Az Európai Unió
Tanácsa

Brüsszel, 2023. április 20.
(OR. en)

8512/23

Intézményközi referenciaszám:
2023/0109(COD)

CYBER 92
TELECOM 108
CADREFIN 51
FIN 448
BUDGET 6
IND 181
JAI 471
MI 314
DATAPROTECT 110
RELEX 481
CODEC 662

JAVASLAT

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2023. április 19.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2023) 209 final
Tárgy:	Javaslat – AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról

Mellékelten továbbítjuk a delegációknak a COM(2023) 209 final számú dokumentumot.

Melléklet: COM(2023) 209 final

EURÓPAI
BIZOTTSÁG

Strasbourg, 2023.4.18.
COM(2023) 209 final

2023/0109 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

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

INDOKOLÁS

1. A JAVASLAT HÁTTERE

• A javaslat indokai és céljai

Ez az indokolás a kiberszolidaritásról szóló jogszabályra irányuló javaslatot kíséri. Az információs és kommunikációs technológiák alkalmazása és az azoktól való függés alapvetően fontos tényezővé vált a gazdasági tevékenységek valamennyi ágazatában, mivel az európai közigazgatási szervek, vállalatok és polgárok ágazatok közötti és határokon átnyúló összekapcsoltságának és egymástól való függésének mértéke minden eddiginél nagyobb méreteket ölt. A digitális technológiák fokozott elterjedése növeli a kiberbiztonsági eseményeknek való kitettséget és azok lehetséges hatásait. Ugyanakkor a tagállamok növekvő kiberbiztonsági kockázatokkal és átfogó, összetett fenyegetettségi helyzettel néznek szembe, ami egyértelműen azzal a kockázattal jár, hogy a kiberbiztonsági események gyorsan tovagyűrűzhetnek az egyik tagállamból a másikba.

Ráadásul a kiberműveletek egyre inkább beépülnek a hibrid hadviselési stratégiákba, ami jelentős hatást gyakorol a célpontra. Ebben az összefüggésben Oroszország Ukrajna elleni katonai agresszióját ellenséges kiberműveleteket alkalmazó stratégia előzte meg és kíséri, ami megváltoztatja az EU kiberbiztonsági válságok kezelésére való kollektív felkészültségének megítélését és értékelését, és sürgős fellépésre szólít fel. Egy, a kritikus infrastruktúrákban jelentős fennakadásokat és károkat okozó esetleges nagyszabású kiberbiztonsági esemény veszélye az EU kiberbiztonsági ökoszisztémájának minden szintjén fokozott felkészültséget igényel. Ez a veszély túlmutat az Ukrajna elleni orosz katonai agresszión, és magában foglalja az állami és nem állami szereplőknek tulajdonítható folyamatos kiberfenyegetéseket, amelyek – tekintettel a jelenlegi geopolitikai feszültségekben közreműködő, államközeli bűnözői és haktivista körök sokféleségére – valószínűleg nem fognak alábbhagyni. Az elmúlt években drámaian megnőtt a kibertámadások száma, ideértve az ellátási láncok ellen elkövetett, kiberkémkedést, zsarolóvírusokkal való fenyegetést vagy zavarkeltést célzó támadásokat. A SolarWinds ellátási lánca ellen 2020-ban elkövetett támadás világszerte több mint 18 000 szervezetet érintett, köztük kormányzati ügynökségeket és nagyobb vállalatokat. A jelentős kiberbiztonsági események olyan súlyos zavarokat okozhatnak, amelyeket az érintett tagállam vagy tagállamok önállóan nem tudnak elhárítani. Ezért a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés és reagálás érdekében meg kell erősíteni az uniós szintű szolidaritást.

Ami a kiberbiztonsági fenyegetések és események észlelését illeti, sürgősen fokozni kell az információcserét és fejleszteni kell közös képességeinket annak érdekében, hogy – mielőtt azok jelentős károkat és költségeket okozhatnának – drasztikusan csökkenjen a kiberfenyegetések észleléséhez szükséges idő[1]. Bár számos kiberbiztonsági fenyegetés és

[1] A Ponemon Institute és az IBM Security jelentése szerint 2022-ben az adatvédelmi incidensek feltárása átlagosan 207 napot, majd felszámolásuk további 70 napot vett igénybe. Ugyanakkor 2022-ben a 200 napnál hosszabb életciklusú adatvédelmi incidensek átlagos költsége 4,86 millió EUR volt, a 200 nap alattiaké pedig 3,74 millió EUR. („Cost of a data breach 2022”, https://www.ibm.com/reports/data-breach)

esemény potenciálisan határokon átnyúló dimenzióval rendelkezik, a digitális infrastruktúrák összekapcsoltsága miatt a releváns információk tagállamok közötti megosztása továbbra is korlátozott. Az észlelési és reagálási képességek javítása céljából e probléma megoldását hivatott elősegíteni a határokon átnyúló biztonsági műveleti központok hálózatának kiépítése.

Ami a kiberbiztonsági eseményekre való felkészültséget és reagálást illeti, jelenleg korlátozott mind az uniós szintű támogatás, mind a tagállamok közötti szolidaritás. A Tanács a 2021. októberi következtetéseiben[2] kiemelte, hogy kezelni kell ezeket a hiányosságokat, és felkérte a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.

Ez a rendelet egyúttal a 2020 decemberében elfogadott uniós kiberbiztonsági stratégia[3] végrehajtását is szolgálja, amely bejelentette az Európai Kiberpajzs létrehozását, valamint a kiberfenyegetés-észlelési és az információmegosztási képességek megerősítését az Európai Unióban a nemzeti és a határokon átnyúló biztonsági műveleti központok szövetsége révén.

Ez a rendelet a főbb érdekelt felekkel szoros együttműködésben már kidolgozott és a Digitális Európa program által támogatott kezdeti lépésekre épül. A biztonsági műveleti központokat illetően a Digitális Európa program 2021–2022-es kiberbiztonsági munkaprogramja keretében részvételi szándék kifejezésére való felhívást tettek közzé a határokon átnyúló biztonsági műveleti központok létrehozásához szükséges eszközök és infrastruktúra közös beszerzésére, és ezenfelül az állami és magánszervezeteket kiszolgáló biztonsági műveleti központok kapacitásépítését előmozdító támogatási felhívást is közzétették. A felkészültség és a kiberbiztonsági eseményekre való reagálás tekintetében az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) számára elkülönített további finanszírozás révén a Bizottság a tagállamok támogatása érdekében létrehozta a súlyos kiberbiztonsági eseményekre való felkészültség és reagálási képességek azonnali megerősítését szolgáló rövid távú programot. Mindkét intézkedést a tagállamokkal szoros együttműködésben dolgozták ki. Ez a rendelet orvosolja a hiányosságokat, és integrálja az említett intézkedéseknek köszönhető tapasztalatokat.

Végezetül ez a javaslat a november 10-én elfogadott, az EU kibervédelmi politikájáról szóló közös közleménnyel[4] összhangban eleget tesz annak a kötelezettségvállalásnak, hogy előkészít egy uniós kiberszolidaritási kezdeményezésre irányuló javaslatot, amelynek céljai a következők: a közös uniós észlelési, helyzetismereti és reagálási képességek megerősítése, a megbízható magánszolgáltatók által biztosított uniós szintű kiberbiztonsági tartalék fokozatos kiépítése, valamint a kritikus szervezetek tesztelésének támogatása.

Mindezek fényében a Bizottság a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés és reagálás érdekében megerősítendő

---

[2] A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról, amelyet a Tanács a 2022. május 23-i ülésén jóváhagyott (9364/22).

[3] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kiberbiztonsági stratégiája a digitális évtizedre, JOIN(2020) 18 final.

[4] Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022) 49 final.

uniós szintű szolidaritás céljából előterjeszti a kiberszolidaritásról szóló jogszabályt, és ebben az összefüggésben a következő egyedi célkitűzéseket határozza meg:

- a kiberbiztonsági fenyegetések és események közös uniós észlelésének és helyzetismeretének megerősítése, és ezáltal hozzájárulás Európa technológiai szuverenitásához a kiberbiztonság területén;
- a kritikus szervezetek felkészültségének megerősítése Unió-szerte, valamint a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, többek között a Digitális Európa programhoz társult harmadik országok számára kiberbiztonsági eseményekre való reagáláshoz nyújtott támogatással;
- az Unió rezilienciájának fokozása és a hatékony reagáláshoz való hozzájárulás a jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése révén, beleértve a levont tanulságokat és adott esetben az ajánlásokat is.

E célkitűzések teljesítésére a következő intézkedések révén kerül sor:

- A biztonsági műveleti központok páneurópai infrastruktúrájának kiépítése (Európai Kiberpajzs) a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében.
- Egy kiberbiztonsági vészhelyzeti mechanizmus létrehozása, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az eseményt követő azonnali helyreállításban. A kiberbiztonsági eseményekre való reagáláshoz nyújtott támogatást elérhetővé kell tenni az uniós intézmények, szervek, hivatalok és ügynökségek számára is.
- A kiberbiztonsági események európai felülvizsgálati mechanizmusának létrehozása konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából.

Az Európai Kiberpajzshoz és a kiberbiztonsági vészhelyzeti mechanizmushoz a Digitális Európa program nyújt finanszírozást, amelyet ez a jogalkotási eszköz módosítani fog annak érdekében, hogy meg lehessen valósítani a fent említett intézkedéseket, pénzügyi támogatás álljon rendelkezésre a szóban forgó fejlesztésekhez, és egyértelmű feltételek mellett lehessen igénybe venni a pénzügyi támogatást.

• Összhang a szabályozási terület jelenlegi rendelkezéseivel

Az uniós keret számos, már meglévő vagy uniós szinten javasolt jogszabályt foglal magában a sebezhetőségek csökkentése, a kritikus szervezetek kiberbiztonsági kockázatokkal szembeni fokozott rezilienciája és a nagyszabású kiberbiztonsági események és válsághelyzetek összehangolt irányításának támogatása érdekében, nevezetesen az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló irányelvet (NIS 2 irányelv)[5], a

[5] 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 (NIS 2 irányelv).

kiberbiztonsági jogszabályt[6], az információs rendszerek elleni támadásokról szóló irányelvet[7], valamint a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1584 bizottsági ajánlást[8].

A kiberszolidaritásról szóló jogszabály keretében javasolt intézkedések kiterjednek a helyzetismeretre, az információmegosztásra, valamint a kiberbiztonsági eseményekre való felkészültség és reagálás támogatására. Ezek az intézkedések összhangban állnak a meglévő uniós szabályozási keret – különösen az (EU) 2022/2555 irányelv (a NIS 2 irányelv) – célkitűzéseivel, és egyúttal hozzá is járulnak azok megvalósításához. A kiberszolidaritásról szóló jogszabály elsősorban a kiberbiztonság terén már meglévő, operatív együttműködést és válságkezelést szolgáló keretekre – különösen az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatára (a továbbiakban: EU-CyCLONe) és a számítógép-biztonsági eseményekre reagáló csoportok (a továbbiakban: CSIRT-ek) hálózatára – támaszkodik, és támogatja is azokat.

A határokon átnyúló biztonsági műveleti központok platformjainak olyan új képességet kell kialakítaniuk, amely oly módon egészíti ki a CSIRT-ek hálózatát, hogy összegyűjti és megosztja az állami és magánszervezetektől származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatokat, majd szakértői elemzések és a legkorszerűbb eszközök révén növeli az ilyen adatok értékét, valamint hozzájárul az uniós képességek és az EU technológiai szuverenitásának elmélyítéséhez.

Végezetül e javaslat összhangban van a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlással[9], amely felkéri a tagállamokat, hogy hozzanak sürgős és hatékony intézkedéseket, továbbá hogy folytassanak lojális, hatékony, szolidáris és összehangolt együttműködést egymással, a Bizottsággal és más érintett hatóságokkal, valamint az érintett szervezetekkel a belső piacon az alapvető szolgáltatások nyújtásához használt kritikus infrastruktúrák fokozott rezilienciája érdekében.

- **Összhang az Unió egyéb szakpolitikáival**

A javaslat összhangban áll más válságelhárítási mechanizmusokkal és protokollokkal, például az uniós politikai szintű integrált válságelhárítási mechanizmussal (a továbbiakban: IPCR-mechanizmus). A kiberszolidaritásról szóló jogszabály a kiberbiztonsági eseményekre való

[6] 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).

[7] 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.

[8] Javaslat – Az Európai Parlament és a Tanács rendelete a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről és az (EU) 2019/1020 rendelet módosításáról, COM(2022) 454 final.

[9] A Tanács ajánlása (2022. december 8.) a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről (EGT-vonatkozású szöveg) 2023/C 20/01.

felkészültséghez és reagáláshoz nyújtott célzott támogatás révén egészíti ki ezeket a válságkezelési kereteket és protokollokat. A javaslat összhangban lesz az EU közös kül- és biztonságpolitika (KKBP) keretében – többek között az uniós kiberdiplomáciai eszköztár igénybevételével – folytatott, nagyszabású kiberbiztonsági eseményekre reagáló külső tevékenységével is. A javaslat kiegészíti az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésével összefüggésben vagy az Európai Unió működéséről szóló szerződés 222. cikkében meghatározott helyzetekben végrehajtott intézkedéseket.

Kiegészíti továbbá a 2013 decemberében létrehozott uniós polgári védelmi mechanizmust (a továbbiakban: UCPM)[10], amelyet egy új, 2021 májusában elfogadott jogszabály[11] tovább bővített, megerősítve az UCPM megelőzési, felkészültségi és reagálási pilléreit, további kapacitásokat biztosítva az EU számára ahhoz, hogy reagálni tudjon az Európában és a világban jelentkező új kockázatokra, és bővítve a rescEU-képességet.

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

• Jogalap

E javaslat jogalapja az Európai Unió működéséről szóló szerződés (a továbbiakban: EUMSZ) 173. cikkének (3) bekezdése és 322. cikke (1) bekezdésének a) pontja. Az EUMSZ 173. cikke értelmében az Unió és a tagállamok biztosítják az uniós ipar versenyképességéhez szükséges feltételek meglétét. E rendelet célja, hogy a digitalizált gazdaság egészét tekintve megerősítse az uniós ipari és szolgáltatási ágazat versenyhelyzetét, és a digitális egységes piac kiberbiztonsági szintjének megerősítése révén előmozdítsa e szektorok digitális átalakulását. Célja különösen a kritikus és a kiemelten kritikus ágazatokban érintett polgárok, vállalkozások és szervezetek növekvő, adott esetben pusztító társadalmi és gazdasági hatásokkal járó kiberbiztonsági fenyegetésekkel szembeni rezilienciájának növelése.

A javaslat az EUMSZ 322. cikke (1) bekezdésének a) pontján is alapul, mivel az (EU, Euratom) 2018/1046 európai parlamenti és tanácsi rendeletben (a továbbiakban: költségvetési rendelet)[12] foglalt évenkéntiség elvétől eltérő egyedi átviteli szabályokat tartalmaz. A hatékony és eredményes pénzgazdálkodás érdekében, valamint figyelembe véve a kiberbiztonsági környezet és a kiberfenyegetések kiszámíthatatlan, rendkívüli és egyedi jellegét, a kiberbiztonsági vészhelyzeti mechanizmus bizonyos fokú rugalmasságot igényel a költségvetési gazdálkodás tekintetében, különösen azáltal, hogy a rendeletben meghatározott célkitűzéseket megvalósító intézkedésekre előirányzott, ám fel nem használt kötelezettségvállalási és kifizetési előirányzatok automatikusan átvihetők a következő pénzügyi évre. Ez az új szabály kérdéseket vet fel a költségvetési rendelet összefüggésében,

---

[10] Az Európai Parlament és a Tanács 1313/2013/EU határozata (2013. december 17.) az uniós polgári védelmi mechanizmusról (EGT-vonatkozású szöveg).

[11] Az Európai Parlament és a Tanács (EU) 2021/836 rendelete (2021. május 20.) az uniós polgári védelmi mechanizmusról szóló 1313/2013/EU határozat módosításáról (EGT-vonatkozású szöveg).

[12] Az Európai Parlament és a Tanács (EU, Euratom) 2018/1046 rendelete (2018. július 18.) az Unió általános költségvetésére alkalmazandó pénzügyi szabályokról (HL L 193., 2018.7.30., 1. o.).

ezért azokkal a költségvetési rendelet átdolgozásáról jelenleg folyó tárgyalások keretében lehetne foglalkozni.

- **Szubszidiaritás (nem kizárólagos hatáskör esetén)**

A kiberbiztonsági fenyegetések erőteljes, határokon átnyúló jellege, valamint a határokon, ágazatokon és termékeken tovagyűrűző hatásokkal járó, egyre gyakoribb kockázatok és kiberbiztonsági események miatt a szóban forgó beavatkozás célkitűzéseit a tagállamok önállóan nem tudják hatékonyan megvalósítani, ezért uniós szintű közös fellépésre és szolidaritásra van szükség.

