és az uniós kiberbiztonsági tartalékból a Digitális Európa programhoz társult harmadik országoknak nyújtott támogatás végrehajtásával kapcsolatban. Ezen túlmenően a Bizottság figyelembe veszi az ENISA által az említett kérelmekkel kapcsolatban adott véleményeket is.

20. cikk

Koordináció az uniós válságkezelési mechanizmusokkal

(1) Amennyiben egy jelentős, egy nagyszabású vagy egy nagyszabásúval egyenértékű kiberbiztonsági esemény az 1313/2013/EU határozat 4. cikkének 1. pontjában meghatározottak szerinti katasztrófából ered vagy ilyen katasztrófához vezet, az e rendelet alapján az ilyen eseményre való reagáláshoz nyújtott támogatásnak ki kell egészítenie az említett határozat szerinti intézkedéseket, és nem sértheti azokat.

(2) Olyan nagyszabású vagy nagyszabásúval egyenértékű kiberbiztonsági esemény esetén, amely aktiválja az (EU) 2018/1993 végrehajtási határozat szerinti uniós politikai szintű integrált válságelhárítási mechanizmust (a továbbiakban: IPCR-mechanizmus), az e rendelet alapján az ilyen eseményre való reagáláshoz nyújtott támogatást az IPCR-mechanizmus szerinti vonatkozó eljárásokkal összhangban kell kezelni.

IV. fejezet

A kiberbiztonsági események európai felülvizsgálati mechanizmusa

21. cikk

A kiberbiztonsági események európai felülvizsgálati mechanizmusa

(1) A Bizottság vagy az EU-CyCLONe kérésére az ENISA a CSIRT-ek hálózatának támogatásával és az érintett tagállamok jóváhagyásával felülvizsgálja és értékeli az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó kiberfenyegetéseket, ismert, kihasználható sebezhetőségeket és mérséklési intézkedéseket. Egy adott kiberbiztonsági esemény felülvizsgálatának és értékelésének lezárultával az ENISA a tanulságok jövőbeli események elkerülése vagy mérséklése érdekében való levonása céljából eseményértékelési jelentést nyújt be az EU-CyCLONe-nak, a CSIRT-ek hálózatának, az érintett tagállamoknak és a Bizottságnak, hogy támogassa őket – különösen az (EU) 2022/2555 irányelv 15. és 16. cikkében foglalt – feladataik ellátásában. Amennyiben egy esemény hatással van egy, a Digitális Európa programhoz társult harmadik országra, az ENISA-nak el kell juttatnia a jelentést a Tanácsnak. A Bizottság ilyen esetekben eljuttatja a jelentést a főképviselőnek.

(2) Az e cikk (1) bekezdésében említett eseményértékelési jelentés elkészítése érdekében az ENISA együttműködik valamennyi érdekelt féllel, és visszajelzést gyűjt azoktól, beleértve a tagállamok képviselőit, a Bizottságot és más érintett uniós intézményeket, szerveket, hivatalokat és ügynökségeket, az iparágakat – többek között az irányított biztonsági szolgáltatókat –, és a kiberbiztonsági szolgáltatások felhasználóit. Az ENISA – együttműködve adott esetben a CSIRT-ekkel és releváns esetben az (EU) 2022/2555 irányelv 8. cikkének (1) bekezdése szerint kijelölt vagy létrehozott illetékes hatóságokkal – együttműködik a jelentős vagy nagyszabású kiberbiztonsági események által érintett szervezetekkel is. A konzultációba bevont képviselőknek jelezniük kell bármilyen esetleges összeférhetetlenséget.

(3) Az e cikk (1) bekezdésében említett eseményértékelési jelentésnek ki kell terjednie az adott jelentős vagy nagyszabású kiberbiztonsági esemény felülvizsgálatára és elemzésére, beleértve a fő okokat, az ismert, kihasználható sebezhetőségeket és a levont tanulságokat. Az ENISA biztosítja, hogy a jelentés megfeleljen az érzékeny vagy minősített adatok védelmére vonatkozó uniós vagy nemzeti jognak. Az esemény által érintett tagállamok vagy a 14. cikk (3) bekezdésében említett egyéb felhasználók kérésére a jelentés csak anonimizált adatokat és információkat tartalmazhat. Nem tartalmazhat semmilyen részletet az aktívan kihasznált sebezhetőségekről, amelyek továbbra is orvosolatlanok.

