Az Európai Unió
Tanácsa

Brüsszel, 2025. június 6.
(OR. en)

9794/25

Intézményközi referenciaszám:
2025/0036(NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Dátum:	2025. június 6.
Címzett:	a delegációk
Tárgy:	A Tanács ajánlása a kiberbiztonsági válságkezelésre vonatkozó uniós tervről – A Tanács által a 2025. június 6-i ülésén jóváhagyott tanácsi ajánlás

Mellékelten továbbítjuk a delegációknak a Tanács által a 2025. június 6-i ülésén jóváhagyott tanácsi ajánlást.

MELLÉKLET

A TANÁCS AJÁNLÁSA

a kiberbiztonsági válságkezelésre vonatkozó uniós tervről

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. és 292. cikkére,

tekintettel az Európai Bizottság javaslatára,

mivel:

(1) A digitális technológia és a globális konnektivitás az Unió gazdasági növekedésének, versenyképességének és a kritikus infrastruktúrák átalakulásának gerincét képezi. Az összekapcsolt és egyre digitalizáltabb gazdaság ugyanakkor növeli a kiberbiztonsági események és a kibertámadások kockázatát. A rossz szándékú kibertevékenységek hatása, volumene és kifinomultsága fémjelzi a fokozódó geopolitikai feszültségeket, konfliktusokat és stratégiai rivalizálást. Az ilyen tevékenységek hibrid kampányok vagy katonai műveletek részét is képezhetik. Mindemellett közvetlen hatással lehetnek az Unió biztonságára, gazdaságára és társadalmára. Ezenfelül továbbgyűrűző hatással is járhatnak, különösen akkor, ha célkeresztjükben nemzetközi stratégiai partnerországok, például tagjelölt vagy szomszédos országok állnak.

(2) Egy nagyszabású kiberbiztonsági esemény akár olyan mértékű zavart is okozhat, amely meghaladja az érintett tagállam reagálási képességét, vagy amely több tagállamra is jelentős hatást gyakorol. Okuktól és hatásuktól függően ezek az események eszkalálódhatnak, és olyan teljes körű válsággá válhatnak, amely kihat a belső piac megfelelő működésére, illetve súlyos közrendi és közbiztonsági kockázatot jelent a szervezetekre vagy a polgárokra nézve több tagállamban vagy az Unió egészében. A hatékony válságkezelés elengedhetetlen a gazdasági stabilitás fenntartásához, az európai kormányok, kritikus infrastruktúrák, vállalkozások és polgárok védelméhez, valamint a kibertér nemzetközi biztonságához és stabilitásához. A kiberbiztonsági válságkezelés ennek megfelelően az átfogó uniós válságkezelési keret szerves része.

(3) Tekintettel az uniós szervezetek és a tagállamok IKT-környezetei közötti kölcsönös függőségekre és összekapcsolódásokra, egy uniós szervezeten belüli esemény kiberbiztonsági kockázatot jelenthet a tagállamok számára, és ugyanez igaz fordítva is. A nagyszabású kiberbiztonsági eseményekkel és az (EU, Euratom) 2023/2841 rendelet[1] 3. cikkének 8. pontjában meghatározott súlyos biztonsági eseményekkel kapcsolatos releváns információk megosztása és a koordináció kulcsfontosságú a kiberbiztonsági válságkezelésre vonatkozó uniós tervvel (a továbbiakban: kiberbiztonsági terv) összefüggésben.

[1] Az Európai Parlament és a Tanács (EU, Euratom) 2023/2841 rendelete (2023. december 13.) az uniós intézmények, szervek, hivatalok és ügynökségek egységesen magas szintű kiberbiztonságát biztosító intézkedések meghatározásáról (HL L, 2023/2841, 2023.12.18., 1.o.).

(4) Olyan válság esetén, amelyre vonatkozóan aktiválták az (EU) 2018/1993 tanácsi végrehajtási határozat[2] szerinti uniós politikai szintű integrált válságelhárítási mechanizmust (a továbbiakban: IPCR), a kiberbiztonsági tervnek a koordináció és elhárítás tekintetében teljes mértékben tiszteletben kell tartania az IPCR-t. A politikai és stratégiai koordinációra az IPCR keretében kerülne sor. Az IPCR az uniós politikai szintű horizontális koordináció és elhárítás eszköze. Az IPCR értelmében a mechanizmus aktiválására, illetve alkalmazásának megszüntetésére vonatkozó döntést az Európai Unió Tanácsának elnöksége hozza meg. A Bizottság szolgálatai és az Európai Külügyi Szolgálat (EKSZ) által készített integrált helyzetismereti és -elemzési jelentések támogatják az IPCR munkáját annak információmegosztási és teljes aktiválási üzemmódjában egyaránt.

(5) A kiberbiztonsági események és a kiberválságok kezelése elsődlegesen a tagállamok felelőssége. A kiberbiztonsági események esetleges határokon és ágazatokon átnyúló jellege ugyanakkor megköveteli a tagállamoktól és az érintett uniós szervezetektől, hogy technikai, operatív és politikai szinten együttműködjenek az Unión belüli hatékony koordináció érdekében. A teljes életciklusra kiterjedő kiberbiztonsági válságkezelés magában foglalja a nagyszabású kiberbiztonsági események előrejelzését szolgáló felkészültséget és közös helyzetismeretet, a nagyszabású kiberbiztonsági események megfékezését és hatásainak mérséklését szolgáló megfelelő elhárítási és helyreállítási eszközök azonosításához szükséges felderítési képességeket, valamint az újabb eseményektől való elrettentést és azok megelőzését szolgáló reagálási képességeket.

[2] A Tanács (EU) 2018/1993 végrehajtási határozata (2018. december 11.) az uniós politikai szintű integrált válságelhárítási mechanizmusról (HL L 320., 2018.12.17., 28. o.).

(6) A nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról szóló (EU) 2017/1584 bizottsági ajánlás[3] meghatározza a tagállamok és az uniós szervezetek közötti együttműködés céljait és módjait a nagyszabású kiberbiztonsági eseményekre és kiberválságokra való reagálás terén. Feltérképezi a technikai, operatív és politikai szinten érintett szereplőket, és kifejti, azok hogyan integrálódnak a meglévő uniós válságkezelési mechanizmusokba, így például az IPCR-be. Az (EU) 2017/1584 ajánlásban meghatározott alapelvek, nevezetesen a szubszidiaritás, a komplementaritás és az információk bizalmas kezelése, valamint a háromszintű (technikai, operatív és politikai) megközelítés továbbra is érvényesek. Ez az ajánlás ezekre az alapelvekre épül, és célja, hogy felváltsa az (EU) 2017/1584 ajánlást, és ezzel meghatározza a kiberbiztonsági válságkezelés új uniós keretét.