Az Ukrajna elleni háborúnak tulajdonítható kiberfenyegetések elhárítása során szerzett tapasztalatok, valamint a francia elnökség alatt folytatott kiberbiztonsági gyakorlat (EU CyCLES) tanulságai azt mutatják, hogy az uniós szintű szolidaritás megteremtése érdekében konkrét kölcsönös támogatási mechanizmusokat kell kidolgozni, ideértve különösen a magánszektorral való együttműködést. Ennek fényében az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetések felkérik a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.

A kiberbiztonsági fenyegetések eredményesebb észlelésére, valamint a felkészültségi és reagálási kapacitások bővítésére irányuló uniós szintű támogatások és intézkedések – a párhuzamos uniós és tagállami erőfeszítések kiküszöbölésével – hozzáadott értéket teremtenek. Ez biztosítaná a meglévő eszközök hatékonyabb kiaknázását, valamint jobb koordinációt és a levont tanulságokkal kapcsolatos információcserét eredményez. A kiberbiztonsági vészhelyzeti mechanizmus azt is előirányozza, hogy az uniós kiberbiztonsági tartalékból a Digitális Európa programhoz társult harmadik országok is részesülhessenek támogatásban.

Az uniós szinten létrehozandó és finanszírozandó különböző kezdeményezések keretében nyújtott támogatás kiegészíti, nem pedig megkettőzi a kiberbiztonsági fenyegetések és események észlelését, helyzetismeretét, és az azokra való felkészültséget és reagálást szolgáló nemzeti képességeket.

- **Arányosság**

Az intézkedések nem lépik túl a rendelet általános és egyedi célkitűzéseinek eléréséhez szükséges mértéket. Az e rendeletben foglalt intézkedések nem érintik a tagállamoknak a nemzetbiztonsággal, a közbiztonsággal, valamint a bűncselekmények megelőzésével, kivizsgálásával, felderítésével és büntetőeljárás alá vonásával kapcsolatos felelősségét. Nem érintik továbbá a kritikus és a kiemelten kritikus ágazatokban működő szervezetek azon jogi kötelezettségeit, hogy a NIS 2 irányelvvel összhangban kiberbiztonsági intézkedéseket fogadjanak el.

Az e rendelet hatálya alá tartozó intézkedések kiegészítik az említett erőfeszítéseket és intézkedéseket azáltal, hogy előmozdítják a fenyegetések eredményesebb észlelését és

elemzését szolgáló infrastruktúrák létrehozását, valamint támogatást nyújtanak a jelentős vagy nagyszabású kiberbiztonsági eseményekre való felkészültséghez és reagáláshoz.

- **A jogi aktus típusának megválasztása**

A javasolt jogi eszköz: európai parlamenti és tanácsi rendelet. Ez a legmegfelelőbb jogi eszköz, mivel – közvetlenül alkalmazandó jogi rendelkezéseinek köszönhetően – csak egy rendelet biztosíthatja az Európai Kiberpajzs és a kiberbiztonsági vészhelyzeti mechanizmus létrehozásához és működtetéséhez szükséges mértékű egységességet azáltal, hogy rendelkezik az említettek létrehozásához a Digitális Európa program keretében nyújtandó támogatásról, valamint egyértelmű feltételeket ír elő e támogatás felhasználására és allokációjára vonatkozóan.

3. AZ UTÓLAGOS ÉRTÉKELÉSEK, AZ ÉRDEKELT FELEKKEL FOLYTATOTT KONZULTÁCIÓK ÉS A HATÁSVIZSGÁLATOK EREDMÉNYEI

- **Az érdekelt felekkel folytatott konzultációk**

E rendelet intézkedéseihez a Digitális Európa program nyújt támogatást, amely széles körű konzultáció tárgyát képezte. Emellett az intézkedések alapját a főbb érdekelt felekkel szoros együttműködésben kidolgozott kezdeti lépések képezik. Ami a biztonsági műveleti központokat illeti, a Bizottság az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) keretében, a tagállamokkal szoros együttműködésben dolgozta ki a határokon átnyúló biztonsági műveleti központok platformjainak kialakításáról szóló stratégiai dokumentumot és a részvételi szándék kifejezésére való felhívást. Ezzel összefüggésben felmérést végeztek a nemzeti biztonsági műveleti központok kapacitásairól, és az ECCC tagállami képviselőkből álló technikai munkacsoportja keretében megvitatták a közös megközelítéseket és a technikai követelményeket. Emellett az ágazat képviselőivel is egyeztettek, nevezetesen az ENISA és az Európai Kiberbiztonsági Szervezet (ECSO) által létrehozott, biztonsági műveleti központokkal foglalkozó szakértői csoport keretében.

Másodszor, a felkészültség és a kiberbiztonsági eseményekre való reagálás tekintetében a Digitális Európa program forrásaiból az ENISA számára elkülönített további finanszírozás révén a Bizottság a tagállamok támogatása érdekében létrehozta a súlyos kiberbiztonsági eseményekre való felkészültség és reagálási képességek azonnali megerősítését szolgáló rövid távú programot. A rövid távú program végrehajtása során a tagállami és az ágazati szereplőktől kért visszajelzések már ebben a szakaszban is értékes meglátásokkal szolgálnak, így ezeket a feltárt hiányosságok kezelése érdekében figyelembe vették a rendeletjavaslat előkészítése során. Az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a Bizottság felkérést kapott, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan; e felkérés nyomán az említett program jelentette a kezdeti lépést.

Emellett egy vitaanyag alapján 2023. február 16-án munkaértekezletre került sor, amelynek keretében tagállami szakértők részvételével folytattak eszmecserét a kiberbiztonsági vészhelyzeti mechanizmusról. A munkaértekezleten valamennyi tagállam részt vett, tizenegy tagállam pedig írásban további észrevételeket is benyújtott.

- **Hatásvizsgálat**

A javaslat sürgős jellegére tekintettel nem került sor hatásvizsgálatra. E rendelet intézkedéseihez a Digitális Európa program nyújt támogatást, és az intézkedések összhangban állnak a Digitális Európa programról szóló, célzott hatásvizsgálatnak alávetett rendelettel. Ez a rendelet a Digitális Európa programról szóló rendelet hatásvizsgálatában már értékelteken felül nem jár jelentős adminisztratív vagy környezeti hatásokkal.

Emellett a főbb érdekelt felekkel szoros együttműködésben kidolgozott, fent említett kezdeti intézkedésekre épül, és a Bizottság válasza arra a tagállami felkérésre, hogy 2022 harmadik negyedévének végéig nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.

Konkrétabban, az Európai Kiberpajzs égisze alatt végzendő helyzetismereti és észlelési tevékenységeket illetően a Digitális Európa program 2021–2022-es kiberbiztonsági munkaprogramja keretében részvételi szándék kifejezésére való felhívást tettek közzé a határokon átnyúló biztonsági műveleti központok létrehozásához szükséges eszközök és infrastruktúra közös beszerzésére, és ezenfelül az állami és magánszervezeteket kiszolgáló biztonsági műveleti központok kapacitásépítését előmozdító támogatási felhívást is közzétették.

A felkészültség és a kiberbiztonsági eseményekre való reagálás területén a Bizottság létrehozta a fent már említett, a tagállamokat a Digitális Európa program révén támogató rövid távú programot, amelyet az ENISA hajt végre. A program többek között olyan felkészültségi intézkedéseket is magában foglal, mint a kritikus szervezeteknél a sebezhetőségek azonosítása végett végzett behatolási tesztelés. A program emellett szélesebb körű lehetőségeket biztosít a tagállamoknak való segítségnyújtásra a kritikus szervezeteket érintő súlyos kiberbiztonsági események esetén. Az ENISA megkezdte e rövid távú program végrehajtását, és az ennek eredményeképpen felmerült releváns meglátásokat figyelembe vették e rendelet előkészítése során.

- **Alapjogok**

A digitális információk biztonságához való hozzájárulás révén e javaslat az Európai Unió Alapjogi Chartájának 6. cikkével összhangban elő fogja mozdítani a szabadsághoz és a biztonsághoz való jog védelmét, csakúgy mint a magán- és a családi élet tiszteletben tartásához való, az Európai Unió Alapjogi Chartájának 7. cikke szerinti jogot. A javaslat védelmet nyújt a vállalkozásoknak a gazdasági károkat okozó kibertámadásokkal szemben, így az Európai Unió Alapjogi Chartájának 16. cikkével összhangban hozzájárul a vállalkozás szabadságához, az Európai Unió Alapjogi Chartájának 17. cikkével összhangban pedig a

tulajdonhoz való joghoz is. Végezetül a kritikus infrastruktúrák integritásának kibertámadásokkal szembeni védelme révén a javaslat hozzá fog járulni az Európai Unió Alapjogi Chartájának 35. cikke szerinti egészségügyi ellátáshoz való joghoz, valamint az Európai Unió Alapjogi Chartájának 36. cikke szerinti, az általános gazdasági érdekű szolgáltatásokhoz való hozzáféréshez való joghoz.

4. KÖLTSÉGVETÉSI VONZATOK

E rendelet intézkedéseit a Digitális Európa program „Kiberbiztonság” stratégiai célkitűzése keretében rendelkezésre álló forrásokból finanszírozzák.

A teljes költségvetés 100 millió EUR összeggel bővül, amelyet e rendeletjavaslat értelmében a Digitális Európa program más stratégiai célkitűzéseiből csoportosítanak át. Így a Digitális Európa program keretében a kiberbiztonsági intézkedésekre rendelkezésre álló új teljes összeg 842,8 millió EUR összegre módosul.

A további 100 millió EUR egy részét az ECCC által kezelt költségvetés bővítésére fordítják, hogy a kompetenciaközpont munkaprogramja(i) részeként a biztonsági műveleti központokkal és a felkészültséggel kapcsolatos intézkedéseket hajtson végre. A kiegészítő finanszírozás emellett az uniós kiberbiztonsági tartalék létrehozásának támogatására is szolgál majd.

Kiegészíti a hasonló intézkedésekre a Digitális Európa program egészére fordítandó, illetve a Digitális Európa program kiberbiztonsági célkitűzésére vonatkozó munkaprogramban a 2023–2027-es időszak tekintetében már előirányzott költségvetést, így a javaslat értelmében a 2023–2027-es időszakra a teljes összeg 551 millió EUR-t tesz ki, míg 115 millió EUR-t már korábban elkülönítettek a 2021–2022-es időszakban folytatott kísérleti projektekre. A tagállami hozzájárulásokat is figyelembe véve a teljes költségvetés elérheti az 1,109 milliárd eurót.

A felmerülő költségek áttekintését az e javaslatot kísérő pénzügyi kimutatás tartalmazza.

5. EGYÉB ELEMEK

- **Végrehajtási tervek, valamint a nyomon követés, az értékelés és a jelentéstétel szabályai**

A Bizottság nyomon fogja követni ezen új rendelkezések végrehajtását, alkalmazását és az azoknak való megfelelést azzal a céllal, hogy értékelje eredményességüket. A Bizottság az e rendelet alkalmazásának kezdőnapjától számított négy éven belül jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a rendelet értékeléséről és felülvizsgálatáról.

- **A javaslat egyes rendelkezéseinek részletes magyarázata**

Általános célkitűzések, tárgy és fogalommeghatározások (I. fejezet)

Az I. fejezet meghatározza a rendelet célkitűzéseit, amelyek a következők: a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés és reagálás érdekében az uniós szintű szolidaritás megerősítése, és különösen a kiberbiztonsági fenyegetések és események közös uniós észlelésének és helyzetismeretének megerősítése, a kritikus és a kiemelten kritikus ágazatokban működő szervezetek felkészültségének megerősítése Unió-szerte, a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, valamint az Unió rezilienciájának fokozása a jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése révén. Ez a fejezet azokat az intézkedéseket is meghatározza, amelyek révén e célkitűzések megvalósulnak: az Európai Kiberpajzs kiépítése, egy kiberbiztonsági vészhelyzeti mechanizmus létrehozása, valamint a kiberbiztonsági események felülvizsgálati mechanizmusának létrehozása. A fejezet tartalmazza továbbá a jogalkotási eszközben használt fogalmak meghatározását.

Európai Kiberpajzs (II. fejezet)

A II. fejezet létrehozza az Európai Kiberpajzsot, meghatározza annak különféle elemeit, és rögzíti a részvétel feltételeit. Először is meghatározza az Európai Kiberpajzs átfogó célkitűzését – fejlett uniós képességek kialakítása az Unión belüli kiberbiztonsági fenyegetések és események észlelése, elemzése és a vonatkozó adatok feldolgozása érdekében –, továbbá megállapítja a konkrét operatív célkitűzéseket is. Előírja, hogy az Európai Kiberpajzshoz nyújtott uniós finanszírozást a Digitális Európa programról szóló rendelettel összhangban kell végrehajtani.

A fejezet ismerteti továbbá az Európai Kiberpajzsot alkotó szervezetek típusait. A pajzs a nemzeti biztonsági műveleti központokat (a továbbiakban: nemzeti SOC-k) és a határokon átnyúló biztonsági műveleti központokat (a továbbiakban: határokon átnyúló SOC-k) foglalja magában. A nemzeti biztonsági műveleti központokat az egyes részt vevő tagállamok jelölik ki. A nemzeti biztonsági műveleti központ referenciapontként és átjáróként szolgál a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos információkat gyűjtő és elemző, valamint a határokon átnyúló biztonsági műveleti központokhoz hozzájáruló más nemzeti szintű állami és magánszervezetek számára. Az ECCC részvételi szándék kifejezésére való felhívás nyomán kiválaszthatja a nemzeti biztonsági műveleti központot, hogy részt vegyen az eszközök és infrastruktúrák ECCC-vel közösen bonyolított közbeszerzésében, és támogatásban részesüljön az eszközök és infrastruktúrák működtetéséhez. Ha egy nemzeti SOC uniós támogatásban részesül, kötelezettséget vállal arra, hogy két éven belül pályázik valamely határokon átnyúló biztonsági műveleti központban való részvételre.

A határokon átnyúló biztonsági műveleti központokat konzorciumok alkotják, legalább három, nemzeti biztonsági műveleti központ által képviselt tagállam részvételével, amelyek kötelezettséget vállalnak arra, hogy együttműködnek a kibertámadások észlelését és a fenyegetettség nyomon követését célzó tevékenységeik összehangolása terén. A részvételi szándék kifejezésére való előzetes felhívást követően az ECCC kiválaszthatja az üzemeltetési konzorciumot, hogy részt vegyen az eszközök és infrastruktúrák ECCC-vel közösen

bonyolított közbeszerzésében, és támogatásban részesüljön az eszközök és infrastruktúrák működtetéséhez. Az üzemeltetési konzorcium tagjai írásos konzorciumi megállapodást kötnek, amely meghatározza belső szabályaikat. A fejezet részletezi továbbá a határokon átnyúló biztonsági műveleti központok résztvevői közötti, a határokon átnyúló biztonsági műveleti központok közötti, valamint az érintett uniós szervezetekkel való információmegosztásra vonatkozó követelményeket. A valamely határokon átnyúló biztonsági műveleti központban részt vevő nemzeti biztonsági műveleti központok megosztják egymással a kiberfenyegetésekkel kapcsolatos releváns információkat; az ezzel kapcsolatos részleteket – beleértve a jelentős mennyiségű adat megosztására vonatkozó kötelezettségvállalást és a kapcsolódó feltételeket – a konzorciumi megállapodásban kell meghatározni. A határokon átnyúló biztonsági műveleti központoknak gondoskodniuk kell arról, hogy egymás között magas szintű interoperabilitást alakítsanak ki. A határokon átnyúló biztonsági műveleti központoknak ezenfelül az információmegosztás elveit meghatározó együttműködési megállapodásokat kell kötniük más határokon átnyúló biztonsági műveleti központokkal is. Ha a határokon átnyúló biztonsági műveleti központok információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a releváns információkat az (EU) 2022/2555 irányelv szerinti válságkezelési szerepük figyelembevételével eljuttatják az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak. Végül a II. fejezet az Európai Kiberpajzsban való részvétel biztonsági feltételeit határozza meg.

Kiberbiztonsági vészhelyzeti mechanizmus (III. fejezet)

A III. fejezet létrehozza a kiberbiztonsági vészhelyzeti mechanizmust, amelynek célja az Unió súlyos kiberbiztonsági fenyegetésekkel szembeni rezilienciájának javítása, valamint a szolidaritás szellemében a jelentős és nagyszabású kiberbiztonsági események vagy válsághelyzetek rövid távú hatásaira való felkészülés és e hatások enyhítése. A kiberbiztonsági vészhelyzeti mechanizmust végrehajtó intézkedésekhez a Digitális Európa program nyújt finanszírozást. A mechanizmus rendelkezik a felkészültséget támogató intézkedésekről, beleértve a kiemelten kritikus ágazatokban működő szervezetek összehangolt tesztelését, a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást, illetve a jelentős kiberbiztonsági fenyegetések mérséklését és a kölcsönös segítségnyújtási intézkedéseket.