(4) Az eseményértékelési jelentés adott esetben ajánlásokat fogalmaz meg az Unió kiberbiztonsági helyzetének javítása érdekében, és tartalmazhat az érdekelt felektől származó bevált gyakorlatokat és levont tanulságokat.

(5) Az ENISA kiadhatja az eseményértékelési jelentés nyilvánosan hozzáférhető változatát. A jelentés említett változata csak megbízható nyilvános információkat, vagy az érintett tagállamok hozzájárulásával egyéb megbízható információkat és – a 14. cikk (3) bekezdésének b) vagy c) pontjában említett felhasználókra vonatkozó információk tekintetében – az adott felhasználó hozzájárulásával tartalmazhat.

V. fejezet
ZÁRÓ RENDELKEZÉSEK

22. cikk

Az (EU) 2021/694 rendelet módosításai

Az (EU) 2021/694 rendelet a következőképpen módosul:

1. A 6. cikk a következőképpen módosul:

a) az (1) bekezdés a következőképpen módosul:

i. a bekezdés a következő ponttal egészül ki:

„aa) az (EU) .../... európai parlamenti és tanácsi rendelettel[*+] létrehozott európai kiberbiztonsági riasztási rendszer (a továbbiakban: európai kiberbiztonsági riasztási rendszer) kialakításának támogatása, beleértve a nemzeti és a határokon átnyúló kiberközpontok fejlesztését, telepítését és működtetését, amelyek hozzájárulnak az Unión belüli helyzetismerethez és az Unió kiberfenyegetettség felderítési képességeinek megerősítéséhez;

---

[*] Az Európai Parlament és a Tanács (EU) .../... rendelete (…) a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról, és az (EU) 2021/694 rendelet módosításáról (a kiberszolidaritásról szóló rendelet) ((HL L, …, ELI: …).”;

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS 94/24 (2023/0109(COD)) dokumentumban szereplő rendelet számát, és illesszék be a lábjegyzetbe az említett rendelet számát, dátumát, HL-hivatkozását és ELI-hivatkozását.

ii. a bekezdés a következő ponttal egészül ki:

„g) a nemzeti erőforrásokat és képességeket, valamint az uniós szinten rendelkezésre álló egyéb támogatási formákat kiegészítő, az (EU) …/… rendelet[+] 10. cikkével létrehozott kiberbiztonsági vészhelyzeti mechanizmus – beleértve az említett rendelet 14. cikkével létrehozott európai kiberbiztonsági tartalékot (a továbbiakban: európai kiberbiztonsági tartalék) – létrehozása és működtetése annak érdekében, hogy támogassa a tagállamokat a jelentős és a nagyszabású kiberbiztonsági eseményekre való felkészülésben és reagálásban, és hogy támogassa az egyéb felhasználókat a jelentős és a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálásban.”;

b) a (2) bekezdés helyébe a következő szöveg lép:

„(2) A 3. sz. egyedi célkitűzés alá tartozó fellépéseket elsősorban az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont és a nemzeti koordinációs központok hálózata révén kell végrehajtani, az (EU) 2021/887 európai parlamenti és tanácsi rendelettel* összhangban. Az uniós kiberbiztonsági tartalékot azonban a Bizottság és – az (EU) .../... rendelet**[+] 14. cikkének (6) bekezdésével összhangban – az ENISA hajtja végre.

---

* Az Európai Parlament és a Tanács (EU) 2021/887 rendelete (2021. május 20.) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról (HL L 202., 2021.6.8., 1. o.).”

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS 94/24 (2023/0109(COD)) dokumentumban található rendelet számát.