(7) Az ezen ajánlásban használt fogalommeghatározások közül néhány az (EU) 2022/2555 irányelvben[4] használt fogalommeghatározásokon és terminusokon alapul. Ezen ajánlás hatálya azonban eltér az (EU) 2022/2555 irányelv hatályától. Ez az ajánlás a nagyszabású kiberbiztonsági eseményekre és az ilyen eseményekből eredő kiberválságokra való általános uniós felkészültséggel összefüggésben meghatározza a kiberbiztonsági válságkezelés uniós keretét, amely az érintett ágazattól vagy szervezettől függetlenül minden ilyen eseményre érvényes. Amennyire lehetséges, a fogalommeghatározások az (EU) 2022/2555 irányelvben foglalt fogalommeghatározásokon alapulnak.

---

[3] 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.).

[4] 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.).

(8) Szükség van egy naprakésszé tett kiberbiztonsági tervre, hogy egyértelmű és hozzáférhető iránymutatás álljon rendelkezésre, amely ismerteti a nagyszabású kiberbiztonsági esemény és az uniós szintű kiberválság fogalmát, a válságkezelési keret aktiválásának módját, az érintett uniós szintű hálózatok, szereplők és mechanizmusok szerepét, valamint az e szereplők és mechanizmusok közötti interakciót a kiberválság teljes életciklusa során. A kiberbiztonsági terv célja, hogy – többek között az EU és a NATO közötti kapcsolatok elmélyítésének összefüggésében – támogassa az uniós polgári-katonai kapcsolatok tágabb keretét a kiberbiztonsági válságkezelést illetően, lehetőség szerint többek között inkluzív, kölcsönös és megkülönböztetésmentes megerősített információmegosztási mechanizmusok révén a kiberbiztonsági válságkezelés terén.

(9) Az integrált válságelhárítás lehetővé tétele érdekében meg kell erősíteni az uniós szintű ágazatközi válságkezelést, különösen azokban az esetekben, amikor a nagyszabású kiberbiztonsági események és válsághelyzetek fizikai következményekkel járnak. Ez az ajánlás kiegészíti az IPCR-t és más uniós válságkezelési mechanizmusokat, így többek között a Bizottság által létrehozott, ARGUS elnevezésű általános sürgősségi riasztórendszert, az uniós polgári védelmi mechanizmusról szóló 1313/2013/EU európai parlamenti és tanácsi határozattal[5] létrehozott Veszélyhelyzet-reagálási Koordinációs Központ (ERCC) által támogatott uniós polgári védelmi mechanizmust (UCPM), az EKSZ válságelhárítási mechanizmusát (CRM), valamint más folyamatokat, például az uniós kiberdiplomáciai eszköztárban[6], a hibrid eszköztárban[7] és a hibrid fenyegetésekkel szembeni fellépés felülvizsgált uniós protokolljában[8] leírt folyamatokat. Kiegészíti továbbá a kritikus infrastruktúrák számottevő mértékben határokon átnyúló jelentőségű zavaraira való uniós szintű reagálás koordinálására szolgáló tervről szóló (EU) 2024/4371 tanácsi ajánlást[9] (a továbbiakban: a kritikus infrastruktúrákra vonatkozó uniós terv), és összhangban kell állnia az említett ajánlással, amely a nem kiberbiztonsági vonatkozású fizikai rezilienciára is kiterjed, és amelynek célja, hogy javítsa a koordinált uniós szintű reagálást e területen.

---

5 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.).

6 A Tanács következtetései a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről (9916/17)

7 A Tanács következtetései a hibrid hadjáratokra való összehangolt uniós reagálás keretéről, 2022. június 22.

8 Közös szolgálati munkadokumentum a hibrid fenyegetésekkel szembeni fellépés uniós operatív protokolljáról, SWD(2023) 116 final.

9 HL C, C/2024/4371, 2024.7.5.

(10) A nagyszabású kiberbiztonsági események és válsághelyzetek kezelésének operatív szintű koordinálása az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatának (a továbbiakban: EU-CyCLONe) feladata, többek között ágazatközi nagyszabású kiberbiztonsági események és kiberválság esetén is. Annak érdekében, hogy a meglévő keretek ne váljanak még összetettebbé, el kell kerülni olyan ágazati struktúrák létrehozását, amelyek megkettőznék az EU-CyCLONe feladatait. Az EU-CyCLONe-nak az ágazatoktól operatív kiberbiztonsági információkat kell kapnia, amelyeket politikai szinten is integrálni kell.

(11) A tagállamokat ara ösztönözzük, hogy teljes mértékben használják ki a releváns uniós programok által a kiberbiztonság céljára biztosított pénzügyi forrásokat. Gondoskodni kell arról, hogy ezek a programok minimális adminisztratív terheket rójanak a finanszírozást kérelmezőkre, és a tagállamok e programokban való részvételét megfelelő iránymutatás segítse az életképes pénzügyi támogatási lehetőségekre vonatkozóan.

(12) Ez az ajánlás hozzájárul a felkészültséget célzó azon szélesebb körű intézkedésekhez, amelyeket az Uniónak meg kell hoznia az ágazatközi válságokkal szemben, összhangban a felkészültségi unióról szóló uniós stratégiában foglalt elvekkel, nevezetesen az integrált, összkormányzati, az összes veszélyre és a társadalom egészére kiterjedő megközelítéssel, különös tekintettel a kockázatokkal és fenyegetésekkel kapcsolatos tudatosság növelésére és az ágazatközi válságelhárításra,

ELFOGADTA EZT AZ AJÁNLÁST:

I.: Az uniós kiberbiztonsági válságkezelési keret célja, hatálya és irányadó elvei

Cél és hatály

1. Ez a kiberbiztonsági válságkezelésre vonatkozó uniós tervről (a továbbiakban: kiberbiztonsági terv) szóló ajánlás meghatározza a kiberbiztonsági válságkezelés uniós keretét az EU nagyszabású kiberbiztonsági eseményekre és kiberválságokra való általános felkészültségének összefüggésében. A keret tükrözi mind a tagállamok, mind az uniós intézmények, szervek, hivatalok és ügynökségek (a továbbiakban: uniós szervezetek) szerepét saját hatáskörükön belül, a nemzeti jogszabályok és a belső szabályok teljes körű tiszteletben tartása mellett, az átfogó és koordinált uniós szintű fellépés biztosítása érdekében.

2. A kiberbiztonsági tervet a kritikus infrastruktúrákra vonatkozó uniós tervvel összhangban kell alkalmazni, különösen a kritikus infrastruktúrák fizikai rezilienciáját és kiberbiztonságát egyaránt érintő események esetében[10].