A kiberbiztonsági vészhelyzeti mechanizmus felkészültségi intézkedései magukban foglalják a kiemelten kritikus ágazatokban működő szervezetek összehangolt felkészültségi tesztelését. A Bizottságnak az ENISA-val és a Kiberbiztonsági Együttműködési Csoporttal folytatott konzultációt követően rendszeresen azonosítania kell az (EU) 2022/2555 irányelv I. mellékletében felsorolt, kiemelten kritikus ágazatok közül azokat a releváns ágazatokat, illetve alágazatokat, amelyeket érintően uniós szinten összehangolt felkészültségi tesztelés végezhető.

A kiberbiztonsági eseményekre való reagálással kapcsolatos javasolt intézkedések végrehajtása céljából ez a rendelet létrehozza az uniós kiberbiztonsági tartalékot, amely az e rendeletben meghatározott kritériumok alapján kiválasztott megbízható szolgáltatók

eseményreagálási szolgáltatásaiból áll össze. Az uniós kiberbiztonsági tartalék szolgáltatásainak felhasználói közé tartoznak a tagállamok kiberbiztonsági válságkezelő hatóságai, a CSIRT-ek, valamint az uniós intézmények, szervek és ügynökségek. A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért, és részben vagy egészben az ENISA-t bízhatja meg az uniós kiberbiztonsági tartalék működtetésével és igazgatásával.

Ahhoz, hogy a felhasználók támogatást kapjanak az uniós kiberbiztonsági tartalékból, saját intézkedéseket kell hozniuk annak érdekében, hogy enyhítsék a támogatás iránti kérelem tárgyát képező esemény hatásait. Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmeknek tartalmazniuk kell az eseményre és a felhasználók által már meghozott intézkedésekre vonatkozó szükséges és releváns információkat. A fejezet a végrehajtás módozatait is ismerteti, beleértve az uniós kiberbiztonsági tartalékhoz benyújtott kérelmek értékelését is.

A rendelet rendelkezik továbbá az uniós kiberbiztonsági tartalék megbízható szolgáltatóira vonatkozó közbeszerzési elvekről és kiválasztási szempontokról.

Az uniós kiberbiztonsági tartalék nyújtotta támogatást harmadik országok is kérelmezhetik, ha a velük kötött társulási megállapodás a Digitális Európa programban való részvételükről ekképpen rendelkezik. Ez a fejezet az ilyen részvétel további feltételeit és módozatait is ismerteti.

A kiberbiztonsági események felülvizsgálati mechanizmusa (IV. fejezet)

A Bizottság, az EU-CyCLONe vagy a CSIRT-ek hálózatának kérésére az ENISA-nak felül kell vizsgálnia és értékelnie kell az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó fenyegetéseket, sebezhetőségeket és mérséklési intézkedéseket. A felülvizsgálatot és az értékelést az ENISA-nak a CSIRT-ek hálózatának, az EU-CyCLONe-nak és a Bizottságnak szóló eseményértékelési jelentés formájában kell elkészítenie, hogy támogassa őket feladataik ellátásában. Ha az esemény harmadik országgal kapcsolatos, a Bizottságnak meg kell osztania a jelentést a főképviselővel. A jelentésnek tartalmaznia kell a levont tanulságokat és adott esetben az Unió kiberbiztonsági helyzetének javítására vonatkozó ajánlásokat.

Záró rendelkezések (V. fejezet)

Az V. fejezet tartalmazza a Digitális Európa programról szóló rendelet módosításait, valamint előírja, hogy a Bizottságnak rendszeres jelentéseket kell benyújtania az Európai Parlamentnek és a Tanácsnak a rendelet értékeléséről és felülvizsgálatáról. A Bizottság felhatalmazást kap arra, hogy a 21. cikkben említett vizsgálóbizottsági eljárás keretében végrehajtási jogi aktusokat fogadjon el a következő célokból: a határokon átnyúló biztonsági műveleti központok közötti interoperabilitás feltételeinek meghatározása; a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos információknak a határokon átnyúló biztonsági műveleti központok és az uniós szervezetek közötti megosztására vonatkozó eljárási szabályok meghatározása; technikai követelmények

meghatározása az infrastruktúra magas szintű adatbiztonsága és fizikai biztonsága érdekében, továbbá az Unió biztonsági érdekeinek védelme érdekében az információk olyan szervezetekkel való megosztása során, amelyek nem tagállami közjogi szervek; az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának meghatározása; valamint az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályok pontosítása.

2023/0109 (COD)

Javaslat

AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE

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

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,

mivel:

(1) Az információs és kommunikációs technológiák alkalmazása és az azoktól való függés alapvetően fontos tényezővé vált a gazdasági tevékenységek valamennyi ágazatában, mivel az európai közigazgatási szervek, vállalatok és polgárok ágazatok közötti és határokon átnyúló összekapcsoltságának és egymástól való függésének mértéke minden eddiginél nagyobb méreteket ölt.

(2) A kiberbiztonsági események nagyságrendje, gyakorisága és hatása egyre számottevőbb, ideértve az ellátási láncok ellen elkövetett, kiberkémkedést, zsarolóvírusokkal való fenyegetést vagy zavarkeltést célzó támadásokat. E jelenségek komoly veszélyt jelentenek a hálózati és információs rendszerek működésére nézve. Tekintettel a fenyegetettségi helyzet gyorsan változó jellegére, a kritikus infrastruktúrákban jelentős fennakadásokat vagy károkat okozó esetleges nagyszabású kiberbiztonsági események veszélye az EU kiberbiztonsági keretének minden szintjén fokozott felkészültséget igényel. Ez a veszély túlmutat az Ukrajna elleni orosz katonai agresszión, és tekintettel a jelenlegi geopolitikai feszültségekben közreműködő, államközeli bűnözői és haktivista körök sokféleségére, valószínűleg nem fog alábbhagyni. Az ilyen események akadályozhatják a közszolgáltatások nyújtását és a gazdasági tevékenységek folytatását – többek között a kritikus, illetve a kiemelten kritikus ágazatokban –, jelentős pénzügyi veszteségeket idézhetnek elő, alááshatják a felhasználók bizalmát, jelentős károkat okozhatnak az Unió gazdaságában, és akár egészségügyi vagy az emberi életet veszélyeztető következményekkel is járhatnak.

[1] HL C […]., […]., […]. o.
[2] HL C […]., […]., […]. o.
[3] HL C […]., […]., […]. o.

Ezenkívül a kiberbiztonsági események kiszámíthatatlanok, mivel gyakran igen rövid időn belül alakulnak ki és eszkalálódnak, nem korlátozódnak egy adott földrajzi területre, hiszen több országot érintően egyidejűleg is előfordulhatnak vagy gyorsan terjedhetnek.

(3) Szükséges a digitalizált gazdaság egészét tekintve megerősíteni az uniós ipari és szolgáltatási ágazat versenyhelyzetét, és a digitális egységes piac kiberbiztonsági szintjének megerősítése révén előmozdítani e szektorok digitális átalakulását. Az Európa jövőjéről szóló konferencia[4] három különböző javaslatában is szerepelt az ajánlás, miszerint növelni kell a polgárok, a vállalkozások és a kritikus infrastruktúrákat működtető szervezetek növekvő, adott esetben pusztító társadalmi és gazdasági hatásokkal járó kiberbiztonsági fenyegetésekkel szembeni rezilienciáját. Ezért olyan infrastruktúrákba és szolgáltatásokba történő beruházásokra van szükség, amelyek támogatják a kiberbiztonsági fenyegetések és események mielőbbi észlelését és az azokra való gyorsabb reagálást, továbbá a tagállamoknak segítségre van szükségük ahhoz, hogy jobban felkészüljenek és hatékonyabban reagáljanak a jelentős és nagyszabású kiberbiztonsági eseményekre. Az Uniónak e területeken is meg kell erősítenie képességeit, különösen a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos adatok gyűjtése és elemzése tekintetében.

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

(5) A növekvő kiberbiztonsági kockázatok és az általánosságban összetett fenyegetettségi helyzet okán – amely egyértelműen azzal a kockázattal jár, hogy a kiberbiztonsági események gyorsan tovagyűrűzhetnek az egyik tagállamból a másikba, illetve valamely harmadik országból az Unióba – a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés és reagálás érdekében meg kell erősíteni az uniós szintű szolidaritást. Az Európai Unió

---

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

5 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.).

6 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.).

7 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.).

8 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.).

kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben[9] a tagállamok felkérték a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan.

(6) Az EU kibervédelmi politikájáról szóló, 2022. november 10-én elfogadott közös közlemény[10] bejelentette az uniós kiberszolidaritási kezdeményezést, amelynek céljai a következők: a biztonsági műveleti központok (a továbbiakban: SOC-k) alkotta uniós infrastruktúra kiépítésének előmozdítása révén a közös uniós észlelési, helyzetismereti és reagálási képességek megerősítése, a megbízható szolgáltatók szolgáltatásait igénybe vevő uniós szintű kiberbiztonsági tartalék fokozatos kiépítésének támogatása, valamint a kritikus szervezetek uniós kockázatértékeléseken alapuló tesztelése az esetleges sebezhetőségek tekintetében.

(7) Unió-szerte meg kell erősíteni a kiberbiztonsági fenyegetések és események észlelését és helyzetismeretét, valamint a tagállamok és az Unió jelentős és nagyszabású kiberbiztonsági eseményekre való felkészültségét és reagálását szolgáló képességeinek javítása révén meg kell erősíteni a szolidaritást is. Ezért a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében ki kell építeni a biztonsági műveleti központok páneurópai infrastruktúráját (a továbbiakban: Európai Kiberpajzs). Létre kell hozni a kiberbiztonsági vészhelyzeti mechanizmust, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az azonnali helyreállításban. Létre kell hozni a kiberbiztonsági események felülvizsgálati mechanizmusát konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából. Ezek az intézkedések nem érintik az Európai Unió működéséről szóló szerződés (EUMSZ) 107. és 108. cikkét.

(8) E célkitűzések elérése érdekében bizonyos területeket érintően módosítani kell az (EU) 2021/694 európai parlamenti és tanácsi rendeletet[11] is. Konkrétabban, e rendeletnek módosítania kell az (EU) 2021/694 rendeletet annak érdekében, hogy a Digitális Európa program 3. sz. egyedi célkitűzését kiegészítse az Európai Kiberpajzshoz és a kiberbiztonsági vészhelyzeti mechanizmushoz kapcsolódó új operatív célkitűzésekkel, amelynek célja a digitális egységes piac rezilienciájának, 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 megerősítése. Ezenfelül meg kell állapítani azokat az egyedi feltételeket, amelyek mellett pénzügyi támogatás nyújtható az említett intézkedésekhez, és meg kell határozni a célkitűzések eléréséhez szükséges irányítási és koordinációs mechanizmusokat is. 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 e rendelet szerinti intézkedések finanszírozásáról az (EU) 2021/694 rendelet rendelkezik, amely változatlanul a Digitális Európa program 3. sz. egyedi

---

9 A Tanács következtetései az Európai Unió kiberbiztonsági helyzetének javításáról, amelyet a Tanács a 2022. május 23-i ülésén jóváhagyott (9364/22).

10 Közös közlemény az Európai Parlamentnek és a Tanácsnak – Az EU kibervédelmi politikája, JOIN(2022) 49 final.

11 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.).

célkitűzésében foglalt intézkedések releváns alap-jogiaktusának számít. Az (EU) 2021/694 rendelet alkalmazandó rendelkezéseivel összhangban a vonatkozó munkaprogramok határozzák meg az egyes intézkedések egyedi részvételi feltételeit.

(10) Erre a rendeletre az Európai Parlament és a Tanács által az EUMSZ 322. cikke alapján elfogadott horizontális költségvetési szabályok alkalmazandók. E szabályokat a költségvetési rendelet 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 meghatározott általános feltételrendszert is magukban foglalják.

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

(12) A kiberbiztonsági fenyegetések és események eredményesebb megelőzése és értékelése, valamint az azokra való hatékonyabb reagálás érdekében átfogóbb ismereteket kell kialakítani az Unió területén található stratégiai eszközöket és kritikus infrastruktúrákat fenyegető veszélyekről, beleértve azok földrajzi elhelyezkedését, összekapcsoltságát és az ezen infrastruktúrákat érintő kibertámadások lehetséges hatásait is. Ki kell építeni a biztonsági műveleti központok nagyszabású uniós infrastruktúráját (a továbbiakban: Európai Kiberpajzs), amelyet olyan interoperabilitás jellemezte, határokon átnyúló platformok alkotnak, amelyek mindegyike több nemzeti biztonsági műveleti központot tömörít. Ennek a korszerű technológiákra támaszkodó fejlett adatgyűjtési és -elemzési eszközöket használó, a kiberfenyegetések észlelésére és kezelésére irányuló képességeket javító, és valós idejű helyzetismeretet biztosító infrastruktúrának a nemzeti és uniós kiberbiztonsági érdekeket és igényeket kell szolgálnia. Az infrastruktúra a kiberbiztonsági fenyegetések és események fokozott észlelését hivatott előmozdítani, és ezáltal kiegészíteni és támogatni az Unión belüli válságkezelésért felelős uniós szervezeteket és hálózatokat, nevezetesen az (EU) 2022/2555 európai parlamenti és tanácsi irányelvben[12] meghatározott Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (a továbbiakban: EU-CyCLONe).

(13) Minden tagállamnak ki kell jelölnie egy nemzeti szintű közjogi szervet, amelynek feladata a kiberfenyegetés-észlelési tevékenységek összehangolása az adott tagállamban. Ezeknek a nemzeti biztonsági műveleti központoknak nemzeti szinten referenciapontként és átjáróként kell szolgálniuk az Európai Kiberpajzsban való részvételhez, és biztosítaniuk kell, hogy az állami és magánszervezetektől származó,

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

kiberfenyegetésekkel kapcsolatos információkat nemzeti szinten hatékonyan és egységesen osszák meg és gyűjtsék össze.

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

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

(16) A határokon átnyúló biztonsági műveleti központoknak olyan központi pontként kell működniük, amely lehetővé teszi a releváns adatok és kiberfenyegetettségi információk kiterjedt gyűjtését, és a szóban forgó információk különféle szereplők közötti (pl. hálózatbiztonsági vészhelyzeteket elhárító csoportok (CERT), CSIRT-ek, információmegosztó és -elemző központok (ISAC), kritikus infrastruktúrák üzemeltetői) széles körű terjesztését. A határokon átnyúló biztonsági műveleti központok résztvevői közötti információcsere kiterjedhet a hálózatokból és érzékelőkből származó adatokra, a kiberfenyegetettségi információk hírcsatornáira, a fertőzöttségi mutatókra, valamint a kiberbiztonsági eseményekre, fenyegetésekre és sebezhetőségekre vonatkozó, kontextusba helyezett információkra. Emellett a határokon átnyúló biztonsági műveleti központoknak együttműködési megállapodásokat kell kötniük más határokon átnyúló biztonsági műveleti központokkal is.

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

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

(18) Az Európai Kiberpajzsban 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, valamint a biztonságos kommunikációs csatornákat, az alkalmazási réteg minimális biztonsági szintjét, a helyzetismereti jelzőrendszert és a mutatókat. A kiberbiztonsági események technikai okait és hatásait leíró helyzetjelentések egységes taxonómiájának és sablonjának elfogadása kapcsán figyelembe kell venni az események bejelentésével kapcsolatban az (EU) 2022/2555 irányelv végrehajtásával összefüggésben már folyamatban lévő munkát.

(19) Annak érdekében, hogy a különböző forrásokból származó, kiberbiztonsági fenyegetésekkel kapcsolatos adatcserére széles körben és megbízható környezetben kerülhessen sor, az Európai Kiberpajzsban részt vevő szervezeteket korszerű és rendkívül biztonságos eszközökkel, berendezésekkel és infrastruktúrákkal kell felszerelni. Ez várhatóan lehetővé teszi a közös észlelési képességek javítását és a hatóságok és az érintett szervezetek időben történő figyelmeztetését, különösen a legkorszerűbb mesterségesintelligencia- és adatelemzési technológiák alkalmazásával.

(20) Az Európai Kiberpajzs az adatgyűjtésnek, -megosztásnak és -cserének köszönhetően várhatóan meg fogja erősíteni az Unió technológiai szuverenitását. A kiváló minőségű gondozott adatok összevonása minden bizonnyal hozzájárul a fejlett mesterségesintelligencia- és adatelemzési technológiák fejlesztéséhez is. Ezt az Európai Kiberpajzsnak az (EU) 2021/1173 tanácsi rendelettel[13] létrehozott páneurópai nagy teljesítményű számítástechnikai infrastruktúrával való összekapcsolása révén kell elősegíteni.