2. A 9. cikk a következőképpen módosul:

a) a (2) bekezdés b), c) és d) pontja helyébe a következő szöveg lép:

„b) 1 760 806 000 EUR a 2. sz. Mesterséges intelligencia egyedi célkitűzésre;

c) 1 372 020 000 EUR a 3. sz. Kiberbiztonság és bizalom egyedi célkitűzésre;

d) 482 640 000 EUR a 4. sz. Fejlett digitális készségek egyedi célkitűzésre;”

b) a cikk a következő (8) bekezdéssel egészül ki:

„(8) A költségvetési rendelet 12. cikkének (1) bekezdésétől eltérve, az uniós kiberbiztonsági tartalék és az (EU)…/… rendelet[+] szerinti kölcsönös segítségnyújtást támogató intézkedések végrehajtásával és a kölcsönös segítségnyújtást támogató intézkedésekkel összefüggésben az e rendelet 6. cikke (1) bekezdésének g) pontjában meghatározott célkitűzések megvalósítására irányuló fellépésekre elkülönített, fel nem használt kötelezettségvállalási és kifizetési előirányzatokat automatikusan át kell vinni a következő pénzügyi évre, és terhükre a következő pénzügyi év december 31-éig kötelezettségek vállalhatók és kifizetések teljesíthetők. Az Európai Parlamentet és a Tanácsot tájékoztatni kell a költségvetési rendelet 12. cikkének (6) bekezdése szerint átvitt előirányzatokról.”

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS 94/24 (2023/0109(COD)) dokumentumban található rendelet számát.

3. A 12. cikk a következőképpen módosul:

a) a cikk a következő bekezdésekkel egészül ki:

„(5a) Az (5) bekezdés az Unióban letelepedett, de harmadik országokból irányított jogalanyok tekintetében nem alkalmazandó az európai kiberbiztonsági riasztási rendszert végrehajtó fellépésekre, amennyiben az adott fellépés tekintetében mindkét alábbi feltétel teljesül:

a) figyelembe véve az (EU) .../... rendelet[+] 9. cikkének (4) bekezdése szerint elvégzett feltérképezés eredményeit, fennáll annak a valós kockázata, hogy azok az eszközök, infrastruktúrák vagy szolgáltatások, amelyek szükségesek és elégségesek ahhoz, hogy az említett fellépés megfelelően hozzájáruljon az európai kiberbiztonsági riasztási rendszer célkitűzéséhez, nem állnak majd rendelkezésre a tagállamokban letelepedett vagy letelepedettnek tekintett és a tagállamok vagy a tagállamok állampolgárai irányítása alatt álló jogalanyok részéről;

b) az ilyen jogalanyoktól való, az európai kiberbiztonsági riasztási rendszeren belüli beszerzés biztonsági kockázata arányos az előnyökkel, és nem veszélyezteti az Unió és tagállamai alapvető biztonsági érdekeit.

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS 94/24 (2023/0109(COD)) dokumentumban szereplő rendelet számát.

(5b) Az (5) bekezdés az Unióban letelepedett, de harmadik országokból irányított jogalanyok tekintetében nem alkalmazandó az európai kiberbiztonsági tartalékot végrehajtó fellépésekre, amennyiben az érintett fellépés tekintetében mindkét alábbi feltétel teljesül:

a) figyelembe véve az (EU) .../... rendelet[+] 14. cikkének (6) bekezdése szerint elvégzett feltérképezés eredményeit, fennáll annak a valós kockázata, hogy az uniós kiberbiztonsági tartalék feladatainak megfelelő ellátásához szükséges és elégséges technológia, szakértelem vagy kapacitás nem áll majd rendelkezésre a tagállamokban letelepedett vagy letelepedettnek tekintett és a tagállamok vagy a tagállamok állampolgárai irányítása alatt álló jogalanyok részéről;

b) az ilyen jogalanyok az uniós kiberbiztonsági tartalékba való felvételének biztonsági kockázata arányos az előnyökkel, és nem ássa alá az Unió és tagállamai alapvető biztonsági érdekeit.”;

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS 94/24 (2023/0109(COD)) dokumentumban szereplő rendelet számát.

b) a (6) bekezdés helyébe a következő szöveg lép:

„(6) Ha biztonsági okokból kellően indokolt, a munkaprogram rendelkezhet úgy is, hogy társult országokban letelepedett jogalanyok és az Unióban letelepedett, de harmadik országokból irányított jogalanyok csak akkor jogosultak részt venni az 1. sz. és a 2. sz. egyedi célkitűzés alá tartozó valamennyi vagy egyes fellépésekben, ha megfelelnek az Unió és a tagállamok alapvető biztonsági érdekeinek védelmét garantáló és a minősített dokumentumokban foglalt információ védelmét biztosító, ezen jogalanyok által teljesítendő követelményeknek. Az említett követelményeket a munkaprogramban kell meghatározni.

Az első albekezdés az Unióban letelepedett, de harmadik országokból irányított jogalanyok tekintetében is alkalmazandó a 3. sz. egyedi célkitűzés alá tartozó fellépésekre:

a) az európai kiberbiztonsági riasztási rendszer végrehajtására amennyiben az (5a) bekezdés alkalmazandó; és

b) az uniós kiberbiztonsági tartalék végrehajtására amennyiben az (5b) bekezdés alkalmazandó.”

4. A 14. cikk (2) bekezdésének helyébe a következő szöveg lép:

„(2) 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.

Amennyiben valamely fellépés célkitűzésének eléréséhez innovatív termékek és szolgáltatások beszerzésére van szükség, csak olyan kedvezményezetteknek ítélhető oda vissza nem térítendő támogatás, amelyek a 2014/24/EU* és a 2014/25/EU** európai parlamenti és tanácsi irányelvben meghatározottak szerinti ajánlatkérő szervek vagy közszolgáltató ajánlatkérők.

Amennyiben valamely fellépés célkitűzéseinek eléréséhez olyan innovatív áruk vagy szolgáltatások nyújtása szükséges, amelyek kereskedelmi forgalomban nagy volumenben még nem beszerezhetők, az ajánlatkérő szerv vagy a közszolgáltató ajánlatkérő engedélyezheti ugyanazon eljárás keretében több szerződés odaítélését is.

Kellően indokolt közbiztonsági okokból az ajánlatkérő szerv vagy a közszolgáltató ajánlatkérő megkövetelheti, hogy a szerződés teljesítésének helye az Unió területén legyen.

Az uniós kiberbiztonsági tartalékra irányuló közbeszerzési eljárások lefolytatásakor a Bizottság és az ENISA központi beszerző szervként járhat el az e rendelet 10. cikkével összhangban a programhoz társult harmadik országok javára vagy nevében történő beszerzések során. A Bizottság és az ENISA nagykereskedőként is eljárhat áruk és szolgáltatások az említett harmadik országoknak történő vásárlása, készletezése, továbbértékesítése vagy adományozása révén, beleértve a bérbeadást is. Az (EU, Euratom) 2024/2509 európai parlamenti és tanácsi rendelet[***] 168. cikkének (3) bekezdésétől eltérve egyetlen harmadik ország által benyújtott kérelem elegendő ahhoz, hogy a Bizottság vagy az ENISA megbízást kapjon eljárni.

Az uniós kiberbiztonsági tartalékra irányuló közbeszerzési eljárások lefolytatásakor a Bizottság és az ENISA központi beszerző szervként járhat el az uniós intézmények, szervek, hivatalok vagy ügynökségek javára vagy nevében történő beszerzések során. A Bizottság és az ENISA nagykereskedőként is eljárhat áruk és szolgáltatások uniós intézményeknek, szerveknek, hivataloknak vagy ügynökségeknek történő vásárlása, készletezése, továbbértékesítése vagy adományozása révén, beleértve a bérbeadást is. Az (EU, Euratom) 2024/2059 rendelet[+] 168. cikkének (3) bekezdésétől eltérve egyetlen uniós intézmény, szerv, hivatal vagy ügynökség által benyújtott kérelem elegendő ahhoz, hogy a Bizottság vagy az ENISA megbízást kapjon eljárni.