3. A kiberbiztonsági terv iránymutatást nyújt a nagyszabású kiberbiztonsági eseményekre vagy kiberválságokra való reagáláshoz, és azt bármely, így például a II. mellékletben felsorolt releváns ágazati válságelhárítási mechanizmussal kiegészítve kell alkalmazni. A kiberbiztonság tekintetében érdekelt feleknek nemzeti és uniós szinten egyaránt elő kell segíteniük és támogatniuk kell az említett ágazati mechanizmusok céljainak elérését.

4. Olyan uniós szintű ágazatközi válság esetén, amelynek kiberbiztonsági vetülete van, és amelyre vonatkozóan az IPCR-t aktiválják, az uniós politikai szintű reagálást a Tanácsnak kell koordinálnia, az IPCR alkalmazásával. Az IPCR aktiválását követően a kiberbiztonsági terv szerinti intézkedéseknek támogatniuk kell az uniós reagálást politikai szinten, konkrét kiberbiztonsági támogatást nyújtva.

[10] A kritikus infrastruktúrákra vonatkozó uniós terv a melléklete I. részének 4. szakaszában tovább részletezi az ilyen esetekben folytatott koordinációt.

Irányadó elvek

5. Az uniós szintű kiberbiztonsági válságkezelésre a következő irányadó elvek vonatkoznak:

a) *Arányosság*: a tagállamokat érintő kiberbiztonsági események többsége elmarad attól a szinttől, ami nemzeti vagy uniós szintű nagyszabású kiberbiztonsági eseménynek vagy kiberválságnak tekinthető. Kiberbiztonsági események és fenyegetések esetén a tagállamok önkéntes alapon, rendszeresen együttműködnek és információt cserélnek a számítógép-biztonsági eseményekre reagáló csoportok hálózatán (CSIRT-hálózat) és az EU-CyCLONe-on belül, a hálózatok eljárási standardjaival összhangban.

b) *Szubszidiaritás*: Az őket érintő kiberbiztonsági események, nagyszabású kiberbiztonsági események és kiberválság elhárítása és a helyreállítás elsődlegesen a tagállamok felelőssége. A határokon átnyúló lehetséges hatásokra tekintettel a Tanácsnak, a Bizottságnak, a főképviselőnek, az Európai Uniós Kiberbiztonsági Ügynökségnek (ENISA), az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjának (CERT-EU), az Europolnak és minden más érintett uniós szervezetnek a válság teljes életciklusa során együtt kell működnie. Ez a szerep az uniós jogból következik, és tükrözi azt, hogy a nagyszabású kiberbiztonsági események és kiberválságok hatással lehetnek az egységes piacon belüli gazdasági tevékenységek egy vagy több szegmensére, az Unió biztonságára és nemzetközi kapcsolataira, valamint magukra az uniós szervezetekre.

c) *Komplementaritás*: ez az ajánlás teljes mértékben figyelembe veszi a II. mellékletben felsorolt, meglévő uniós szintű válságkezelési mechanizmusokat, különösen az IPCR-t, az ARGUS-t és az EKSZ válságelhárítási mechanizmusát. Ez az ajánlás figyelembe veszi a CSIRT-hálózat és az EU-CyCLONe megbízatását, valamint az (EU, Euratom) 2023/2841 rendeletet. Az IPCR aktiválása esetén folytatni kell az érintett hálózatok, szervezetek és aktivált ágazati mechanizmusok munkáját, és e munkának hozzá kell járulnia az IPCR keretében zajló politikai és stratégiai koordinációhoz, és azt támogatnia kell.

d) *Az információk bizalmas kezelése*: az ezen ajánlással összefüggésben folytatott minden információcserének meg kell felelnie a biztonságra és a személyes adatok védelemére vonatkozó szabályoknak. Adott esetben figyelembe kell venni az olyan nem hivatalos titoktartási megállapodásokat, mint például az érzékeny információk címkézésére vonatkozó TLP-protokoll. A minősített adatok cseréje tekintetében – az alkalmazott minősítési rendszertől függetlenül – a rendelkezésre álló akkreditált eszközök mellett a minősített adatok kezelésére vonatkozó meglévő kötelező szabályokat és megállapodásokat kell alkalmazni.

6. A fent említett irányadó elvekkel összhangban a tagállamoknak és az uniós szervezeteknek el kell mélyíteniük a kiberválságok kezelése terén folytatott együttműködésüket, előmozdítva a kölcsönös bizalmat, és építve a meglévő hálózatokra és mechanizmusokra. A kiberbiztonsági terv keretében folytatott ezen együttműködés során kihasználhatók az (EU, Euratom) 2023/2841 rendelet 22. és 23. cikkének végrehajtásából származó előnyök. Így az (EU, Euratom) 2023/2841 rendelet 23. cikke alapján létrehozott kiberbiztonsági válságkezelési terv hozzájárul például többek között a releváns információknak az uniós szervezetek közötti és a tagállamokkal való rendszeres cseréjéhez, és szabályokat határoz meg az uniós szervezetek közötti koordinációra és információáramlásra vonatkozóan.

II.: Fogalommeghatározások

7. E kiberbiztonsági terv alkalmazásában:

a) „esemény”: olyan esemény, amely veszélyezteti a hálózati és információs rendszereken tárolt, továbbított vagy kezelt adatok vagy az e rendszerek által kínált vagy azokon keresztül elérhető szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét vagy bizalmasságát;

b) „jelentős esemény”: olyan esemény, amely:

a. súlyos működési zavart okozott vagy okozhat a szolgáltatásokban, vagy pénzügyi veszteséget okozott vagy okozhat az érintett szervezetnek;

b. jelentős vagyoni vagy nem vagyoni kár okozásával más természetes vagy jogi személyeket érintett vagy érinthet;

c) „nagyszabású kiberbiztonsági esemény”: esemény, amely olyan mértékű zavart okoz, amely meghaladja az érintett tagállam reagálási képességét, vagy amely legalább két tagállamra jelentős hatást gyakorol;

d) „kiberválság”: nagyszabású kiberbiztonsági esemény, amely olyan teljes körű válsággá eszkalálódott, amely nem teszi lehetővé a belső piac megfelelő működését, illetve súlyos közrendi és közbiztonsági kockázatot jelent a szervezetekre vagy a polgárokra nézve több tagállamban vagy az Unió egészében.

III.: Nemzeti kiberbiztonsági válságkezelési struktúrák és felelősségi körök

8. Az őket érintő nagyszabású kiberbiztonsági események és kiberválságok elhárítása elsődlegesen a tagállamok felelőssége. Az (EU) 2022/2555 irányelvvel összhangban minden tagállam rendelkezik legalább egy kiberválságok kezelésével foglalkozó hatósággal, valamint legalább egy számítógép-biztonsági eseményekre reagáló csoporttal (CSIRT-tel).