(21) Jóllehet az Európai Kiberpajzs polgári projekt, a kibervédelmi közösség számára is előnyt jelenthetnek a kritikus infrastruktúrák védelmére kifejlesztett, erősebb polgári észlelési és helyzetismereti képességek. A határokon átnyúló biztonsági műveleti központoknak a Bizottság és az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) támogatásával, valamint az Unió külügyi és biztonságpolitikai főképviselőjének (a továbbiakban: főképviselő) közreműködésével a kibervédelmi közösséggel való együttműködés érdekében célzott

[13] A Tanács (EU) 2021/1173 rendelete (2021. július 13.) az európai nagy teljesítményű számítástechnikával foglalkozó közös vállalkozás létrehozásáról és az (EU) 2018/1488 rendelet hatályon kívül helyezéséről (HL L 256., 2021.7.19., 3. o.).

protokollokat és szabványokat kell fokozatosan kidolgozniuk, beleértve az ellenőrzési és biztonsági feltételeket is. Az Európai Kiberpajzsnak a főképviselővel szoros együttműködésben folytatott fejlesztését olyan szemléletnek kell kísérnie, amely lehetővé teszi a kibervédelmi közösségen belüli információmegosztásért felelős hálózatokkal és platformokkal való együttműködést.

(22) Az Európai Kiberpajzs résztvevői közötti információmegosztásnak meg kell felelnie a meglévő jogi követelményeknek, különösen az uniós és nemzeti adatvédelmi jogszabályoknak, 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 szervet arról, hogy az adatokat megsemmisítették.

(23) Az EUMSZ 346. cikkének sérelme nélkül az uniós vagy nemzeti szabályok értelmében bizalmas információk cseréjét az információcsere célja szempontjából releváns és azzal arányos információkra kell korlátozni. A szóban forgó információcsere során meg kell őrizni az információk bizalmas jellegét, és a kereskedelmi és üzleti titkok teljes körű tiszteletben tartása mellett óvni kell az érintett szervezetek biztonsági és kereskedelmi érdekeit.

(24) Tekintettel arra, hogy a tagállamokat érintő kiberbiztonsági események egyre nagyobb kockázatot jelentenek és egyre gyakoribbak, létre kell hozni egy válsághelyzetek kezelését célzó támogatási eszközt, amely javítja az Unió jelentős és nagyszabású kiberbiztonsági eseményekkel szembeni rezilienciáját, és a felkészültséghez, a reagáláshoz és az alapvető szolgáltatások azonnali helyreállításához nyújtott vészhelyzeti pénzügyi támogatás révén kiegészíti a tagállamok intézkedéseit. Ennek az eszköznek lehetővé kell tennie a meghatározott körülmények közötti és egyértelmű feltételek melletti gyors segítségnyújtást, valamint a források felhasználásának részletes nyomon követését és értékelését. Míg a kiberbiztonsági események és válsághelyzetek megelőzése, valamint az azokra való felkészülés és reagálás elsősorban a tagállamok feladata, a kiberbiztonsági vészhelyzeti mechanizmus az Európai Unióról szóló szerződés (a továbbiakban: EUSZ) 3. cikkének (3) bekezdésével összhangban előmozdítja a tagállamok közötti szolidaritást.

(25) Jelentős és nagyszabású kiberbiztonsági eseményekre való reagálás alkalmával és az eseményt követő azonnali helyreállítás során a kiberbiztonsági vészhelyzeti mechanizmusnak a tagállami intézkedéseket és erőforrásokat, valamint a rendelkezésre álló egyéb támogatási lehetőségeket – például az Európai Uniós Kiberbiztonsági Ügynökség (a továbbiakban: ENISA) által a megbízatásával összhangban nyújtott szolgáltatásokat, a CSIRT-ek hálózata nyújtotta összehangolt reagálást és segítséget, az EU-CyCLONe mérséklési támogatását, valamint a tagállamok közötti, többek között az EUSZ 42. cikkének (7) bekezdésével összefüggésben az állandó strukturált együttműködés (PESCO) kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportjai[14] és a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatai keretében nyújtott kölcsönös segítségnyújtást – kiegészítve kell támogatnia a tagállamokat. A mechanizmusnak az igényekre reagálva biztosítania kell, hogy Unió-szerte és

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

harmadik országokban speciális eszközök álljanak rendelkezésre, amelyek támogatják a kiberbiztonsági eseményekre való felkészültséget és reagálást.

(26) Ez az eszköz nem érinti a válságelhárítás uniós szintű összehangolására szolgáló eljárásokat és kereteket, így különösen az uniós polgári védelmi mechanizmust[15], az uniós politikai szintű integrált válságelhárítási mechanizmust[16], sem az (EU) 2022/2555 irányelvet. Hozzájárulhat ugyanakkor az EUSZ 42. cikkének (7) bekezdésével összefüggésben vagy az EUMSZ 222. cikkében meghatározott helyzetekben végrehajtott intézkedésekhez, illetve kiegészítheti azokat. Ezen eszköz használatát adott esetben össze kell hangolni a kiberdiplomáciai eszköztár intézkedéseinek végrehajtásával is.

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

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

(29) A következetes megközelítés előmozdítása, valamint az Unió és belső piaca biztonságának megerősítése érdekében a felkészültségi intézkedések részeként támogatást kell nyújtani az (EU) 2022/2555 irányelv alapján azonosított, kiemelten kritikus ágazatokban működő szervezetek kiberbiztonságának összehangolt teszteléséhez és értékeléséhez. E célból a Bizottságnak az ENISA támogatásával és az (EU) 2022/2555 irányelvvel létrehozott Kiberbiztonsági Együttműködési Csoporttal együttműködésben rendszeresen azonosítania kell azokat az érintett ágazatokat vagy

---

15 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.).

16 Uniós politikai szintű integrált válságelhárítási mechanizmus (IPCR-mechanizmus) és a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló, 2017. szeptember 13-i (EU) 2017/1584 bizottsági ajánlással összhangban.

alágazatokat, amelyeket az uniós szinten összehangolt tesztelés összefüggésében pénzügyi támogatásra jogosultnak kell minősíteni. Az ágazatokat vagy alágazatokat az (EU) 2022/2555 irányelv I. mellékletéből („A kiemelten kritikus ágazatok”) kell kiválasztani. Az összehangolt tesztelésnek közös kockázati forgatókönyveken és módszereken kell alapulnia. Az ágazatok kiválasztása és a kockázati forgatókönyvek kidolgozása során figyelembe kell venni a vonatkozó uniós szintű kockázatértékeléseket és kockázati forgatókönyveket, többek között a párhuzamosságok elkerülése végett, például az Európai Unió kiberbiztonsági helyzetének javításáról szóló tanácsi következtetésekben a Bizottsághoz, a főképviselőhöz és a Kiberbiztonsági Együttműködési Csoporthoz intézett felkérés szerinti, az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – többek között az EU-CyCLONe-nal – koordinációban elvégzendő kockázatértékeléssel és kidolgozandó kiberbiztonsági szempontú kockázati forgatókönyvvel, vagy a távközlési hálózatokra és infrastruktúrákra vonatkozóan a nevers-i közös miniszteri felhívás nyomán a Kiberbiztonsági Együttműködési Csoport által, a Bizottság és az ENISA támogatásával, az Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben elvégzendő kockázatértékeléssel, vagy az (EU) 2022/2555 irányelv 22. cikke alapján elvégzendő összehangolt kockázatértékelésekkel, illetve az (EU) 2022/2554 európai parlamenti és tanácsi rendeletben[17] előírt digitális működési reziliencia tesztelésével. Az ágazatok kiválasztásakor figyelembe kell venni a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlást is.

(30) Emellett a kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell nyújtania más felkészültségi intézkedésekhez, és támogatnia kell a felkészültséget más olyan ágazatokban, amelyekre nem terjed ki a kiemelten kritikus ágazatokban működő szervezetek összehangolt tesztelése. A szóban forgó intézkedések különböző típusú nemzeti szintű felkészültségi tevékenységeket foglalhatnak magukban.

(31) A kiberbiztonsági vészhelyzeti mechanizmusnak emellett támogatást kell nyújtania a jelentős és nagyszabású kiberbiztonsági események hatásának enyhítését, az azonnali helyreállítás 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.

(32) A kiberbiztonsági vészhelyzeti mechanizmusnak támogatást kell biztosítania azokban az esetekben, amikor a tagállamok segítséget nyújtanak egy jelentős vagy nagyszabású kiberbiztonsági esemény által érintett tagállamnak, többek között az (EU) 2022/2555 irányelv 15. cikkében meghatározott CSIRT-ek hálózata révén. A segítséget nyújtó tagállamok számára lehetővé kell tenni, hogy kérelmeket nyújtsanak be a szakértői csoportok kölcsönös segítségnyújtás keretében történő kiküldésével kapcsolatos költségek fedezésére. Az elszámolható költségek közé tartozhatnak a kiberbiztonsági szakértők utazási, szállás- és napidíjköltségei.

[17] 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.

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

(34) Az uniós kiberbiztonsági tartalék keretében szolgáltatásokat nyújtó magánszolgáltatók kiválasztása céljából meg kell határozni az e szolgáltatók kiválasztására irányuló ajánlati felhívásban szereplő minimumkritériumokat, biztosítva, hogy a tagállami hatóságok és a kritikus vagy kiemelten kritikus ágazatokban működő szervezetek igényei teljesüljenek.

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

(36) E rendelet azon célkitűzéseinek támogatása érdekében, amelyek a közös helyzetismeret előmozdítására, az Unió rezilienciájának fokozására és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálás lehetővé tételére irányulnak, lehetővé kell tenni, hogy egy adott jelentős vagy nagyszabású kiberbiztonsági esemény kapcsán az EU-CyCLONe, a CSIRT-ek hálózata vagy a Bizottság felkérje az ENISA-t, hogy vizsgálja felül és értékelje a fenyegetéseket, a sebezhetőségeket és a mérséklési intézkedéseket. Az esemény felülvizsgálatának és értékelésének befejeztével az ENISA-nak az érintett érdekelt felekkel, többek között a magánszektor, a tagállamok, a Bizottság és más érintett uniós intézmények, szervek és ügynökségek képviselőivel együttműködésben eseményértékelési jelentést kell készítenie. Ami a magánszektort illeti, az ENISA a szakosodott szolgáltatókkal – többek között az irányított biztonsági megoldások szolgáltatóival és értékesítőivel – folytatott információcserét szolgáló csatornákat fejleszt ki annak érdekében, hogy hozzájáruljon az ENISA azon küldetéséhez, hogy Unió-szerte egységesen magas szintű kiberbiztonságot érjen el. Az érdekelt felekkel – többek között a magánszektorral – folytatott együttműködésre építve a konkrét kiberbiztonsági eseményekkel kapcsolatos eseményértékelési jelentésnek arra kell irányulnia, hogy bekövetkezte után értékelje az esemény okait, hatásait és az azzal kapcsolatos mérséklési intézkedéseket. Különös figyelmet kell fordítani az e rendeletben előírt legmagasabb szintű szakmai feddhetetlenség, pártatlanság és szükséges technikai szakértelem feltételeinek megfelelő irányított biztonsági szolgáltatók által megosztott információkra és tapasztalatokra. A jelentést az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak kell benyújtani, amelyeknek azt munkájuk során figyelembe kell venniük. Ha az esemény harmadik országgal kapcsolatos, a Bizottságnak meg kell osztania a jelentést a főképviselővel.

(37) Figyelembe véve a kiberbiztonsági támadások kiszámíthatatlan jellegét és azt, hogy azok gyakran nem korlátozódnak egy adott földrajzi területre, és így a tovagyűrűzés magas kockázatát hordozzák magukban, a szomszédos országok rezilienciájának és a jelentős és nagyszabású kiberbiztonsági eseményekre való hatékony reagálási képességüknek a megerősítése hozzájárul az Unió egészének védelméhez. Ezért a Digitális Európa programhoz társult harmadik országok is részesülhetnek az uniós kiberbiztonsági tartalékból nyújtott támogatásban, amennyiben erről a Digitális Európa programban való részvételükről kötött társulási megállapodás rendelkezik. A társult harmadik országok a vonatkozó partnerségek és finanszírozási eszközök keretében részesülnek az Unió nyújtotta finanszírozásból. A támogatásnak ki kell terjednie a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálás és az eseményt követő azonnali helyreállítás területén nyújtott szolgáltatásokra. Az e rendeletben az uniós kiberbiztonsági tartalékra és a megbízható szolgáltatókra vonatkozóan meghatározott feltételeket alkalmazni kell a Digitális Európa programhoz társult harmadik országoknak nyújtott támogatásokra.

(38) Ezen rendelet végrehajtása egységes feltételeinek biztosítása érdekében a Bizottságra végrehajtási hatásköröket kell ruházni a következők tekintetében: a határokon átnyúló biztonsági műveleti központok közötti interoperabilitás feltételeinek meghatározása; a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos információknak a határokon átnyúló biztonsági műveleti központok és az uniós szervezetek közötti megosztására vonatkozó eljárási szabályok meghatározása; az Európai Kiberpajzs biztonságát garantáló technikai követelmények meghatározása; az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusainak és számának meghatározása; valamint az uniós kiberbiztonsági tartalék támogatási szolgáltatásainak allokációjára vonatkozó részletes szabályok pontosítása. Ezeket a végrehajtási hatásköröket a 182/2011/EU európai parlamenti és tanácsi rendeletnek megfelelően kell gyakorolni.

(39) E rendelet célkitűzése jobban megvalósítható uniós szinten, mint tagállami szinten. Az Unió ezért intézkedéseket fogadhat el az Európai Unióról szóló szerződés 5. cikkében foglalt szubszidiaritási és arányossági elvnek megfelelően. Ez a rendelet nem lépi túl az e cél eléréséhez szükséges mértéket,

ELFOGADTA EZT A RENDELETET:

I. fejezet

ÁLTALÁNOS CÉLKITŰZÉSEK, TÁRGY ÉS FOGALOMMEGHATÁROZÁSOK

1. cikk

A rendelet tárgya és céljai

(1) Ez a rendelet intézkedéseket állapít meg a kiberbiztonsági fenyegetések és események észlelésére, valamint az azokra való felkészülésre és reagálásra irányuló uniós képességek megerősítésére, különösen a következő intézkedések révén:

a) a biztonsági műveleti központok páneurópai infrastruktúrájának kiépítése (Európai Kiberpajzs) a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében;

b) kiberbiztonsági vészhelyzeti mechanizmus létrehozása, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az eseményt követő azonnali helyreállításban;

c) a kiberbiztonsági események európai felülvizsgálati mechanizmusának létrehozása konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából.

(2) E rendelet célja az uniós szintű szolidaritás megerősítése a következő egyedi célkitűzések révén:

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

b) a kritikus és a kiemelten kritikus ágazatokban működő szervezetek felkészültségének megerősítése Unió-szerte, valamint a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, többek között a Digitális Európa programhoz társult harmadik országok számára kiberbiztonsági eseményekre való reagáláshoz nyújtott uniós támogatással;

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

(3) E rendelet nem érinti a tagállamoknak a nemzetbiztonsággal, a közbiztonsággal, valamint a bűncselekmények megelőzésével, kivizsgálásával, felderítésével és büntetőeljárás alá vonásával kapcsolatos elsődleges felelősségét.

2. cikk

Fogalommeghatározások

E rendelet alkalmazásában:

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

2. „**közjogi szerv**”: a 2014/24/EU európai parlamenti és tanácsi irányelv[18] 2. cikke (1) bekezdésének 4. pontjában meghatározott közjogi intézmény;

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

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

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

6. „**kiberfenyegetés/kiberbiztonsági fenyegetés**”: az (EU) 2019/881 rendelet 2. cikkének 8. pontjában meghatározott kiberfenyegetés;

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

8. „**nagyszabású kiberbiztonsági esemény**”: az (EU) 2022/2555 irányelv 6. cikkének 7. pontjában meghatározott esemény;

9. „**felkészültség**”: egy jelentős vagy nagyszabású kiberbiztonsági eseményre való hatékony és gyors reagálást biztosító, előre meghozott kockázatértékelési és nyomonkövetési intézkedések eredményeként kialakult készenlét és képesség;

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

11. „**megbízható szolgáltatók**”: az (EU) 2022/2555 irányelv 6. cikkének 40. pontjában meghatározott, e rendelet 16. cikkével összhangban kiválasztott irányított biztonsági szolgáltatók.

II. fejezet

EURÓPAI KIBERPAJZS

3. cikk

Az Európai Kiberpajzs létrehozása

(1) Létre kell hozni a biztonsági műveleti központok egymással összekapcsolt páneurópai infrastruktúráját (a továbbiakban: Európai Kiberpajzs) annak érdekében, hogy az Unió fejlett képességeket alakítson ki az Unión belüli kiberbiztonsági fenyegetések és események észlelése, elemzése és a vonatkozó adatok feldolgozása érdekében. A pajzsot az összes

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

nemzeti biztonsági műveleti központ (a továbbiakban: nemzeti SOC) és határokon átnyúló biztonsági műveleti központ (a továbbiakban: határokon átnyúló SOC) alkotja.