A program vegyes finanszírozási műveletek keretében pénzügyi eszközök formájában is nyújthat finanszírozást.

---

* 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., 87. o.).

** Az Európai Parlament és a Tanács 2014/25/EU irányelve (2014. február 26.) a vízügyi, energiaipari, közlekedési és postai szolgáltatási ágazatban működő ajánlatkérők beszerzéseiről és a 2004/17/EK irányelv hatályon kívül helyezéséről (HL L 94., 2014.3.28., 243. o.).

*** Az Európai Parlament és a Tanács (EU, Euratom) 2024/2509 rendelete (2024. szeptember 23.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról (HL L, 2024/2059, ELI: http://data.europa.eu/eli/reg/2024/2509/oj).”

5. A rendelet a következő cikkel egészül ki:

„16a. cikk

A szabályok ütközése

Az Európai Kiberbiztonsági Riasztási Rendszert végrehajtó fellépések esetében az (EU) .../... rendelet[+] 4., 5. és 9. cikkében meghatározott szabályok alkalmazandók. Az e rendeletben és az (EU) .../... rendelet[+] 4., 5. és 9. cikkében foglalt rendelkezések ütközése esetén az utóbbiak az irányadók és alkalmazandók az említett egyedi fellépésekre.

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS CONS 94/24 (2023/0109(COD)) dokumentumban szereplő rendelet számát.

Az uniós kiberbiztonsági tartalék esetében a programhoz társult harmadik országok részvételére vonatkozó különös szabályokat az (EU).../... rendelet[+] 19. cikke állapítja meg. Az e rendeletben és az (EU) .../... rendelet[+] 19. cikkében foglalt rendelkezések ütközése esetén az utóbbiak az irányadók és alkalmazandók az említett egyedi fellépésekre.”

6. A 19. cikk helyébe a következő szöveg lép:

„19. cikk
Vissza nem térítendő támogatások

A program keretében nyújtott vissza nem térítendő támogatásokat a költségvetési rendelet VIII. címével összhangban kell odaítélni és irányítani, és azok a költségvetési rendelet 190. cikkében megállapított társfinanszírozási elv sérelme nélkül az elszámolható költségek legfeljebb 100 %-át fedezhetik. Az ilyen vissza nem térítendő támogatásokat az egyes egyedi célkitűzésekre vonatkozóan meghatározottak szerint kell odaítélni és irányítani.

A vissza nem térítendő támogatásként nyújtott támogatást az ECCC a költségvetési rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti az (EU) .../... rendelet[+] 9. cikke szerint kiválasztott tagállamoknak és az (EU) .../... rendelet[+] 5. cikkében említett üzemeltetési konzorciumnak.

A kiberbiztonsági vészhelyzeti mechanizmushoz vissza nem térítendő támogatásként nyújtandó támogatást az ECCC a költségvetési rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti a tagállamoknak.

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS CONS 94/24 (2023/0109(COD)) dokumentumban szereplő rendelet számát.

Az (EU) .../... rendelet[+] 18. cikkében előírt, a kölcsönös segítségnyújtást támogató fellépések tekintetében az ECCC tájékoztatja a Bizottságot és az ENISA-t a tagállamok pályázati felhívás nélküli közvetlen támogatásra irányuló kérelmeiről.

Az (EU) .../... rendelet[+] 18. cikkében előírt, a kölcsönös segítségnyújtást támogató fellépések tekintetében, és a költségvetési rendelet 193. cikke (2) bekezdése második albekezdésének a) pontjával összhangban kellően indokolt esetekben a költségek akkor is elszámolhatónak tekinthetők, ha azok a vissza nem térítendő támogatás elnyerésére irányuló pályázat benyújtása előtt merültek fel.”

7. Az I. és a II. melléklet e rendelet mellékletének megfelelően módosul.

23. 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 14. cikk (7) bekezdésében említett, felhatalmazáson alapuló jogi aktus elfogadására vonatkozó felhatalmazása ötéves időtartamra szól ... [e rendelet hatálybalépésének időpontja]-tól/től kezdődő hatállyal. A Bizottság legkésőbb 9 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 3 hónappal minden egyes időtartam letelte előtt.