9. A tagállamok azzal, hogy elfogadták az (EU) 2022/2555 irányelvet és elfogadtak más, a kiberbiztonságra vonatkozó jogalkotási és nem jogalkotási eszközöket is, összehangolták kiberbiztonsági kereteiket: minimumszabályokat határoztak meg a koordinált szabályozási keret működésére vonatkozóan, mechanizmusokat alakítottak ki az egyes tagállamok felelős hatóságai közötti hatékony együttműködésre, valamint az említett kötelezettségek tényleges érvényesítéséhez fontos hatékony jogorvoslatokról és végrehajtási intézkedésekről rendelkeztek.

10. Az (EU) 2022/2555 irányelv 9. cikkének (4) bekezdésével összhangban a tagállamoknak a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervet kell elfogadniuk. Ezek a tervek magukban foglalják többek között a nemzeti felkészültségi intézkedéseket, a kiberbiztonsági válságkezelési eljárásokat, valamint a nemzeti eljárásokat és megállapodásokat a nemzeti hatóságok és szervek vonatkozásában, hogy azok hatékonyan részt vehessenek a nagyszabású kiberbiztonsági események és kiberválságok uniós szintű összehangolt kezelésében, és elő tudják segíteni azt. A kiberválságok kezelésére szolgáló eljárásokat integrálni kell az általános nemzeti válságkezelési keretbe és az információcserére szolgáló csatornákba.

11. Az (EU) 2022/2555 irányelv 9. cikkének (1) bekezdésével összhangban a tagállamoknak biztosítaniuk kell a koherenciát a meglévő általános nemzeti válságkezelési keretekkel. Az IPCR aktiválása esetén a nemzeti válságkezelési hatóságoknak az IPCR tájékoztatása céljából információkat kell gyűjteniük a kiberválságok kezelésével foglalkozó hatóságoktól és a nemzeti ágazati válságelhárítási mechanizmusoktól.

12. Az (EU) 2022/2555 irányelv 9. cikkének (5) bekezdésével összhangban az EU-CyCLONe-nak – a bevált gyakorlatok cseréje és annak mérlegelése érdekében, hogy az átfogó keret a gyakorlatban is működne-e – valamely érintett tagállam kérésére meg kell osztania az információkat a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervek releváns részeiről, különösen a nagyszabású kiberbiztonsági események és kiberválságok uniós szintű összehangolt kezelésében való hatékony részvételt és annak támogatását biztosító rendelkezésekről.

13. A Tanács felkéri az EU-CyCLONe-t és az Intézményközi Kiberbiztonsági Testületet (a továbbiakban: IICB), hogy adott esetben foglalkozzanak az IICB által az (EU, Euratom) 2023/2841 rendelet 23. cikkével összhangban létrehozott válságkezelési terv és a nagyszabású kiberbiztonsági események és válságok elhárítására szolgáló nemzeti tervek közötti koherencia kérdésével.

14. Az EU-CyCLONe-nak – az ENISA titkárságként nyújtott támogatásával – az EU-CyCLONe tisztviselők és vezető tisztviselők elérhetőségét is tartalmazó naprakész jegyzéket kell vezetnie a kiberválságok kezelésével foglalkozó nemzeti hatóságokról, és azt az EU-CyCLONe tagjai rendelkezésére kell bocsátania.

IV.: Az uniós kiberbiztonsági válságkezelési ökoszisztéma fő hálózatai és szereplői

15. Az eseményekkel kapcsolatos releváns információk megosztására szolgáló fő technikai hálózat – különösen az ezen ajánlás hatálya alá tartozó területeken – a CSIRT-hálózat, az (EU) 2022/2555 irányelv 15. cikkének (3) bekezdésében foglalt vonatkozó feladatok értelmében. A hálózat hozzájárul a bizalom kialakulásához, és előmozdítja a tagállamok közötti gyors és hatékony operatív együttműködést. A CSIRT-hálózat elnöke megfigyelőként részt vehet az IICB-ben.

16. A CERT-EU valamennyi uniós szervezet kiberbiztonsági szolgálata. A CERT-EU az (EU) 2023/2841 rendelet 13. cikkével összhangban a kiberbiztonsági információcsere és az eseményekre való reagálás koordinációs központjaként működik. A CERT-EU tagja a CSIRT-hálózatnak is, és támogatja a Bizottságot az EU-CyCLONe-ban. A CERT-EU technikai szinten működik, és az uniós szervezeteket érintő súlyos biztonsági események kezelésének koordinálásáért felel.

17. Az EU-CyCLONe közvetítőként működik a technikai és a politikai szint között, különösen nagyszabású kiberbiztonsági események és kiberválságok idején. Támogatja a nagyszabású kiberbiztonsági események és kiberválságok operatív szintű összehangolt kezelését, és az (EU) 2022/2555 irányelv 16. cikkével összhangban biztosítja a releváns információk rendszeres cseréjét a tagállamok és az uniós intézmények, szervek, hivatalok és ügynökségek között. A EU-CyCLONe elnöke megfigyelőként részt vehet az IICB-ben.

18. Az ENISA az az uniós ügynökség, amely az (EU) 2019/881 rendelet[11] értelmében rá ruházott feladatokat látja el azzal a céllal, hogy Unió-szerte egységesen magas szintű kiberbiztonságot érjen el, többek között a tagállamok és az uniós intézmények, szervek és ügynökségek aktív támogatása révén. Az ENISA többek között titkárságot biztosít a CSIRT-hálózat és az EU-CyCLONe részére, helyzetismereti szolgáltatásokat nyújt, és uniós szintű kiberbiztonsági gyakorlatok rendszeres megszervezésével segíti a tagállamokat. Az (EU) 2022/2555 irányelvvel és az (EU) 2024/2847 rendelettel[12] összhangban az ENISA tájékoztatást kap a jelentős, határokon átnyúló eseményekről és a digitális termékek gyakran kihasznált sérülékenységeiről, valamint a digitális termékeket érintő eseményekről.

19. Az Európai Unió Tanácsa (a Tanács) az Európai Unióról szóló szerződés (a továbbiakban: az EUSZ) 16. cikke értelmében politikameghatározási és koordinatív feladatokat ellátó intézmény, és mint ilyen, az uniós politikai szintű koordinációt és válságelhárítást magában foglaló IPCRis az ő feladatkörébe tartozik. A Tanács a tanácsi formációk keretében, az Állandó Képviselők Bizottságában és az érintett tanácsi előkészítő szervekben, így különösen a kiberkérdésekkel foglalkozó horizontális munkacsoportban (HWPCI), valamint adott esetben az IPCR keretében jár el.