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

(2) Az Európai Kiberpajzs:

a) a határokon átnyúló biztonsági műveleti központok révén összegyűjti és megosztja a különböző forrásokból származó, kiberbiztonsági fenyegetésekre és eseményekre vonatkozó adatokat;

b) a legkorszerűbb eszközök, nevezetesen a mesterséges intelligencia és az adatelemzési technológiák alkalmazásával magas színvonalú, hasznosítható információkat és kiberfenyegetettségi információkat állít elő;

c) hozzájárul a fokozott védelemhez és a kiberfenyegetésekre való hatékonyabb reagáláshoz;

d) Unió-szerte hozzájárul a kiberfenyegetések gyorsabb észleléséhez és a helyzetismerethez;

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

A pajzsot az (EU) 2021/1173 rendelet alapján létrehozott páneurópai nagy teljesítményű számítástechnikai infrastruktúrával együttműködésben kell kialakítani.

4. cikk

Nemzeti biztonsági műveleti központok

(1) Az Európai Kiberpajzsban való részvétel érdekében minden tagállamnak ki kell jelölnie legalább egy nemzeti biztonsági műveleti központot. A nemzeti biztonsági műveleti központ közjogi szerv.

Képesnek kell lennie arra, hogy nemzeti szintű referenciapontként és átjáróként szolgáljon más állami és magánszervezetek számára a kiberbiztonsági fenyegetésekre és eseményekre vonatkozó információk gyűjtése és elemzése, valamint a valamely határokon átnyúló biztonsági műveleti központhoz való hozzájárulás tekintetében. Fel kell szerelni a kiberbiztonsági fenyegetések és események észlelésére, valamint a kapcsolódó adatok összesítésére és elemzésére alkalmas legkorszerűbb technológiákkal.

(2) Az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (a továbbiakban: ECCC) részvételi szándék kifejezésére való felhívás nyomán választja ki azokat a nemzeti biztonsági műveleti központokat, amelyek részt vesznek az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda a kiválasztott nemzeti biztonsági műveleti központoknak az említett eszközök és infrastruktúrák működtetésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 50 %-át és a működési költségek

legfeljebb 50 %-át fedezi, a fennmaradó költségek pedig a tagállamra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és a nemzeti biztonsági műveleti központ az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

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

5. cikk

Határokon átnyúló biztonsági műveleti központok

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

(2) Az ECCC részvételi szándék kifejezésére való felhívás nyomán választja ki azt az üzemeltetési konzorciumot, amely részt vesz az ECCC-vel közösen bonyolított eszköz- és infrastruktúra-beszerzésben. Az ECCC támogatást ítélhet oda az üzemeltetési konzorciumnak az említett eszközök és infrastruktúrák működtetésének finanszírozására. Az uniós pénzügyi hozzájárulás az eszközök és infrastruktúrák beszerzési költségeinek legfeljebb 75 %-át és a működési költségek legfeljebb 50 %-át fedezi, a fennmaradó költségek pedig az üzemeltetési konzorciumra hárulnak. Az eszközök és infrastruktúrák beszerzésére irányuló eljárás megindítása előtt az ECCC és az üzemeltetési konzorcium az eszközök és infrastruktúrák használatát szabályozó üzemeltetési és használati megállapodást köt.

(3) Az üzemeltetési konzorcium tagjai írásos konzorciumi megállapodást kötnek, amely meghatározza az üzemeltetési és használati megállapodás végrehajtásának belső szabályait.

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

6. cikk

Együttműködés és információmegosztás a határokon átnyúló biztonsági műveleti központokon belül és azok között

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

a) célja, hogy megelőzze, észlelje az eseményeket, reagáljon azokra vagy az eseményeket követően helyreállítsa a működést, illetve mérsékelje az események hatását;

b) növeli a kiberbiztonság szintjét, különösen 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 vagy 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 határozni a következőket:

a) az (1) bekezdésben említett jelentős mennyiségű adat megosztására vonatkozó kötelezettségvállalás, valamint a szóban forgó információcsere feltételei;

b) irányítási keret, amely minden résztvevőt az információk megosztására ösztönöz;

c) célértékek a fejlett mesterséges intelligenciát és adatelemzést szolgáló eszközök fejlesztéséhez való hozzájárulás tekintetében.

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

(4) A határokon átnyúló biztonsági műveleti központok együttműködési megállapodásokat kötnek egymással, amelyben meghatározzák a határokon átnyúló platformok közötti információmegosztás elveit.

7. cikk

Együttműködés és információmegosztás az uniós szervezetekkel

(1) Ha a határokon átnyúló biztonsági műveleti központok információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a releváns információkat az (EU) 2022/2555 irányelv szerinti válságkezelési szerepük figyelembevételével indokolatlan késedelem nélkül eljuttatják az EU-CyCLONe-nak, a CSIRT-ek hálózatának és a Bizottságnak.

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

8. cikk

Biztonság

(1) Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak az Európai Kiberpajzs infrastruktúrájának magas szintű adatbiztonságáról és fizikai biztonságáról, biztosítják, hogy az infrastruktúrát megfelelő irányítás és ellenőrzés révén megvédjék a fenyegetésektől, továbbá biztosítják az infrastruktúra és a rendszerek – többek között az infrastruktúrán keresztül kicserélt adatok – biztonságát is.

(2) Az Európai Kiberpajzsban részt vevő tagállamok gondoskodnak arról, hogy az Európai Kiberpajzs keretében nem tagállami közjogi szerveknek minősülő szervezetekkel folytatott információmegosztás ne érintse hátrányosan az Unió biztonsági érdekeit.

(3) A Bizottság végrehajtási jogi aktusokat fogadhat el, amelyekben technikai követelményeket állapít meg a tagállamok számára az (1) és (2) bekezdés szerinti kötelezettségeik teljesítéséhez. Ezeket a végrehajtási jogi aktusokat az e rendelet 21. cikkének (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni. Ennek során a katonai szereplőkkel való együttműködés megkönnyítése érdekében a Bizottság – a főképviselő támogatásával – figyelembe veszi a vonatkozó védelmi szintű biztonsági előírásokat.

III. fejezet

KIBERBIZTONSÁGI VÉSZHELYZETI MECHANIZMUS

9. cikk

A kiberbiztonsági vészhelyzeti mechanizmus létrehozása

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

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

10. cikk

Intézkedéstípusok

(1) A mechanizmus a következő intézkedéstípusokat támogatja:

a) felkészültségi intézkedések, amelyek magukban foglalják a kiemelten kritikus ágazatokban működő szervezetek Unió-szerte összehangolt felkészültségi tesztelését;

b) a jelentős és nagyszabású kiberbiztonsági eseményekre való reagálást és az eseményt követő azonnali helyreállítást támogató reagálási intézkedések, amelyeket a 12. cikk alapján létrehozott uniós kiberbiztonsági tartalékban részt vevő megbízható szolgáltatók biztosítanak;

c) kölcsönös segítségnyújtási intézkedések, amelyek magukban foglalják az egyik tagállam nemzeti hatóságai által egy másik tagállamnak nyújtott segítséget, különösen az (EU) 2022/2555 irányelv 11. cikke (3) bekezdésének f) pontjában előírtak szerint.

11. cikk

A szervezetek összehangolt felkészültségi tesztelése

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

(2) A Kiberbiztonsági Együttműködési Csoport a Bizottsággal, az ENISA-val és a főképviselővel együttműködve közös kockázati forgatókönyveket és módszereket dolgoz ki az összehangolt teszteléshez.

12. cikk

Az uniós kiberbiztonsági tartalék létrehozása

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

(2) Az uniós kiberbiztonsági tartalék a 16. cikkben meghatározott kritériumoknak megfelelően kiválasztott megbízható szolgáltatók eseményreagálási szolgáltatásaiból áll össze. A tartalék előzetes kötelezettségvállalás keretében rendelkezésre bocsátott szolgáltatásokat tartalmaz. A szolgáltatások valamennyi tagállamban igénybe vehetők.

(3) Az uniós kiberbiztonsági tartalék szolgáltatásainak felhasználói közé a következők tartoznak:

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

b) az uniós intézmények, szervek és ügynökségek.

(4) A (3) bekezdés a) pontjában említett felhasználóknak az uniós kiberbiztonsági tartalék szolgáltatásait kell igénybe venniük a kritikus vagy kiemelten kritikus ágazatokban működő szervezeteket érintő jelentős vagy nagyszabású biztonsági eseményekre való reagáláshoz vagy a reagálás támogatásához, valamint az ilyen eseményeket követő azonnali helyreállításhoz.

(5) A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság a (3) bekezdésben említett felhasználók igényeivel összhangban határozza meg az uniós kiberbiztonsági tartalék prioritásait és alakulását, továbbá felügyeli annak végrehajtását, és biztosítja az e rendelet szerinti egyéb támogatási intézkedésekkel, valamint az egyéb uniós intézkedésekkel és programokkal való kiegészítő jelleget, következetességet, szinergiákat és kapcsolatokat.

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

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

(8) A Bizottság végrehajtási jogi aktusok útján meghatározhatja az uniós kiberbiztonsági tartalékhoz szükséges reagálási szolgáltatások típusait és számát. E végrehajtási jogi aktusokat a 21. cikk (2) bekezdésében említett vizsgálóbizottsági eljárás keretében kell elfogadni.

13. cikk

Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmek

(1) A 12. cikk (3) bekezdésében említett felhasználók szolgáltatásokat kérhetnek az uniós kiberbiztonsági tartalékból a jelentős vagy nagyszabású kiberbiztonsági eseményekre való reagálás és az eseményt követő azonnali helyreállítás támogatása érdekében.

(2) Ahhoz, hogy a 12. cikk (3) bekezdésében említett felhasználók támogatást – beleértve a közvetlen technikai segítségnyújtást és az eseményre való reagálást, valamint az eseményt követő azonnali helyreállítási erőfeszítéseket segítő egyéb erőforrásokat – kapjanak az uniós kiberbiztonsági tartalékból, intézkedéseket kell hozniuk annak érdekében, hogy enyhítsék a támogatás iránti kérelem tárgyát képező esemény hatásait.

(3) Az e rendelet 12. cikke (3) bekezdésének a) pontjában említett felhasználók támogatás iránti kérelmeit a tagállam által az (EU) 2022/2555 irányelv 8. cikkének (3) bekezdésével összhangban kijelölt vagy létrehozott egyedüli kapcsolattartó ponton keresztül kell továbbítani a Bizottságnak és az ENISA-nak.

(4) A tagállamok tájékoztatják a CSIRT-ek hálózatát és adott esetben az EU-CyCLONe-t az e cikk szerinti, kiberbiztonsági eseményekre való reagáláshoz és azonnali helyreállításhoz támogatást igénylő kérelmeikről.

(5) A kiberbiztonsági eseményekre való reagáláshoz és azonnali helyreállításhoz támogatást igénylő kérelmek a következőket tartalmazzák:

a) megfelelő információk az érintett szervezetről és a kiberbiztonsági esemény lehetséges hatásairól, valamint a kért támogatás tervezett felhasználásáról, beleértve a becsült szükségletek megjelölését is;

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

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

(6) Az ENISA a Bizottsággal és a Kiberbiztonsági Együttműködési Csoporttal együttműködve sablont dolgoz ki az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmek benyújtásának megkönnyítésére.

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

14. cikk

Az uniós kiberbiztonsági tartalékból nyújtott támogatás végrehajtása

(1) Az uniós kiberbiztonsági tartalékból nyújtott támogatás iránti kérelmeket a Bizottság az ENISA közreműködésével vagy a 12. cikk (6) bekezdése szerinti hozzájárulási megállapodásokban meghatározottak szerint értékeli, és a választ haladéktalanul továbbítja a 12. cikk (3) bekezdésében említett felhasználóknak.

(2) Több párhuzamos megkeresés esetén a kérelmek rangsorolásához adott esetben a következő kritériumokat kell figyelembe venni:

a) a kiberbiztonsági esemény súlyossága;

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

c) az érintett tagállam(ok)ra vagy felhasználókra gyakorolt lehetséges hatás;

d) a kiberbiztonsági esemény lehetséges határokon átnyúló jellege és annak kockázata, hogy tovagyűrűzhet más tagállamokra vagy felhasználókra;

e) a felhasználó által a reagálás elősegítése érdekében hozott intézkedések és az azonnali helyreállítási erőfeszítések a 13. cikk (2) bekezdésében és a 13. cikk (5) bekezdésének b) pontjában említettek szerint.

(3) Az uniós kiberbiztonsági tartalék szolgáltatásait a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi megállapodásokkal összhangban kell nyújtani. E megállapodásoknak tartalmazniuk kell felelősségre vonatkozó feltételeket is.

(4) A (3) bekezdésben említett megállapodások alapulhatnak az ENISA által a tagállamokkal folytatott konzultációt követően készített sablonokon.

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

(6) A támogatási intézkedés befejezését követő egy hónapon belül a felhasználók összefoglaló jelentést nyújtanak be a Bizottságnak és az ENISA-nak a nyújtott szolgáltatásról, az elért eredményekről és a levont tanulságokról. Amennyiben a felhasználó a 17. cikkben meghatározott harmadik országból származik, a szóban forgó jelentést meg kell osztani a főképviselővel.

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

15. cikk

Koordináció a válságkezelési mechanizmusokkal

(1) Azokban az esetekben, amikor a jelentős vagy nagyszabású kiberbiztonsági események az 1313/2013/EU határozatban[19] meghatározott katasztrófák nyomán alakulnak ki, vagy ilyen katasztrófát okoznak, az ilyen eseményekre való reagáláshoz az e rendelet alapján nyújtott támogatásnak azok sérelme nélkül ki kell egészítenie az 1313/2013/EU határozat szerinti intézkedéseket.

(2) Ha olyan nagyszabású, határokon átnyúló kiberbiztonsági esemény következik be, amely kiváltja az uniós politikai szintű integrált válságelhárítási mechanizmus (a továbbiakban: IPCR-mechanizmus) alkalmazását, a kiberbiztonsági eseményhez való reagáláshoz az e rendelet szerint nyújtott támogatást az IPCR-mechanizmus szerinti vonatkozó protokollokkal és eljárásokkal összhangban kell kezelni.

(3) A főképviselővel folytatott konzultáció alapján a kiberbiztonsági vészhelyzeti mechanizmus keretében nyújtott támogatás kiegészítheti a közös kül- és biztonságpolitika, valamint a közös biztonság- és védelempolitika keretében – többek között a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok révén – nyújtott segítséget. Kiegészítheti továbbá az egyik tagállam által egy másik tagállamnak az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésével összefüggésben nyújtott segítséget, vagy hozzájárulhat ahhoz.

(4) A kiberbiztonsági vészhelyzeti mechanizmus keretében nyújtott támogatás az Európai Unió működéséről szóló szerződés 222. cikkében említett helyzetekben az Unió és a tagállamok közötti közös reagálás részét képezheti.

[19] 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.).

16. cikk

Megbízható szolgáltatók

(1) Az uniós kiberbiztonsági tartalék létrehozását célzó közbeszerzési eljárások során az ajánlatkérő szerv az (EU, Euratom) 2018/1046 rendeletben meghatározott elvekkel és a következő elvekkel összhangban jár el:

a) biztosítja, hogy az uniós kiberbiztonsági tartalék olyan szolgáltatásokat foglaljon magában, amelyek valamennyi tagállamban igénybe vehetők, figyelembe véve különösen az ilyen szolgáltatások nyújtására vonatkozó nemzeti követelményeket, beleértve a tanúsítást, illetve az akkreditációt is;

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 EU-ban.

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

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

b) a szolgáltatónak, leányvállalatainak és alvállalkozóinak olyan kerettel kell rendelkezniük, amely védi a szolgáltatással kapcsolatos érzékeny információkat, különösen a bizonyítékokat, a megállapításokat és a jelentéseket, és megfelel az EU-minősített adatok védelmére vonatkozó uniós biztonsági szabályoknak;

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

d) a szolgáltatónak megfelelő biztonsági tanúsítvánnyal kell rendelkeznie, legalább azon személyek tekintetében, akiket a szolgáltatásnyújtásban alkalmazni kíván;

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

f) a szolgáltatónak rendelkeznie kell a kért szolgáltatáshoz szükséges műszaki berendezésekkel, beleértve a hardvereket és szoftvereket is;

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

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

i) a szolgáltatónak képesnek kell lennie arra, hogy a szolgáltatást azon tagállam(ok) helyi nyelvén nyújtsa, ahol a szolgáltatást nyújtani tudja;

j) amint életbe lép az (EU) 2019/881 rendelet szerinti, irányított biztonsági szolgáltatásokra vonatkozó uniós tanúsítási rendszer, a szolgáltatónak az említett rendszerrel összhangban kell tanúsítást szereznie.