[+] HL: Kérjük, illesszék be a szövegbe a PE-CONS CONS 94/24 (2023/0109(COD)) dokumentumban szereplő rendelet számát.

(3) Az Európai Parlament vagy a Tanács bármikor visszavonhatja a 14. 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 megállapított elvekkel összhangban 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 14. 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 2 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. Az Európai Parlament vagy a Tanács kezdeményezésére ez az időtartam 2 hónappal meghosszabbodik.

24. cikk

A bizottsági eljárás

(1) A Bizottságot az (EU) 2021/694 rendelet 31. cikkének (1) bekezdésében említett, Digitális Európa programot koordináló bizottság segíti. Ez a bizottság a 182/2011/EU rendelet értelmében vett bizottságnak minősül.

(2) Az e bekezdésre történő hivatkozáskor a 182/2011/EU rendelet 5. cikkét kell alkalmazni.

25. cikk

Értékelés és felülvizsgálat

(1) A Bizottság ... [e rendelet hatálybalépésének napjától számított 2 évvel]-ig, és azt követően legalább négyévente értékeli az e rendeletben előírt intézkedések működését, és jelentést nyújt be az Európai Parlamentnek és a Tanácsnak.

(2) Az (1) bekezdésben említett értékelés különösen a következőket értékeli:

a) a létrehozott nemzeti kiberközpontok és határokon átnyúló kiberközpontok száma, a megosztott információk köre, beleértve lehetőség szerint a CSIRT-ek hálózatának munkájára gyakorolt hatást, valamint azt, hogy ezek milyen mértékben járultak hozzá a kiberfenyegetések és -események közös uniós észlelésének és helyzetismeretének megerősítéséhez, valamint a legkorszerűbb technológiák fejlesztéséhez; a Digitális Európa program finanszírozásának felhasználása a közösen beszerzett kiberbiztonsági eszközökre, infrastruktúrára, vagy a közösen beszerzett szolgáltatásokra; és amennyiben az információk rendelkezésre állnak, a nemzeti kiberközpontok, valamint az (EU) 2022/2555 irányelv 3. cikkében említett alapvető és fontos szervezetek ágazati és ágazatközi közösségei közötti együttműködés szintje.

b) a kiberbiztonsági vészhelyzeti mechanizmus keretében a készültséget támogató intézkedések alkalmazása és hatékonysága, beleértve a képzéseket, a jelentős, a nagyszabású és a nagyszabásúval egyenértékű kiberbiztonsági eseményekre való reagálást, és az azokat követő helyreállítás megkezdését, beleértve a Digitális Európa program finanszírozásának felhasználását, valamint a kiberbiztonsági vészhelyzeti mechanizmus végrehajtása során levont tanulságokat és ajánlásokat;

c) az uniós kiberbiztonsági tartalék felhasználása és hatékonysága a felhasználók típusa tekintetében, beleértve a Digitális Európa program finanszírozásának felhasználását, a szolgáltatások igénybevételét, beleértve azok típusát is, a kérelmek megválaszolásához és az uniós kiberbiztonsági tartalék telepítéséhez szükséges átlagos idő, az események megelőzésével és az azokra való reagálással kapcsolatos felkészültségi szolgáltatásokká átalakított szolgáltatások százalékos aránya, valamint az uniós kiberbiztonsági tartalék végrehajtása során levont tanulságok és ajánlások;

d) e rendelet hozzájárulása az uniós ipar és szolgáltatások – többek között a mikrovállalkozások, valamint a kis- és középvállalkozások, továbbá az induló innovatív vállalkozások – versenyképességének megerősítéséhez a digitális gazdaságban, valamint a munkaerő kiberbiztonsági készségeinek és kapacitásainak megerősítésére irányuló átfogó célkitűzéshez való hozzájárulás.

(3) Az (1) bekezdésben említett jelentések alapján a Bizottság adott esetben jogalkotási javaslatot nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet módosítása céljából.

26. cikk

Hatálybalépés

Ez a rendelet az *Európai Unió Hivatalos Lapjában* való kihirdetését követő huszadik napon lép hatályba.