---

[11] 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.).

[12] Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., 1.o.).

20. Az Unió általános érdekeit előmozdító és e célból megfelelő kezdeményezéseket tevő, valamint a Szerződéseknek és az intézmények által az EUSZ 17. cikke alapján elfogadott intézkedéseknek az alkalmazását biztosító intézményként a Bizottság felel bizonyos általános uniós szintű felkészültségért és bizonyos helyzetismereti intézkedésekért, ideértve a Veszélyhelyzet-reagálási Koordinációs Központ (ERCC) és a közös veszélyhelyzeti kommunikációs és tájékoztatási rendszer (CECIS) irányítását, az uniós polgári védelmi mechanizmusról szóló határozattal összhangban. A Bizottság elősegíti a kapcsolódó uniós szintű válságelhárítási intézkedések közötti koherenciát és koordinációt operatív szinten. A Tanács konzultál a Bizottsággal az IPCR aktiválására, illetve alkalmazásának megszüntetésére vonatkozó döntésekről. A Bizottság szolgálatai az EKSZ-szel közösen kidolgozzák az integrált helyzetismereti és -elemzési jelentéseket. A Bizottság az EU-CyCLONe tagja azokban az esetekben, amikor egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági esemény jelentős hatást gyakorol vagy gyakorolhat az (EU) 2022/2555 irányelv hatálya alá tartozó szolgáltatásokra és tevékenységekre, más esetekben pedig megfigyelő. Emellett az IICB kapcsolattartó pontja az EU-CyCLONe felé. Megfigyelő a CSIRT-hálózatban.

21. Az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: főképviselő) irányítja az Unió közös kül- és biztonságpolitikáját (a továbbiakban: KKBP) az EKSZ támogatásával, és javaslatai révén hozzájárul e politika, valamint a közös biztonság- és védelempolitika (KBVP) alakításához. Ez diplomáciai, hírszerzési és katonai struktúrákat és mechanizmusokat foglal magában: ezek közé tartozik az egységes információelemzési kapacitás (SIAC), amely a tagállami hírszerzési információk egységes beviteli pontja, az Európai Unió Katonai Törzse (EUKT), amely a katonai szakértelem forrása, az uniós kiberdiplomáciai eszköztár, valamint az uniós küldöttségek hálózata, amely a külső dimenzió tekintetében járulhat hozzá a válságkezeléshez. Az EKSZ – a Bizottsággal közösen – elkészíti az integrált helyzetismereti és -elemzési jelentéseket.

22. A II. melléklet ismerteti az érintett uniós szintű szereplők – köztük a főbb hálózatok és szereplők – kiberbiztonsági válságkezeléssel kapcsolatos szerepét és hatásköreit.

V.: Felkészülés nagyszabású kiberbiztonsági eseményekre és kiberválságra

Fenyegetettségi helyzet

23. A tagállamoknak és az érintett uniós szervezeteknek meg kell tenniük a helyzetismeret javításához szükséges intézkedéseket, elismerve, hogy a fenyegetettségi helyzet és az eseményspecifikus helyzetismeret eltérő működési módokat igényel. A tagállamoknak és az érintett uniós szervezeteknek ellenőrzött és megbízható adatok – többek között az események, taktikák, technikák és eljárások tekintetében megfigyelhető trendek, valamint az aktívan kihasznált sérülékenységek – alapján kell együttműködniük.

24. Az adatok uniós szintű megosztása során a tagállamoknak teljes mértékben ki kell használniuk a technikai és operatív együttműködés meglévő platformjait, például a CSIRT-hálózat és az EU-CyCLONe által használt platformokat.

25. A közös helyzetismeret javítása és az EU által kifejtett hatás értékelésének megkönnyítése érdekében az EU-CyCLONe-nak és a CSIRT-hálózatnak – az ENISA támogatásával – belsőleg jóváhagyott jelentéstételi mechanizmust kell alkalmaznia, hogy a nemzeti szinten gyűjtött információk alapján uniós szintű áttekintést tudjon adni a technikai és operatív tevékenységekről.

26. Az EU-CyCLONe-nak és a CSIRT-hálózatnak:

a) együtt kell működnie a technikai és operatív szint, valamint a helyzetismeret egésze közötti információmegosztás javítása érdekében;

b) továbbra is munkálkodnia kell azon, hogy tagjai és a hálózatok körében bizalmi légkör alakuljon ki;

c) az ENISA támogatásával maradéktalanul ki kell használnia az információmegosztásra rendelkezésre álló eszközöket, és mérlegelnie kell, hogyan lehetne javítani ezeket az eszközöket és biztosítani a hálózatok közötti interoperabilitást.

27. A releváns információk hatékony cseréjének biztosítása érdekében az EU-CyCLONe-nak, a CSIRT-hálózatnak és az IICB-nek együtt kell működnie.

28. Az ENISA-nak mint a CSIRT-hálózat és az EU-CyCLONe titkárságának központi szerepe van abban, hogy támogassa a tagállamokat és az uniós intézményeket, szerveket és ügynökségeket abban, hogy technikai és operatív szinten közös uniós helyzetismeretet alakítsanak ki a nagyszabású kiberbiztonsági eseményekre és válságokra való felkészülés támogatása érdekében.

29. Az (EU) 2022/2555 irányelvvel és az (EU) 2019/881 rendelettel összhangban a tagállamoknak és az érintett uniós szervezeteknek az információmegosztás javítása érdekében koordinálniuk kell a magánszektorral, így többek között a nyílt forráskódú szoftvereket fejlesztő közösségekkel és gyártókkal is. Az ENISA-nak e tekintetben különösen ki kell használnia partnerségi programját. Emellett a kiberbiztonsági kapacitás növelése és a kiberbiztonsági eseményekre való reagálás érdekében a tagállamok és az érintett uniós szervezetek a meglévő uniós és nemzeti szintű információmegosztó és -elemző központokra (ISAC) is támaszkodhatnak, többek között azzal, hogy közös találkozókat szerveznek a magánszektor és az EU-CyCLONe vagy vagy a CSIRT-hálózat számára.