17. cikk

Harmadik országoknak nyújtott támogatás

(1) Az uniós kiberbiztonsági tartalék nyújtotta támogatást harmadik országok is kérelmezhetik, ha a velük kötött társulási megállapodás a Digitális Európa programban való részvételükről ekképpen rendelkezik.

(2) Az uniós kiberbiztonsági tartalékból nyújtott támogatásnak összhangban kell lennie e rendelettel, és meg kell felelnie az (1) bekezdésben említett társulási megállapodásokban meghatározott bármely egyedi feltételnek.

(3) Az uniós kiberbiztonsági tartalék szolgáltatásainak igénybevételére jogosult társult harmadik országbeli felhasználók közé tartoznak az illetékes hatóságok, így például a CSIRT-ek és a kiberválságok kezelésével foglalkozó hatóságok.

(4) Az uniós kiberbiztonsági tartalékból támogatásra jogosult minden egyes harmadik ország kijelöl egy hatóságot, amely e rendelet alkalmazásában egyedüli kapcsolattartó pontként jár el.

(5) Mielőtt a harmadik országok bármilyen támogatást kapnának az uniós kiberbiztonsági tartalékból, tájékoztatják a Bizottságot és a főképviselőt kiberreziliencia- és kockázatkezelési képességeikről, beleértve legalább a jelentős vagy nagyszabású kiberbiztonsági eseményekre való felkészülés érdekében hozott nemzeti intézkedésekre vonatkozó információkat, valamint a felelős nemzeti szervezetekre – köztük a CSIRT-ekre vagy azokkal egyenértékű szervezetekre –, azok képességeire és a hozzájuk rendelt erőforrásokra vonatkozó információkat. Amennyiben e rendelet 13. és 14. cikkének rendelkezései a tagállamokra hivatkoznak, azok az (1) bekezdésben meghatározott harmadik országokra is alkalmazandók.

(6) A Bizottság egyeztet a főképviselővel a beérkezett kérelmekről és az uniós kiberbiztonsági tartalékból harmadik országoknak nyújtott támogatás végrehajtásáról.

IV. fejezet

A KIBERBIZTONSÁGI ESEMÉNYEK FELÜLVIZSGÁLATI MECHANIZMUSA

18. cikk

A kiberbiztonsági események felülvizsgálati mechanizmusa

(1) A Bizottság, az EU-CyCLONe vagy a CSIRT-ek hálózatának kérésére az ENISA felülvizsgálja és értékeli az egy adott jelentős vagy nagyszabású kiberbiztonsági eseményhez kapcsolódó fenyegetéseket, sebezhetőségeket és mérséklési intézkedéseket. Egy adott kiberbiztonsági esemény felülvizsgálatának és értékelésének lezárultával az ENISA eseményértékelési jelentést nyújt be a CSIRT-ek hálózatának, az EU-CyCLONe-nak és a Bizottságnak, hogy támogassa őket – különösen az (EU) 2022/2555 irányelv 15. és 16.

cikkében foglalt – feladataik ellátásában. A Bizottság adott esetben megosztja a jelentést a főképviselővel.

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

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

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

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

V. fejezet

ZÁRÓ RENDELKEZESEK

19. 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:

1. a szöveg a következő aa) ponttal egészül ki:

„aa) az Európai Kiberpajzs kialakításának támogatása, beleértve a nemzeti és a határokon átnyúló biztonsági műveleti központok platformjainak fejlesztését, telepítését és működtetését, amelyek hozzájárulnak az Unión belüli helyzetismerethez és az Unió kiberfenyegetettségi információszerző képességeinek megerősítéséhez;”.

2. A szöveg a következő g) ponttal egészül ki:

„g) a nemzeti erőforrásokat és képességeket, valamint az uniós szinten rendelkezésre álló egyéb támogatási formákat kiegészítő kiberbiztonsági vészhelyzeti mechanizmus

létrehozása és működtetése annak érdekében, hogy támogassa a tagállamokat a jelentős kiberbiztonsági eseményekre való felkészülésben és reagálásban, ideértve az uniós kiberbiztonsági tartalék létrehozását is.”

a) 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[20] összhangban, kivéve az uniós kiberbiztonsági tartalékot végrehajtó fellépéseket, amelyeket a Bizottság és az ENISA hajt végre.”

2. A 9. cikk a következőképpen módosul:

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

„b) 1 776 956 000 EUR a 2. sz. Mesterséges intelligencia egyedi célkitűzésre;

c) 1 629 566 000 EUR a 3. sz. Kiberbiztonság és bizalom egyedi célkitűzésre;

d) 482 347 000 EUR a 4. sz. Fejlett digitális készségek egyedi célkitűzésre;”

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

„(8) Az (EU, Euratom) 2018/1046 rendelet 12. cikkének (4) bekezdésétől eltérve az e rendelet 6. cikke (1) bekezdésének g) pontjában meghatározott célkitűzések megvalósítására irányuló fellépésekre elkülönített, fel nem használt kötelezettségvállalási és kifizetési előirányzatok automatikusan átvihetők a következő pénzügyi évre, és terhükre a következő év december 31-éig kötelezettségek vállalhatók és kifizetések teljesíthetők.”

3. 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[27] és a 2014/25/EU[28] európai parlamenti és tanácsi irányelv által meghatározott ajánlatkérő szervek vagy közszolgáltató ajánlatkérők.

[20] 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.).

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 követelheti, hogy a szerződés teljesítésének helye az Unió területén legyen kijelölve.

Az (EU) 2023/XX rendelet 12. cikkével létrehozott uniós kiberbiztonsági tartalékra vonatkozó közbeszerzési eljárások végrehajtáskor a Bizottság és az ENISA központi beszerző szervként járhat el a 10. cikkel összhangban a programhoz társult harmadik országok érdekében 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) XXXX/XXX rendelet [FR-átdolgozott szöveg] 169. cikkének (3) bekezdésétől eltérve egyetlen harmadik ország által benyújtott kérelem elegendő ahhoz, hogy a Bizottság vagy az ENISA megbízást kapjon eljárni.

Az (EU) 2023/XX rendelet 12. cikkével létrehozott uniós kiberbiztonsági tartalékra vonatkozó közbeszerzési eljárások végrehajtásakor a Bizottság és az ENISA központi beszerző szervként járhat el az uniós intézmények, szervek és ügynökségek érdekében vagy nevében történő beszerzések során. A Bizottság és az ENISA nagykereskedőként is eljárhat áruk és szolgáltatások uniós intézményeknek, szerveknek és ügynökségeknek történő vásárlása, készletezése, továbbértékesítése vagy adományozása révén, beleértve a bérbeadást is. Az (EU) XXXX/XXX rendelet [FR-átdolgozott szöveg] 169. cikkének (3) bekezdésétől eltérve egyetlen uniós intézmény, szerv vagy ügynökség által benyújtott kérelem elegendő ahhoz, hogy a Bizottság vagy az ENISA megbízást kapjon eljárni.

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

4. A szöveg a következő 16a. cikkel egészül ki:

„Az (EU) 2023/XX rendelet 3. cikkével létrehozott Európai Kiberpajzsot végrehajtó intézkedések esetében az (EU) 2023/XX rendelet 4. és 5. cikkében meghatározott szabályok alkalmazandók. Az e rendeletben, illetve az (EU) 2023/XX rendelet 4. és 5. cikkében foglalt rendelkezések ütközése esetén az utóbbiak az irányadók és alkalmazandók az említett egyedi intézkedésekre.”

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

„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 támogatásokat az egyes egyedi célkitűzésekre vonatkozóan meghatározottak szerint kell odaítélni és irányítani.

A vissza nem térítendő támogatásként nyújtott támogatást az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont a költségvetési rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti az XXXX rendelet 4. cikkében említett nemzeti biztonsági műveleti központoknak és az XXXX rendelet 5. cikkében említett üzemeltetési konzorciumnak.

Az XXXX rendelet 10. cikkében meghatározott kiberbiztonsági vészhelyzeti mechanizmushoz vissza nem térítendő támogatásként nyújtott támogatást az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont a költségvetési rendelet 195. cikke (1) bekezdésének d) pontjával összhangban közvetlenül, pályázati felhívás nélkül is odaítélheti a tagállamoknak.

A 202X/XXXX rendelet 10. cikke (1) bekezdésének c) pontjában meghatározott intézkedések esetében az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont tájékoztatja a Bizottságot és az ENISA-t a tagállamok pályázati felhívás nélküli közvetlen támogatásra irányuló kérelmeiről.

Az XXXX rendelet 10. cikkének c) pontjában meghatározott jelentős vagy nagyszabású kiberbiztonsági eseményre való reagáláshoz nyújtott kölcsönös segítségnyújtás támogatása céljából 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.”

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

20. cikk

Értékelés

A Bizottság [négy évvel e rendelet alkalmazásának kezdőnapját követően]-ig jelentést nyújt be az Európai Parlamentnek és a Tanácsnak e rendelet értékeléséről és felülvizsgálatáról.

21. cikk

Bizottsági eljárás

(1) A Bizottságot az (EU) 2021/694 rendelettel létrehozott 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.

22. 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 Strasbourgban, -án/-én.

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

PÉNZÜGYI KIMUTATÁS

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

1.2. Az érintett szakpolitikai terület(ek)

1.3. A javaslat/kezdeményezés a következőre irányul:

1.4. Célkitűzés(ek)

1.4.1. Általános célkitűzés(ek)

1.4.2. Konkrét célkitűzés(ek)

1.4.3. Várható eredmény(ek) és hatás(ok)

1.4.4. Teljesítménymutatók

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével

1.5.2. Az Unió részvételéből származó hozzáadott érték (adódhat többek között a koordinációból eredő előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pontban „az Unió részvételéből származó hozzáadott érték" azt az uniós részvételből adódó értéket jelenti, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák

1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

1.7. Tervezett költségvetés-végrehajtási módszer(ek)

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása

2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk

2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke" hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási sora/sorai

3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása

3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összefoglalása

3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összefoglalása

3.2.3.1. Becsült humánerőforrás-szükségletek

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

3.2.5. Harmadik felek részvétele a finanszírozásban

3.3. A bevételre gyakorolt becsült hatás

1. A JAVASLAT/KEZDEMÉNYEZÉS FŐBB ADATAI

1.1. A javaslat/kezdeményezés címe

Az Európai Parlament és a Tanács rendelete a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról

1.2. Az érintett szakpolitikai terület(ek)

A digitális korra felkészült Európa

Európai stratégiai beruházások

Tevékenység: Európa digitális jövőjének megtervezése

1.3. A javaslat/kezdeményezés a következőre irányul:

☒ **új intézkedés**

☐ **kísérleti projektet/előkészítő intézkedést követő új intézkedés**[33]

☐ **jelenlegi intézkedés meghosszabbítása**

☐ **egy vagy több intézkedés összevonása vagy átalakítása egy másik/új intézkedéssé**

1.4. Célkitűzés(ek)

1.4.1. Általános célkitűzés(ek)

A kiberszolidaritásról szóló jogszabály erősíteni fogja az uniós szintű szolidaritást a kiberbiztonsági fenyegetések és események eredményesebb észlelése, és az azokra való hatékonyabb felkészülés és reagálás érdekében. Céljai:

a) a kiberbiztonsági fenyegetések és események közös uniós észlelésének és helyzetismeretének megerősítése;

b) a kritikus szervezetek felkészültségének megerősítése Unió-szerte, valamint a szolidaritás megerősítése a jelentős vagy nagyszabású kiberbiztonsági eseményekre való közös reagálási kapacitások kialakítása révén, többek között a Digitális Európa programhoz társult harmadik országok számára kiberbiztonsági eseményekre való reagáláshoz nyújtott támogatással;

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

1.4.2. Konkrét célkitűzés(ek)

A kiberszolidaritásról szóló jogszabály célkitűzései a következők révén érhetők el:

[33] A költségvetési rendelet 58. cikke (2) bekezdésének a) vagy b) pontja szerint.

a) a biztonsági műveleti központok páneurópai infrastruktúrájának kiépítése (Európai Kiberpajzs) a közös észlelési és helyzetismereti képességek kialakítása és fejlesztése érdekében;

b) kiberbiztonsági vészhelyzeti mechanizmus létrehozása, amely támogatja a tagállamokat a jelentős és nagyszabású kiberbiztonsági eseményekre való felkészülésben, reagálásban és az eseményt követő azonnali helyreállításban. A kiberbiztonsági eseményekre való reagáláshoz nyújtott támogatást elérhetővé kell tenni az uniós intézmények, szervek, hivatalok és ügynökségek számára is.

Ezekhez az intézkedésekhez a Digitális Európa program nyújt finanszírozást, amelyet ez a jogalkotási eszköz módosítani fog annak érdekében, hogy meg lehessen valósítani a fent említett intézkedéseket, pénzügyi támogatás álljon rendelkezésre a szóban forgó fejlesztésekhez, és egyértelmű feltételek mellett lehessen igénybe venni a pénzügyi támogatást;

c) a kiberbiztonsági események európai felülvizsgálati mechanizmusának létrehozása konkrét jelentős vagy nagyszabású kiberbiztonsági események felülvizsgálata és értékelése céljából.

1.4.3. Várható eredmény(ek) és hatás(ok)

Tüntesse fel, milyen hatásokat gyakorolhat a javaslat/kezdeményezés a kedvezményezettekre/célcsoportokra.

A javaslat jelentős előnyökkel járna a különböző érdekelt felek számára. Az Európai Kiberpajzs javítani fogja a tagállamok kiberfenyegetés-észlelési képességeit. A kiberbiztonsági vészhelyzeti mechanizmus kiegészíti a tagállamok intézkedéseit a felkészültséghez, a reagáláshoz, az azonnali helyreállításhoz, valamint az alapvető szolgáltatások működésének helyreállításához nyújtott vészhelyzeti támogatás révén.

Ezek az intézkedések a digitalizált gazdaság egészét tekintve megerősítik az európai ipar és vállalkozások versenyhelyzetét, és a digitális egységes piac kiberbiztonsági szintjének megerősítése révén előmozdítják ezek digitális átalakulását. Céljuk különösen a kritikus vagy a kiemelten kritikus ágazatokban érintett polgárok, vállalkozások és szervezetek növekvő, adott esetben pusztító társadalmi és gazdasági hatásokkal járó kiberbiztonsági fenyegetésekkel szembeni rezilienciájának növelése. Ehhez olyan eszközökbe ruház be, amelyek támogatják a kiberbiztonsági fenyegetések és események gyorsabb észlelését és az azokra való gyorsabb reagálást, továbbá segítséget nyújt a tagállamoknak ahhoz, hogy jobban felkészüljenek és hatékonyabban reagáljanak a jelentős és nagyszabású kiberbiztonsági eseményekre. Ez várhatóan megerősíti Európa képességeit e területen, különösen a kiberbiztonsági fenyegetésekkel és eseményekkel kapcsolatos adatok gyűjtése és elemzése tekintetében.

1.4.4. Teljesítménymutatók

Határozza meg az előrehaladás és az eredmények nyomon követésére szolgáló mutatókat.

Az uniós szintű szolidaritás előmozdítása érdekében több mutatót is figyelembe lehetne venni:

(1) A közös beszerzésű kiberbiztonsági infrastruktúrák és/vagy eszközök száma

(2) A kiberbiztonsági eseményekre való felkészültséget és reagálást támogató intézkedések száma a kiberbiztonsági vészhelyzeti mechanizmus keretében.

1.5. A javaslat/kezdeményezés indoklása

1.5.1. Rövid vagy hosszú távon kielégítendő szükséglet(ek) a kezdeményezés végrehajtásának részletes ütemtervével

A rendeletet röviddel elfogadását követően, azaz az Európai Unió Hivatalos Lapjában való kihirdetését követő huszadik napon teljes körűen alkalmazni kell.

1.5.2. Az Unió részvételéből származó hozzáadott érték (adódhat többek között a koordinációból eredő előnyökből, a jogbiztonságból, a fokozott hatékonyságból vagy a kiegészítő jellegből). E pontban „az Unió részvételéből származó hozzáadott érték” azt az uniós részvételből adódó értéket jelenti, amely többletként jelentkezik ahhoz az értékhez képest, amely a tagállamok egyedüli fellépése esetén jött volna létre.