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

Kelt Brüsszelben,

az Európai Parlament részéről	*a Tanács részéről*
az elnök	*az elnök*

MELLÉKLET

Az (EU) 2021/694 rendelet a következőképpen módosul:

1. Az I. mellékletben a „3. sz. egyedi célkitűzés – Kiberbiztonság és bizalom” szakasz helyébe a következő szöveg lép:

„3. sz. egyedi célkitűzés – Kiberbiztonság és bizalom

A program ösztönzi az Unió digitális gazdaságának, társadalmának és demokráciájának biztosításához szükséges alapvető kapacitások megerősítését, kiépítését és beszerzését azáltal, hogy megerősíti az Unió kiberbiztonsági ipari potenciálját és versenyképességét, valamint javítja a magán- és a közszektor arra irányuló képességét, hogy megvédje a polgárokat és a vállalkozásokat a kiberfenyegetésektől, többek között az (EU) 2016/1148 irányelv végrehajtásának támogatásával.

Ezen célkitűzés keretében a kezdeti és adott esetben a további fellépések a következőket foglalják magukban:

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 Kiberbiztonsági Riasztási Rendszert alkotó nemzeti kiberközpontokat és a határokon átnyúló kiberközpontokat –, valamint egyéb olyan eszközökbe történő befektetések, amelyeket az állami és magánszektor rendelkezésére kell bocsátani egész Európában.

2. A meglévő technológiai kapacitások továbbfejlesztése és a tagállami kompetenciaközpontok hálózatba szervezése, valamint annak biztosítása, hogy ezen kapacitások reagáljanak a közszektorbeli és az ipari igényekre, többek között olyan termékek és szolgáltatások révén, amelyek megerősítik a kiberbiztonságot és a bizalmat a digitális egységes piacon belül.

3. Hatékony és a legkorszerűbb kiberbiztonsági és bizalmi szolgáltatások széles körű bevezetésének biztosítása a tagállamokban. Az ilyen bevezetésbe beletartozik a termékek biztonságának és védelmének megerősítése is, a tervezésüktől kezdve a kereskedelmi forgalmazásukig.

4. Támogatás a kiberbiztonsági készségek terén fennálló hiányok megszüntetéséhez, figyelembe véve a nemek közötti egyensúlyt, például a kiberbiztonsági készségeket célzó programok összhangba hozásával, azok konkrét ágazati szükségletekhez igazításával és a célzott specializált képzéshez való hozzáférés megkönnyítésével.

5. A tagállamok közötti szolidaritás előmozdítása a jelentős és a nagyszabású kiberbiztonsági eseményekre való felkészülés és reagálás terén a kiberbiztonsági szolgáltatások határokon átnyúló bevezetése révén, beleértve a hatóságok közötti kölcsönös segítségnyújtás támogatását és a megbízható irányított biztonsági szolgáltatókból álló uniós szintű tartalék létrehozását.”

2. A II. mellékletben a „3. sz. egyedi célkitűzés – Kiberbiztonság és bizalom” szakasz helyébe a következő szöveg lép:

„3. sz. egyedi célkitűzés – Kiberbiztonság és bizalom

3.1. A közösen – többek között az Európai Kiberbiztonsági Riasztási Rendszerrel összefüggésben – beszerzett kiberbiztonsági infrastruktúrák, vagy eszközök vagy mindkettő száma

3.2. Az európai kiberbiztonsági létesítményekhez hozzáféréssel rendelkező felhasználók és felhasználói közösségek száma

3.3. A kiberbiztonsági eseményekre való felkészültséget és az azokra való reagálást támogató fellépések száma a kiberbiztonsági vészhelyzeti mechanizmus keretében”

E rendelet tekintetében egy nyilatkozat megtételére került sor, amely [a Kiadóhivatal által beillesztendő: HL C XXX., 2024.XX.XX., XX. o.]-án/én található, valamint a következő linken érhető el: [Kiadóhivatal: kérjük, illesszék be a nyilatkozatra mutató linket].