30. Annak érdekében, hogy javítani lehessen a hálózatokon belüli és a hálózatok közötti információmegosztást, valamint tisztázni lehessen az ilyen megosztással kapcsolatos kölcsönös elvárásokat, az EU-CyCLONe-nak – az ENISA mint titkárság támogatásával, valamint a CSIRT-hálózattal és a Kiberbiztonsági Együttműködési Csoporttal folytatott konzultációt követően – ezen ajánlás elfogadásától számított 24 hónapon belül meg kell állapodnia az események súlyossági szintjeinek közös, összehangolt taxonómiájáról. Ennek a taxonómiának lehetővé kell tennie a tagállamokban bekövetkezett események súlyosságának összehasonlítását, figyelemmel a szolgáltatásnyújtásra gyakorolt hatásra, az érintett szervezetek számára és relevanciájára, az egyéb szolgáltatásokat és infrastruktúrát érintő hatásokra, valamint az okozott monetáris, reputációs és politikai károkra. A rendszertannak a meglévő releváns skálákra vagy taxonómiákra, például az eseményosztályozási referenciataxonómiára kell épülnie.

Technikai szint

31. A CSIRT-hálózat az összes tagállam közötti és a CERT-EU-n keresztül az uniós szervezetekkel folytatott technikai együttműködés és információmegosztás platformja.

32. Az (EU) 2022/2555 irányelvvel összhangban a CSIRT-ek feladata a kiberfenyegetések, sérülékenységek és események nyomon követése és elemzése nemzeti szinten. A CSIRT-eknek a közös helyzetismeret elérése érdekében mind a CSIRT-hálózaton belül, mind kétoldalúan meg kell osztaniuk egymással az eseményekre, a majdnem bekövetkezett eseményekre, a kiberfenyegetésekre, a kockázatokra és a sérülékenységekre vonatkozó releváns információkat.

33. Az uniós szintű operatív együttműködés fokozása érdekében a CSIRT-hálózatnak fontolóra kell vennie, hogy felkérje a kiberbiztonsági szakpolitikában érintett uniós szerveket és ügynökségeket – például az Europolt – arra, hogy vegyenek részt a hálózat munkájában.

34. Az (EU) 2023/2841 rendelettel összhangban a CERT-EU-nak információkat kell gyűjtenie, kezelnie, elemeznie és megosztania az uniós intézményekkel, szervekkel, hivatalokkal és ügynökségekkel a nem minősített IKT-infrastruktúrát érintő kiberfenyegetésekről, sérülékenységekről és eseményekről, és szükség esetén konkrét, az uniós intézményeknek, szerveknek, hivataloknak és ügynökségeknek szóló iránymutatásokra és ajánlásokra vonatkozó javaslatokat kell tennie az IICB-nek. A CERT-EU-nak együtt kell működnie és információt kell cserélnie a tagállami partnerekkel, többek között a CSIRT-hálózaton keresztül.

Operatív szint

35. Az (EU) 2022/2555 irányelvvel összhangban az EU-CyCLONe-nak a tagállamok kiberválságok kezelésével foglalkozó hatóságai közötti, illetve a Bizottságon keresztül az érintett uniós szervezetekkel folytatott együttműködés platformjaként kell szolgálnia azzal a céllal, hogy növelje a nagyszabású kiberbiztonsági események és kiberválságok kezelésére való felkészültség szintjét, és közös helyzetismeretet alakítson ki a nagyszabású kiberbiztonsági események és kiberválságok tekintetében.

36. Az (EU) 2022/2555 irányelvvel és az (EU) 2024/2847 rendelettel összhangban az ENISA tájékoztatást kap a jelentős, határokon átnyúló eseményekről és a digitális termékek gyakran kihasznált sérülékenységeiről, valamint a digitális termékeket érintő eseményekről. A titkárságként eljáró ENISA-nak tanácsot kell adnia a CSIRT-hálózat és az EU-CyCLONe számára azzal a céllal, hogy egyrészről támogassa a hálózatokat annak meghatározásában, hogy szükség van-e további intézkedésekre, másrészről pedig hozzájáruljon a közös helyzetismerethez.

Politikai szint

37. A tagállamoknak és az érintett uniós szervezeteknek nyomon kell követniük a kiberbiztonságot érintő nemzetközi fejleményeket (így többek között a kiberfenyegetéseket, a hibrid fenyegetéseket, valamint a külföldi információmanipulációt és beavatkozást, ideértve adott esetben a dezinformációt is). Figyelembe kell venni az olyan kezdeményezéseket, mint a közös kiberbiztonsági értékelő jelentés (JCAR), a SIAC által készített elemzéseket és a speciális betekintést nyújtó egyéb releváns termékeket.

38. A főképviselőnek továbbra is tájékoztatnia kell a tagállamokat úgy a kiberfenyegetésekkel kapcsolatos, különösen az állami szereplőket érintő uniós diplomáciai erőfeszítésekről, mint a harmadik országokkal és a nemzetközi szervezetekkel – többek között a NATO-val – folytatott együttműködéséről, továbbá a diplomáciai intézkedések, többek között a korlátozó intézkedések végrehajtásáról, illetve be kell vonnia a tagállamokat mindezekbe.

39. Az Európai Unió Tanácsának elnöksége az IPCR internetes platformján nyomonkövetési oldalt kezdeményezhet, ahol a tagállamok, valamint az uniós intézmények és szervek információt cserélhetnek egy esetlegesen kialakuló válságról.

Közös gyakorlatok

40. A Bizottságnak a főképviselővel együttműködve és az ENISA támogatásával – az EU-CyCLONe-nal és a CSIRT-hálózattal folytatott konzultációt követően – kiberbiztonsági gyakorlatokból álló hatékony éves gördülő programot kell összeállítania, amely a kiberválságokra való felkészülést és a szervezeti hatékonyság növelését szolgálja. A kiberbiztonsági gyakorlatokból álló gördülő programnak figyelembe kell vennie az uniós polgári védelmi mechanizmus és az uniós szintű egyéb válságelhárítási mechanizmusok gyakorlatait, ideértve a kritikus infrastruktúrákra vonatkozó uniós tervben vázolt gyakorlatot is. Az első gördülő programot a kiberbiztonsági terv elfogadását követő 12 hónapon belül, a későbbi programokat pedig minden év március 31-ig ki kell kidolgozni. A gördülő programot tájékoztatás céljából be kell nyújtani a Tanácsnak.

41. A gördülő programnak ki kell terjednie az összehangolt uniós kockázatértékelési forgatókönyvek felhasználásával kidolgozott gyakorlatokra is. Emellett ki kell terjednie az összes érintett szereplőt, különösen a magánszektort és a NATO-t bevonó gyakorlatokra is.

42. A CSIRT-hálózat és az EU-CyCLONe titkárságaként az ENISA feladata szisztematikusan összegyűjteni a gyakorlatokból levont tanulságokat, azonosítani, hogy a tanulságok alapján milyen intézkedésekre van szükség, valamint javaslatokat tenni arra, hogyan lehet ezeket az intézkedéseket végrehajtani, mindezt azzal a céllal, hogy biztosítani lehessen a hatékony végrehajtásukat és az EU közös rezilienciájára, így többek között a vonatkozó eljárási standardokra gyakorolt pozitív hatásukat.