A kiberbiztonsági fenyegetések összességében erőteljes, határokon átnyúló jellege, valamint a határokon, ágazatokon és termékeken tovagyűrűző hatásokkal járó, egyre gyakoribb kockázatok és kiberbiztonsági események miatt a szóban forgó beavatkozás célkitűzéseit a tagállamok önállóan nem tudják hatékonyan megvalósítani, ezért uniós szintű közös fellépésre és szolidaritásra van szükség. Az Ukrajna elleni háborúnak tulajdonítható kiberfenyegetések elhárítása során szerzett tapasztalatok, valamint a francia elnökség alatt folytatott kiberbiztonsági gyakorlat (EU CyCLES) tanulságai azt mutatják, hogy az uniós szintű szolidaritás megteremtése érdekében konkrét kölcsönös támogatási mechanizmusokat kell kidolgozni, ideértve különösen a magánszektorral való együttműködést. Ennek fényében az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetések felkérik a Bizottságot, hogy nyújtson be javaslatot egy új Kiberbiztonsági Vészhelyzeti Alapra vonatkozóan. A kiberbiztonsági fenyegetések eredményesebb észlelésére, valamint a felkészültségi és reagálási kapacitások bővítésére irányuló uniós szintű támogatások és intézkedések – a párhuzamos uniós és tagállami erőfeszítések kiküszöbölésével – hozzáadott értéket teremtenek. Ez biztosítaná a meglévő eszközök hatékonyabb kiaknázását, valamint jobb koordinációt és a levont tanulságokkal kapcsolatos információcserét eredményez.

1.5.3. Hasonló korábbi tapasztalatok tanulsága

Az Európai Kiberpajzs égisze alatt végzendő helyzetismereti és észlelési tevékenységeket illetően a Digitális Európa program 2021–2022-es kiberbiztonsági munkaprogramja keretében részvételi szándék kifejezésére való felhívást tettek közzé a határokon átnyúló biztonsági műveleti központok létrehozásához szükséges eszközök és infrastruktúra közös beszerzésére, és ezenfelül az állami és magánszervezeteket kiszolgáló biztonsági műveleti központok kapacitásépítését előmozdító támogatási felhívást is közzétették.

A felkészültség és a kiberbiztonsági eseményekre való reagálás tekintetében az ENISA számára elkülönített további finanszírozás révén a Bizottság a tagállamok támogatása érdekében létrehozta a súlyos kiberbiztonsági eseményekre való felkészültség és reagálási képességek azonnali megerősítését szolgáló rövid távú programot. A program többek között olyan felkészültségi intézkedéseket is magában foglal, mint a kritikus szervezeteknél a sebezhetőségek azonosítása végett végzett behatolási tesztelés. A program emellett szélesebb körű lehetőségeket biztosít a tagállamoknak való segítségnyújtásra a kritikus szervezeteket érintő súlyos kiberbiztonsági események esetén. Az ENISA megkezdte e rövid távú program

végrehajtását, és az ennek eredményeképpen felmerült releváns és értékes meglátásokat figyelembe vették e rendelet előkészítése során.

1.5.4. A többéves pénzügyi kerettel való összeegyeztethetőség és egyéb megfelelő eszközökkel való lehetséges szinergiák

A kiberszolidaritásról szóló jogszabály az Unió és a tagállamok által jelenleg támogatott intézkedésekre fog épülni a helyzetismeret és a kiberfenyegetések észlelésének javítása, valamint a nagyszabású és határokon átnyúló kiberbiztonsági eseményekre való eredményesebb reagálás érdekében. Emellett az eszköz összhangban van más válságkezelési keretekkel, többek között az IPCR-mechanizmussal, a közös biztonság- és védelempolitikával, beleértve a kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportokat, valamint az egyik tagállam által egy másik tagállamnak az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésével összefüggésben nyújtott segítséggel. Az új javaslat célja, hogy kiegészítse és támogassa az egyéb kiberbiztonsági eszközök, például az (EU) 2022/2555 irányelv (NIS 2 irányelv) vagy az (EU) 2019/881 rendelet (kiberbiztonsági jogszabály) alapján kidolgozott struktúrákat is.

1.5.5. A rendelkezésre álló különböző finanszírozási lehetőségek értékelése, ideértve az átcsoportosítási lehetőségeket is

Az ENISA-hoz rendelt cselekvési területek irányítása megfelel a jelenlegi megbízatásának és általános feladatainak. Ezek a cselekvési területek konkrét profilokat vagy új feladatokat igényelhetnek, de ezek az ENISA meglévő forrásaiból fedezhetők, valamint a különböző feladatok újraelosztása vagy összekapcsolása révén megoldhatók. Az ENISA jelenleg hajtja végre azt a rövid távú programot, amelyet a Bizottság 2022-ben hozott létre a súlyos kiberbiztonsági eseményekre való felkészültség és reagálási kapacitások azonnali megerősítése érdekében. A vonatkozó szolgáltatások keretében lehetőség lesz a tagállamoknak való segítségnyújtásra a kritikus szervezeteket érintő súlyos kiberbiztonsági események esetén. Az ENISA megkezdte e rövid távú program végrehajtását, és az ennek eredményeképpen felmerült releváns és értékes meglátásokat figyelembe vették e rendelet előkészítése során. A rövid távú programhoz rendelt források e rendelet összefüggésében is felhasználhatók.

1.6. A javaslat/kezdeményezés időtartama és pénzügyi hatása

☒ **határozott időtartam**

– ☒ a kiberbiztonsági fenyegetések és események észlelése, valamint az azokra való felkészülés és reagálás céljából az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról szóló európai parlamenti és tanácsi rendeletre (a kiberszolidaritásról szóló jogszabály) irányuló javaslat elfogadásának időpontjától hatályos.

– ☒ pénzügyi hatás: 2023-tól 2027-ig a kötelezettségvállalási előirányzatok esetében, illetve 2023-tól 2031-ig a kifizetési előirányzatok esetében[34]

☐ **határozatlan időtartam**

– beindítási időszak: ÉÉÉÉ-tól/-től ÉÉÉÉ-ig

– azt követően: rendes ütem

1.7. Tervezett költségvetés-végrehajtási módszer(ek)[35]

☒ **Közvetlen irányítás** a Bizottság által

– ☒ a Bizottság szervezeti egységein keresztül, ideértve az uniós küldöttségek személyzetét

– ☐ végrehajtó ügynökségen keresztül

☐ **Megosztott irányítás** a tagállamokkal

☒ **Közvetett irányítás** a költségvetés végrehajtásával kapcsolatos feladatoknak a következőkre történő átruházásával:

– ☐ harmadik országok vagy az általuk kijelölt szervek

– ☐ nemzetközi szervezetek és ügynökségeik (nevezze meg)

– ☐ az EBB és az Európai Beruházási Alap

– ☒ a költségvetési rendelet 70. és 71. cikkében említett szervek

– ☐ közjogi szervek

– ☐ magánjog alapján működő, közfeladatot ellátó szervek, amennyiben megfelelő pénzügyi garanciákkal rendelkeznek;

– ☐ valamely tagállam magánjoga alapján működő, köz- és magánszféra közötti partnerség végrehajtásával megbízott és megfelelő pénzügyi garanciákkal rendelkező szervek;

– ☐ az EUSZ V. címének értelmében a KKBP terén konkrét fellépések végrehajtásával megbízott, és a vonatkozó alap-jogiaktusban ekként megjelölt szervek vagy személyek.

– *Egynél több irányítási módszer feltüntetése esetén kérjük, adjon részletes felvilágosítást a „Megjegyzések” rovatban.*

---

34 A jogszabályban foglalt intézkedéseket a következő többéves pénzügyi keretnek kell támogatnia.

35 A költségvetés-végrehajtási módszerek ismertetése, valamint a költségvetési rendeletre való megfelelő hivatkozások megtalálhatók a Budgpedia oldalon: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

Megjegyzések

Az Európai Kiberpajzshoz kapcsolódó intézkedéseket az ECCC hajtja végre. Amíg az ECCC nem rendelkezik kapacitással saját költségvetésének végrehajtására, az Európai Bizottság az ECCC nevében közvetlen irányítással hajtja végre az intézkedéseket. Az ECCC részvételi szándék kifejezésére való felhívás alapján is kiválaszthat szervezeteket az eszközök közös beszerzésében való részvételre. Az ECCC ezen eszközök működtetéséhez támogatást ítélhet oda. Ezenfelül az ECCC támogatást ítélhet oda a kiberbiztonsági vészhelyzeti mechanizmus keretében végzett felkészültségi intézkedésekhez. A Bizottság általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. A Bizottság hozzájárulási megállapodások révén részben vagy egészben az ENISA-t bízhatja meg az uniós kiberbiztonsági tartalék működtetésével és igazgatásával. Az e rendelet alapján az ENISA-ra ruházott intézkedések összhangban vannak az ENISA jelenlegi megbízatásával. A szóban forgó intézkedések a következők: i. a Kiberbiztonsági Együttműködési Csoport támogatása a felkészültségi intézkedések kockázatértékelések alapján történő kidolgozásában; ii. a Bizottság támogatása az uniós kiberbiztonsági tartalék létrehozása és végrehajtásának felügyelete terén, beleértve a támogatás iránti kérelmek fogadását és feldolgozását is; iii. sablon kidolgozása a támogatás iránti kérelmek benyújtásának megkönnyítésére és a szolgáltató és az uniós kiberbiztonsági tartalékból támogatásban részesülő felhasználó közötti egyedi megállapodások kidolgozása; iv. egy konkrét jelentős vagy nagyszabású kiberbiztonsági eseménnyel kapcsolatos fenyegetések, sebezhetőségek és mérséklési intézkedések felülvizsgálata és értékelése, valamint jelentések készítése. A becslések szerint mindezen feladatok az ENISA meglévő erőforrásaiból mintegy 7 teljes munkaidős egyenértéket igényelnek, építve az ENISA szakértelmére és az általa a felkészültséghez és a kiberbiztonsági eseményekre való reagáláshoz nyújtott vészhelyzeti támogatás kísérleti projektje keretében végzett előkészítő munkára.

2. IRÁNYÍTÁSI INTÉZKEDÉSEK

2.1. A nyomon követésre és a jelentéstételre vonatkozó rendelkezések

Gyakoriság és feltételek

A Bizottság nyomon fogja követni ezen új rendelkezések végrehajtását, alkalmazását és az azoknak való megfelelést azzal a céllal, hogy értékelje eredményességüket. A Bizottság az e rendelet alkalmazásának kezdőnapjától számított négy éven belül jelentést nyújt be az Európai Parlamentnek és a Tanácsnak a rendelet értékeléséről és felülvizsgálatáról.

2.2. Irányítási és kontrollrendszer(ek)

2.2.1. Az irányítási módszer(ek), a finanszírozás végrehajtási mechanizmusai, a kifizetési módok és a javasolt kontrollstratégia indokolása

A rendelet létrehozza az uniós finanszírozás végrehajtási keretét annak érdekében, hogy jelentős és nagyszabású kiberbiztonsági események esetére az észlelési, reagálási és helyreállítási képességeket javító intézkedések révén növelje a rezilienciát a kiberbiztonság terén. A DG CNECT szakpolitikai területért felelős egységei irányítják az irányelv végrehajtását.

Az új feladatok ellátása érdekében megfelelő erőforrásokat kell biztosítani a Bizottság szolgálatai számára. Az új rendelet végrehajtásához a becslések szerint 6 teljes munkaidős egyenértékre (ebből 3 AD és 3 CA) van szükség a következő feladatok ellátásához:

- a felkészültségi intézkedések meghatározása kockázatértékelések alapján;
- a határokon átnyúló biztonsági műveleti központok platformjai közötti interoperabilitás biztosítása;
- lehetséges végrehajtási jogi aktusok kidolgozása (kettő a biztonsági műveleti központok, kettő pedig a kiberbiztonsági vészhelyzeti mechanizmus esetében);
- a biztonsági műveleti központok üzemeltetési és használati megállapodásainak kezelése;
- az uniós kiberbiztonsági tartalék létrehozása és kezelése közvetlenül vagy hozzájárulási megállapodás alapján az ENISA révén. Az ENISA-val kötött hozzájárulási megállapodás esetén az ENISA-ra bízott feladatok tekintetében a hozzájárulási megállapodás kidolgozása és végrehajtásának felügyelete;
- részvétel az ENISA által a jelentős és nagyszabású kiberbiztonsági események felülvizsgálata és értékelése, valamint a jelentések elkészítése céljából összehívott konzultációs csoportokban.

2.2.2. A felismert kockázatokkal és a csökkentésükre létrehozott belső kontrollrendszerekkel kapcsolatos információk

Az Európai Kiberpajzs tekintetében azonosított kockázat az, hogy a tagállamok nem osztanak meg elegendő mennyiségű releváns kiberfenyegetésekkel kapcsolatos információt sem a határokon átnyúló SOC-platformokon belül, sem pedig a határokon átnyúló platformok és más releváns uniós szintű szervezetek között. E kockázatok csökkentése érdekében a finanszírozás elosztására részvételi szándék kifejezésére való felhívást követően kerül sor, amelynek nyomán a tagállamok

kötelezettséget vállalnak arra, hogy bizonyos mennyiségű információt megosztanak az uniós szinttel. E kötelezettségvállalás ezt követően egy üzemeltetési és használati megállapodás keretében ölt hivatalos formát, amely felhatalmazza az ECCC-t arra, hogy ellenőrzéseket végezzen annak biztosítása érdekében, hogy a közösen beszerzett eszközöket és infrastruktúrát a megállapodással összhangban használják. A határokon átnyúló biztonsági műveleti központokon belüli magas szintű információmegosztásra vonatkozó kötelezettségvállalásokat konzorciumi megállapodás ölti hivatalos formába.

A kiberbiztonsági vészhelyzeti mechanizmus tekintetében azonosított kockázat az, hogy a mechanizmusban részt vevő felhasználók nem tesznek megfelelő intézkedéseket annak érdekében, hogy biztosítsák a kibertámadásokkal szembeni felkészültséget. Ezért ahhoz, hogy támogatást kaphassanak az uniós kiberbiztonsági tartalékból, a felhasználók kötelesek ilyen felkészültségi intézkedéseket hozni. Amikor a felhasználók támogatás iránti kérelmet nyújtanak be az uniós kiberbiztonsági tartalékhoz, ismertetniük kell, hogy milyen korábbi intézkedéseket hoztak a kiberbiztonsági eseményekre való reagálás érdekében, amelyeket figyelembe fognak venni az uniós kiberbiztonsági tartalékhoz benyújtott kérelmek értékelése során.

2.2.3. A kontroll költséghatékonyságának becslése és indokolása (a „kontroll költségei ÷ a kezelt kapcsolódó források értéke” hányados) és a hibakockázat várható szintjeinek értékelése (kifizetéskor és záráskor)

Mivel a Digitális Európa programban való részvételre vonatkozó, a kiberszolidaritásról szóló jogszabály keretében nyújtott támogatásra alkalmazandó szabályok hasonlóak azokhoz, amelyeket a Bizottság a munkaprogramjaiban fog alkalmazni, és a kedvezményezettek körének és a közvetlen irányítás alatt álló programok kedvezményezetti körének kockázati profilja hasonló, a hibahatár várhatóan hasonló lesz ahhoz, amit a Bizottság a Digitális Európa program esetében vár, vagyis megalapozott bizonyossággal szolgál arra, hogy a többéves finanszírozási időszak alatt az éves kockázati szint a 2–5 %-os tartományban marad, és végső soron a többéves programok lezárását követően az összes audit, valamint korrekciós és visszakövetelési intézkedés pénzügyi hatásainak figyelembevételével a fennmaradó hibaarány a lehető legjobban megközelítse a 2 %-ot.

2.3. A csalások és a szabálytalanságok megelőzésére vonatkozó intézkedések

Tüntesse fel a meglévő vagy tervezett megelőző és védintézkedéseket, pl. a csalás elleni stratégiából.

Az Európai Kiberpajzs esetében az ECCC hatáskörrel rendelkezik arra, hogy az információkhoz való hozzáférés és a helyszíni ellenőrzések alapján ellenőrizze a közösen beszerzett eszközöket és infrastruktúrákat, az üzemeltetési konzorcium és az ECCC között aláírandó üzemeltetési és használati megállapodással összhangban.

Az uniós intézmények, szervek és ügynökségek tekintetében a csalások megelőzésére vonatkozó jelenlegi intézkedések a rendelethez szükséges további előirányzatokra is vonatkoznak.

3. A JAVASLAT/KEZDEMÉNYEZÉS BECSÜLT PÉNZÜGYI HATÁSA

3.1. A többéves pénzügyi keret érintett fejezete/fejezetei és a költségvetés érintett kiadási sora/sorai

- Jelenlegi költségvetési sorok

A többéves pénzügyi keret fejezetei, azon belül pedig a költségvetési sorok sorrendjében.

A többéves pénzügyi keret fejezete	Költségvetési sor	Kiadás típusa	Hozzájárulás			
	Szám	diff./nem diff.[36]	EFTA-országoktól[37]	tagjelölt országoktól és potenciális tagjelöltektől[38]	más harmadik országoktól	egyéb címzett bevétel
1	02 04 01 10 – Digitális Európa program – Kiberbiztonság	diff.	IGEN	IGEN	NEM	NEM
1	02 04 01 11 – Digitális Európa program – Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont	diff.	IGEN	IGEN	NEM	NEM
1	02 04 03 – Digitális Európa program – Mesterséges intelligencia	diff.	IGEN	IGEN	NEM	NEM
1	02 04 04 – Digitális Európa program – Készségek	diff.	IGEN	IGEN	NEM	NEM
1	02 01 30 – A Digitális Európa programhoz kapcsolódó támogatási kiadások	nem diff.	IGEN	IGEN	NEM	NEM

[36] diff. = differenciált előirányzatok / nem diff. = nem differenciált előirányzatok.
[37] EFTA: Európai Szabadkereskedelmi Társulás.
[38] Tagjelölt országok és adott esetben a lehetséges tagjelölt országok.