43. A gyakorlatokból levont tanulságok alapján valamennyi szereplőnek és hálózatnak javítania kell a nagyszabású kiberbiztonsági események vagy kiberválságok esetén folytatandó koordinációt. Különösen az EU-CyCLONe-nak és a CSIRT-hálózatnak választ kell adnia a koordináció javítását célzó gyakorlatok során azonosított kihívásokra, kiváltképp a hálózatok közötti együttműködéssel kapcsolatos kihívásokra, és szükség esetén gyors ütemben ki kell igazítania az eljárási standardokat.

44. A Kiberbiztonsági Együttműködési Csoportnak fel kell kérnie a CSIRT-hálózatot, az EU-CyCLONe-t és az ENISA-t, hogy ismertessék egyrészről a gyakorlatokból levont tanulságokat, másrészről azt, hogy a tanulságok alapján milyen intézkedésekre van szükség, harmadrészről pedig arra vonatkozó javaslataikat, hogyan lehet ezeket az intézkedéseket végrehajtani.

45. A Tanács felkérheti a CSIRT-hálózat elnökét, az EU-CyCLONe elnökét, a Kiberbiztonsági Együttműködési Csoport elnökét és az ENISA elnökét, hogy ismertessék, hogyan ültették át intézkedésekbe a gyakorlatokból levont tanulságokat.

46. Az ENISA felkérést kap arra, hogy a Bizottsággal és a főképviselővel együttműködve szervezzen gyakorlatot a kiberbiztonsági tervnek a következő Cyber Europe gyakorlat során való tesztelésére. A gyakorlatba valamennyi érintett szereplőt be kell vonni, ideértve a politikai szintet is. Az ENISA felkérést kap, hogy a politikai szint bevonása tekintetében folytasson koordinációt az Európai Unió Tanácsának elnökségével. A gyakorlat kiterjedhet a magánszektorra és a NATO-ra is.

VI. Olyan esemény észlelése, amely nagyszabású kiberbiztonsági eseménnyé vagy kiberválsággá eszkalálódhat

47. Minden szereplőnek – saját megbízatásával összhangban és az összes veszélyre kiterjedő megközelítés alapján – meg kell osztania a potenciális nagyszabású kiberbiztonsági eseményre vagy a potenciális kiberválságra utaló információkat az érintett hálózatokkal.

48. Összhangban az (EU) 2025/38 rendelettel[13], amennyiben a határokon átnyúló kiberközpontok információkhoz jutnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről, a közös helyzetismeret céljából biztosítaniuk kell, hogy a releváns információkat az EU-CyCLONe-n és a CSIRT-hálózaton keresztül indokolatlan késedelem nélkül eljuttassák a tagállami hatóságoknak és a Bizottságnak.

[13] Az Európai Parlament és a Tanács (EU) 2025/38 rendelete (2024. december 19.) a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és képességek megerősítését célzó intézkedések meghatározásáról, és az (EU) 2021/694 rendelet módosításáról (a kiberszolidaritásról szóló rendelet) (HL L, 2025/38, 2025.1.15., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

49. Jelentős esemény megfigyelése esetén, különösen, ha az azonnali hatást vált ki, az eseményt bejelenthetik egy CSIRT-nek, vagy azt észlelhetik maguk a CSIRT-ek, a tagállamok kiberválságok kezelésével foglalkozó hatóságai vagy más ágazati hatóságok. A tagállamokat arra ösztönözzük, hogy osszák meg az ilyen eseményekkel kapcsolatos információkat azon hálózatokon belül, amelyeknek fontolóra kell venniük a megfelelő intézkedések meghozatalát. A CSIRT-hálózat és az EU-CyCLONe – az esemény jellegétől és a szükséges reagálástól függően – egymástól függetlenül is aktiválható. Ugyanakkor mindkét hálózatot arra ösztönözzük, hogy folytassák együttműködésüket az elfogadott eljárási szabályok alapján. Az aktiválásra vonatkozó döntést kizárólag és független módon az egyes hálózatok hozhatják meg.

50. A CSIRT-hálózatnak tanácsot kell adnia az EU-CyCLONe-nak azzal kapcsolatban, hogy egy észlelt kiberbiztonsági esemény potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseménynek tekinthető-e.

51. A CSIRT-hálózatnak és az EU-CyCLONe-nak – az (EU) 2022/2555 irányelvben foglaltak szerint – késedelem nélkül meg kell állapodnia a potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági események esetére vonatkozó eljárási szabályokról, hogy biztosított legyen a technikai-operatív szintű koordináció, valamint a politikai szint számára időszerű és releváns információk álljanak rendelkezésre.

VII. Uniós szintű reagálás nagyszabású kiberbiztonsági eseményekre vagy kiberválságokra

Reagálás olyan nagyszabású kiberbiztonsági eseményekre vagy olyan kiberválságokra, amelyek esetében az IPCR-t nem aktiválják teljes körűen

52. A nagyszabású kiberbiztonsági eseményekre vagy a kiberválságokra való uniós szintű reagálás hatékonysága az összkormányzati megközelítés keretében folytatott technikai, operatív és politikai együttműködés hatékonyságán múlik, ideértve adott esetben a bűnüldözést is.

53. A közös helyzetismeret és az összehangolt reagálás biztosítása érdekében az érintett szereplőknek az egyes szinteken meghatározott tevékenységeket kell végezniük. Ezeknek az intézkedéseknek biztosítaniuk kell az információk szabályos és hatékony terjesztését.

54. A reagálást a nagyszabású kiberbiztonsági esemény vagy a kiberválság hatásához kell igazítani. A tagállamok kiberválságok kezelésével foglalkozó hatóságainak – az (EU) 2022/2555 irányelvvel összhangban – biztosítaniuk kell, hogy a kiberválságra adott ágazati reagálás nemzeti szinten koherens és koordinált legyen.