3.2. A javaslat előirányzatokra gyakorolt becsült pénzügyi hatása

3.2.1. Az operatív előirányzatokra gyakorolt becsült hatás összefoglalása

– ☐ A javaslat/kezdeményezés nem vonja maga után operatív előirányzatok felhasználását

– ☒ A javaslat/kezdeményezés az alábbi operatív előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

A többéves pénzügyi keret fejezete	Szám	1 **Egységes piac, innováció és digitális gazdaság**

A javaslat nem növeli a Digitális Európa program keretében tett kötelezettségvállalások teljes szintjét. Az e kezdeményezéshez való hozzájárulás a 2. és 4. sz. egyedi célkitűzéshez rendelt kötelezettségvállalások újraelosztása a 3. sz. egyedi célkitűzés és az ECCC költségvetésének megerősítése érdekében. Ha a Digitális Európa program keretében tett kötelezettségvállalások a többéves pénzügyi keret felülvizsgálata nyomán növekednek, az felhasználható e kezdeményezés céljára.

A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága (DG CONNECT)			**2025**. év	**2026**. év	**2027**. év	**2028+.** év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.			**ÖSSZESEN**
○ Operatív előirányzatok										
02.040110 költségvetési sor[39] (újraelosztás a 02.0403 és 02.0404 költségvetési tételből)	Kötelezettségvállalási előirányzatok	(1a)	15,000	15,000	6,000	p.m.				**36,000**
	Kifizetési előirányzatok	(2a)	15,000	15,000	6,000					**36,000**
02.040111.02 költségvetési sor (újraelosztás a 02.0403 és 02.0404 költségvetési tételből)	Kötelezettségvállalási előirányzatok	(1b)	13,000	23,000	28,000	p.m.				**64,000**
	Kifizetési előirányzatok	(2b)	8,450	18,200	25,250	12,100				**64,000**
Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok[40]										

[39] A hivatalos költségvetési nómenklatúra szerint.

Költségvetési sor 02.0130		(3)	0,150	0,150	0,150	p.m.				0,450
A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatóságához tartozó előirányzatok ÖSSZESEN	Kötelezettségvállalási előirányzatok	=1a+1b +3	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Kifizetési előirányzatok	=2a+2b +3	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

○ Operatív előirányzatok ÖSSZESEN	Kötelezettségvállalási előirányzatok	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Kifizetési előirányzatok	(5)	23,450	33,200	31,250	12,100				**100,000**
○ Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN		(6)	0,150	0,150	0,150	p.m.				**0,450**
A többéves pénzügyi keret **1. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**	Kötelezettségvállalási előirányzatok	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Kifizetési előirányzatok	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

Ha a javaslat/kezdeményezés egynél több operatív fejezetet is érint, ismételje meg a fenti szakaszt:

○ Operatív előirányzatok ÖSSZESEN (összes operatív fejezet)	Kötelezettségvállalási előirányzatok	(4)	28,000	38,000	34,000	p.m.				**100,000**
	Kifizetési	(5)	23,450	33,200	31,250	12,100				**100,000**

[40] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

	előirányzatok									
Bizonyos egyedi programok keretéből finanszírozott igazgatási jellegű előirányzatok ÖSSZESEN (összes operatív fejezet)		(6)	0,150	0,150	0,150					**0,450**
A többéves pénzügyi keret **1–6. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN** (Referenciaösszeg)	Kötelezettségvállalási előirányzatok	=4+ 6	**28,150**	**38,150**	**34,150**	**p.m.**				**100,450**
	Kifizetési előirányzatok	=5+ 6	**23,600**	**33,350**	**31,400**	**12,100**				**100,450**

A többéves pénzügyi keret fejezete	7.	„Igazgatási kiadások”

Ezt a részt az igazgatási jellegű költségvetési adatok táblázatában kell kitölteni, melyet először a pénzügyi kimutatás mellékletébe (az Európai Unió általános költségvetése Bizottságra vonatkozó szakaszának végrehajtására vonatkozó belső szabályzatról szóló bizottsági határozat 5. melléklete) kell bevezetni; a mellékletet a szolgálatközi konzultációhoz fel kell tölteni a DECIDE rendszerbe.

millió EUR (három tizedesjegyig)

		2025. év	2026. év	2027. év	**2028+.** év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.			**ÖSSZESEN**
Főigazgatóság: DG CONNECT									
○ Humánerőforrás		0,786	0,786	0,786	p.m.				**2,358**
○ Egyéb igazgatási kiadások		0,035	0,035	0,035	p.m.				**0,105**
A Tartalmak, Technológiák és Kommunikációs Hálózatok Főigazgatósága ÖSSZESEN	Előirányzatok	**0,821**	**0,821**	**0,821**					**2,463**

A többéves pénzügyi keret **7. FEJEZETÉHEZ tartozó előirányzatok ÖSSZESEN**	(Összes kötelezettségvállalási előirányzat = Összes kifizetési előirányzat)	**0,821**	**0,821**	**0,821**					**2,463**

millió EUR (három tizedesjegyig)

		2025. év	2026. év	2027. év	**2028+.** év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.			**ÖSSZESEN**
A többéves pénzügyi keret **1–7. FEJEZETÉHEZ tartozó**	Kötelezettségvállalási előirányzatok	**28,971**	**38,971**	**34,971**	**p.m.**				**102,913**

előirányzatok ÖSSZESEN	Kifizetési előirányzatok	**24,421**	**34,171**	**32,221**	**12,100**				**102,913**

3.2.2. Operatív előirányzatokból finanszírozott becsült kimenet

Kötelezettségvállalási előirányzatok, millió EUR (három tizedesjegyig)

Tüntesse fel a célkitűzéseket és a kimeneteket ⇩			**N**. év		**N+1**. év		**N+2**. év		**N+3**. év		A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.						**ÖSSZESEN**	
	KIMENETEK																	
	Típus [41]	Általános költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Szám	Költség	Összesített szám	Összköltség
1. KONKRÉT CÉLKITŰZÉS[42] …																		
– Kimenet																		
– Kimenet																		
– Kimenet																		
1. konkrét célkitűzés részösszege																		
2. KONKRÉT CÉLKITŰZÉS …																		
– Kimenet																		
2. konkrét célkitűzés részösszege																		
ÖSSZESEN																		

[41] A kimenetek a nyújtandó termékek és szolgáltatások (pl. finanszírozott diákcserék száma, épített utak hossza kilométerben stb.).

[42] Az 1.4.2. szakaszban („Konkrét célkitűzés(ek)…”) feltüntetett célkitűzés.

3.2.3. Az igazgatási előirányzatokra gyakorolt becsült hatás összefoglalása

– ☐ A javaslat/kezdeményezés nem vonja maga után igazgatási jellegű előirányzatok felhasználását.

– ☒ A javaslat/kezdeményezés az alábbi igazgatási jellegű előirányzatok felhasználását vonja maga után:

millió EUR (három tizedesjegyig)

	2025. év	**2026**. év	**2027**. év	**N+3.** év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.	**ÖSSZESEN A többéves pénzügyi keret 7. FEJEZETE**
Humánerőforrás	0,786	0,786	0,786			**2,358**
Egyéb igazgatási kiadások	0,035	0,035	0,035			**0,105**
A többéves pénzügyi keret 7. FEJEZETÉNEK részösszege	**0,821**	**0,821**	**0,821**			**2,463**

A többéves pénzügyi keret 7. FEJEZETÉBE[43] bele nem tartozó előirányzatok								
Humánerőforrás								
Egyéb igazgatási jellegű kiadások	0,150	0,150	0,150					**0,450**
A többéves pénzügyi keret 7. FEJEZETÉBE bele nem tartozó előirányzatok részösszege	**0,150**	**0,150**	**0,150**					**0,450**

ÖSSZESEN	**0,971**	**0,971**	**0,971**					**2,913**

A humánerőforrással és más igazgatási jellegű kiadásokkal kapcsolatos előirányzat-igényeket az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt előirányzatokkal és/vagy az adott főigazgatóságon belüli átcsoportosítással kell teljesíteni. A források adott esetben a költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további allokációkkal.

[43] Technikai és/vagy igazgatási segítségnyújtás, valamint uniós programok és/vagy intézkedések végrehajtásához biztosított támogatási kiadások (korábban: BA-tételek), közvetett kutatás, közvetlen kutatás.

3.2.3.1. Becsült humánerőforrás-szükségletek

– ☐ A javaslat/kezdeményezés nem igényel humánerőforrást.

– ☒ A javaslat/kezdeményezés az alábbi humánerőforrás-igénnyel jár:

A becsléseket teljes munkaidős egyenértékben kell kifejezni

		2025. év	**2026**. év	2027. év	**N+3**. év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.		
O A létszámtervben szereplő álláshelyek (tisztviselők és ideiglenes alkalmazottak)								
20 01 02 01 (a központban és a bizottsági képviseleteken)		3	3	3				
20 01 02 03 (a küldöttségeknél)								
01 01 01 01 (közvetett kutatás)								
01 01 01 11 (közvetlen kutatás)								
Egyéb költségvetési sor (kérjük megnevezni)								
O Külső munkatársak teljes munkaidős egyenértékben (FTE) kifejezve[44]								
20 02 01 (AC, END, INT a teljes keretből)		3	3	3				
20 02 03 (AC, AL, END, INT és JPD a küldöttségeknél)								
XX 01 xx **yy zz** [45]	- a központban							
	- a küldöttségeknél							
01 01 01 02 (AC, END, INT – közvetett kutatás)								
01 01 01 12 (AC, END, INT – közvetlen kutatás)								
Egyéb költségvetési sor (kérjük megnevezni)								
ÖSSZESEN		**6**	**6**	**6**				

XX az érintett szakpolitikai terület vagy költségvetési cím.

A humánerőforrás-igényeknek az adott főigazgatóság rendelkezésére álló, az intézkedés irányításához rendelt és/vagy az adott főigazgatóságon belül átcsoportosított személyzettel kell eleget tenni. A források adott esetben a meglévő költségvetési korlátok betartása mellett kiegészíthetők az éves elosztási eljárás keretében az irányító főigazgatósághoz rendelt további allokációkkal.

Az elvégzendő feladatok leírása:

Tisztviselők és ideiglenes alkalmazottak	- a felkészültségi intézkedések meghatározása kockázatértékelések alapján (11. cikk); - lehetséges végrehajtási jogi aktusok kidolgozása (kettő a biztonsági műveleti központok, kettő pedig a kiberbiztonsági vészhelyzeti mechanizmus esetében); - a biztonsági műveleti központok üzemeltetési és használati megállapodásainak kezelése; - az uniós kiberbiztonsági tartalék létrehozása és kezelése közvetlenül vagy hozzájárulási megállapodás alapján az ENISA révén.
Külső munkatársak	a felkészültségi intézkedések meghatározása tisztviselő felügyelete mellett és kockázatértékelések alapján (11. cikk); - - lehetséges végrehajtási jogi aktusok kidolgozása (kettő a biztonsági műveleti

[44] AC = szerződéses alkalmazott; AL = helyi alkalmazott; END = kirendelt nemzeti szakértő; INT = kölcsönmunkaerő (átmeneti alkalmazott); JPD = küldöttségi pályakezdő szakértő.

[45] Az operatív előirányzatokból finanszírozott külső munkatársakra vonatkozó részleges felső határérték (korábban: BA-tételek).

	központok, kettő pedig a kiberbiztonsági vészhelyzeti mechanizmus esetében); - a biztonsági műveleti központok üzemeltetési és használati megállapodásainak kezelése; - az uniós kiberbiztonsági tartalék létrehozása és kezelése közvetlenül vagy hozzájárulási megállapodás alapján az ENISA révén.

3.2.4. A jelenlegi többéves pénzügyi kerettel való összeegyeztethetőség

A javaslat/kezdeményezés

– [X] teljes mértékben finanszírozható a többéves pénzügyi keret érintett fejezetén belüli átcsoportosítás révén.

Fejtse ki, miként kell átprogramozni a pénzügyi keretet: tüntesse fel az érintett költségvetési sorokat és a megfelelő összegeket. Jelentős átprogramozás esetén mellékeljen Excel-táblát.

	23	24	25	26	27	összesen
1. sz. egye	16 232 897	20 528 765	17 406 899	16 223 464	10 022 366	80 414 391
eredeti 2.	226 316 819	295 067 000	195 649 000	221 809 000	246 608 000	1 185 449 819
átcsoportosítás a kiberbiztonsági kezd			18 000 000	28 000 000	19 000 000	65 000 000
ÚJ 2. sz. e	**226 316 819**	**295 067 000**	**177 649 000**	**193 809 000**	**227 608 000**	**1 120 449 819**
3. sz. egye	24 361 553	35 596 172	3 638 000	3 638 000	11 175 000	78 408 725
átcsoportosítás a 2–4. sz. egyedi célkit			15 000 000	15 000 000	6 000 000	36 000 000
ÚJ 3. sz. e	**24 361 553**	**35 596 172**	**18 638 000**	**18 638 000**	**17 175 000**	**114 408 725**
eredeti EC	176 222 303	208 374 879	104 228 130	90 704 986	84 851 497	664 381 795
átcsoportosítás a 2–4. sz. egyedi célkit			13 000 000	23 000 000	28 000 000	64 000 000
Új ECCC	**176 222 303**	**208 374 879**	**117 228 130**	**113 704 986**	**112 851 497**	**728 381 795**
eredeti 4.	66 902 708	64 892 032	56 577 977	70 477 245	72 107 201	330 957 163
átcsoportosítás a kiberbiztonsági kezd			10 000 000	10 000 000	15 000 000	35 000 000
ÚJ 4. sz. e	**66 902 708**	**64 892 032**	**46 577 977**	**60 477 245**	**57 107 201**	**295 957 163**

– [ ] a többéves pénzügyi keret lekötetlen mozgásterének és/vagy a többéves pénzügyi keretről szóló rendeletben meghatározott különleges eszközök felhasználását teszi szükségessé.

Fejtse ki, mire van szükség, meghatározva az érintett fejezeteket és költségvetési sorokat, a megfelelő összegeket és a felhasználni javasolt eszközöket.

– [ ] a többéves pénzügyi keret módosítását teszi szükségessé.

Fejtse ki a szükségleteket: tüntesse fel az érintett fejezeteket és költségvetési sorokat és a megfelelő összegeket.

3.2.5. Harmadik felek részvétele a finanszírozásban

A javaslat/kezdeményezés

– [X] nem irányoz elő harmadik felek általi társfinanszírozást.

– [ ] előirányoz harmadik felek általi társfinanszírozást az alábbi becslések szerint:

előirányzatok, millió EUR (három tizedesjegyig)

	N. év[46]	**N+1.** év	**N+2.** év	**N+3.** év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.			Összesen
Tüntesse fel a társfinanszírozó szervet								
Társfinanszírozott előirányzatok ÖSSZESEN								

[46] Az N. év a javaslat/kezdeményezés végrehajtásának első éve. Az „N” helyére a végrehajtás várható első évét kell beírni (például: 2021). A következő évek esetében ugyanígy kell eljárni.

3.3. A bevételre gyakorolt becsült hatás

– ☒ A javaslatnak/kezdeményezésnek nincs pénzügyi hatása a bevételre.

– ☐ A javaslatnak/kezdeményezésnek van pénzügyi hatása – a bevételre gyakorolt hatása a következő:

  – ☐ a javaslat a saját forrásokra gyakorol hatást

  – ☐ a javaslat az egyéb bevételekre gyakorol hatást

  – kérjük adja meg, hogy a bevétel kiadási sorhoz van-e rendelve ☐

millió EUR (három tizedesjegyig)

Bevételi költségvetési sor:	Az aktuális költségvetési évben rendelkezésre álló előirányzatok	A javaslat/kezdeményezés hatása[47]						
		N. év	**N+1.** év	**N+2.** év	**N+3.** év	A táblázat a hatás időtartamának megfelelően (vö. 1.6. pont) további évekkel bővíthető.		
... jogcímcsoport								

A címzett bevételek esetében tüntesse fel az érintett kiadáshoz tartozó költségvetési sor(oka)t.

[…]

Egyéb megjegyzések (pl. a bevételre gyakorolt hatás számítására használt módszer/képlet vagy egyéb más információ).

[…]

[47] A tradicionális saját források (vámok, cukorilletékek) tekintetében nettó összeget kell megadni, amely a 20 %-kal (beszedési költségek) csökkentett bruttó összegnek felel meg.