55. Nagyszabású kiberbiztonsági esemény vagy kiberválság esetén az összes szereplő és hálózat reagálását szorosan koordinálni kell az alábbiak szerint:

a) technikai szinten:

i. az érintett tagállamoknak és az azokban működő CSIRT-eknek együtt kell működniük az érintett szervezetekkel az eseményekre való reagálás és adott esetben a segítségnyújtás érdekében;

ii. a CSIRT-eknek együtt kell működniük a CSIRT-hálózaton keresztül annak érdekében, hogy megosszák egymással az eseményre vonatkozó releváns technikai információkat; a CSIRT-ek – az ok és a lehetséges technikai mérséklési intézkedések meghatározása céljából – együttműködnek azon erőfeszítéseik keretében, amelyek az eseményhez kapcsolódó, rendelkezésre álló technikai adatok és egyéb technikai információk elemzésére irányulnak;

iii. ha a CSIRT-ek vagy a tagállamok kiberválságok kezelésével foglalkozó hatóságai tudomást szereznek egy jelentős eseményről, ösztönözni kell, hogy ezt az információt megosszák a CSIRT-hálózaton vagy az EU-CyCLONe-on belül;

iv. a CSIRT-hálózatnak – az ENISA támogatásával – a CSIRT-ek által benyújtott nemzeti jelentésekből összesítést kell készítenie, és azt be kell nyújtania az EU-CyCLONe-nak;

v. amennyiben egy kiberbiztonsági esemény potenciálisan nagyszabású kiberbiztonsági eseménnyé vagy kiberválsággá eszkalálódhat, a CSIRT-hálózatnak meg kell osztania a megfelelő információkat az EU-CyCLONe-nal. Az EU-CyCLONe-nak ezen információk felhasználásával tájékoztatnia kell a Tanácsot;

vi. a CSIRT-hálózatnak – a releváns technikai információk cseréjének biztosítása érdekében – szoros kapcsolatban kell állnia az Europollal. A CSIRT-hálózatnak és az Europolnak kapcsolattartó pontokat kell létrehoznia annak érdekében, hogy nagyszabású kiberbiztonsági események esetén – adott esetben – fokozzák az információmegosztást;

b) operatív szinten:

i. a tagállamoknak megfelelő intézkedésekkel mérsékelniük kell az esemény nemzeti szintű hatását;

ii. a CSIRT-hálózatnak az EU-CyCLONe rendelkezésére kell bocsátania a folyamatban lévő események technikai értékelését, amelyet az EU-CyCLONe felhasználhat;

iii. az EU-CyCLONe-nak értékelnie kell a releváns nagyszabású kiberbiztonsági események és a releváns kiberválságok következményeit és hatását, javaslatot kell tennie a lehetséges mérséklési intézkedésekre, elő kell segítenie a nagyszabású kiberbiztonsági események és a kiberválságok koordinált kezelését, valamint elő kell mozdítania a politikai szintű döntéshozatalt;

iv. amennyiben egy több ágazatra is kiterjedő hatással járó, nagyszabású kiberbiztonsági esemény szükségessé teszi az uniós szintű reagálási intézkedések, különösen a II. mellékletben felsorolt releváns uniós szintű horizontális és ágazati válságkezelési mechanizmusok aktiválását,

a) a megfelelő szereplők – az uniós szintű ágazati válságkezelési mechanizmusok típusától függően – kérhetik, hogy aktiválják az említett mechanizmust;

b) az említett ágazati mechanizmus aktiválása esetén az érintett szervezetek támogatják az ágazati szervezeteket az esemény hatásának mérséklésében;

c) a Bizottságnak meg kell könnyítenie a szükséges információk áramlását a II. mellékletben felsorolt releváns horizontális és ágazati szintű uniós válságkezelési mechanizmusok és az EU-CyCLONe kapcsolattartó pontjai között, és több ágazatot átfogó, integrált elemzést kell végeznie, valamint javaslatot kell tennie a megfelelő integrált reagálási tervre vonatkozóan;

d) a Bizottságnak – az EU-CyCLONe-on keresztül és adott esetben a főképviselővel együttműködve – biztosítania kell a kiberterületre vonatkozó uniós szintű operatív intézkedések és a kapcsolódó uniós szintű reagálási intézkedések közötti koherenciát és koordinációt, különösen az UCPM-en keresztüli segítségnyújtás kérelmezésével kapcsolatban;

e) amennyiben az IPCR internetes platformján nyomonkövetési weboldalt nyitottak, azon keresztül a tagállamokkal és az uniós szervezetekkel is meg kell osztani az eseménnyel kapcsolatos információkat, az esemény hatásait, valamint a meghozott intézkedéseket;

v. a tagállamok az (EU) 2025/38 rendelet 15. cikkével összhangban szolgáltatásokat kérhetnek az uniós kiberbiztonsági tartalékból. Az említett rendelet szerinti jövőbeli végrehajtási jogi aktusok sérelme nélkül, az uniós kiberbiztonsági tartalék szolgáltatásainak igénybevételét a kéréstől számított 24 órán belül biztosítani kell;

c) politikai szinten:

i. a Tanács – a megfelelő politikai és stratégiai reagálás érdekében – tájékoztatást kérhet a legfontosabb érdekelt felektől, különösen a Bizottságtól, a főképviselőtől és az EU-CyCLONe-tól;

ii. a Tanács – a Bizottság és a főképviselő támogatásával – megfelelő intézkedéseket határozhat meg a nagyszabású kiberbiztonsági eseményre való reagálás érdekében, ideértve a IX. fejezet szerinti lehetséges diplomáciai intézkedéseket is;

iii. a tagállamok – az esemény jellegétől és hatásától függően – további kiberbiztonsági válságkezelési mechanizmusokat vagy eszközöket aktiválhatnak;

iv. ha az IPCR-t információmegosztási módban aktiválják, működésbe lép az integrált helyzetismeret és elemzés támogatási képessége, ami fokozza az IPCR internetes platformján keresztül zajló információcserét, és biztosítja a közös helyzetértékelést. Továbbra is az EU-CyCLONe és a CSIRT-hálózat helyzetjelentéseinek kell azon fő eszközöknek lenniük, amelyek áttekintést adnak az operatív, illetve a technikai szintre vonatkozó közös helyzetismeretről. Ezeket a jelentéseket be lehet építeni az integrált helyzetismereti és -elemzési jelentésekbe;

v. olyan esemény esetén, amely szükségessé teszi az uniós szintű reagálási intézkedések – különösen a II. mellékletben felsorolt releváns uniós szintű horizontális és ágazati válságkezelési mechanizmusok – aktiválását, a Tanácsnak a Bizottsággal és a főképviselővel együttműködve biztosítania kell a kiberválságra való reagálás és a kapcsolódó uniós szintű reagálási intézkedések közötti koherenciát és koordinációt;

vi. releváns mechanizmusok, mindenekelőtt a kiberbiztonsági tartalék szolgáltatásainak kérelmezése esetén a Bizottság szolgálatainak és adott esetben az EKSZ-nek, valamint az érintett tanácsi szerveknek – nevezetesen a HWPCI-nek és adott esetben a reziliencia megerősítésével és a hibrid fenyegetésekkel szembeni fellépéssel foglalkozó horizontális munkacsoportnak (HWP-ERCHT) koordinálniuk kell az intézkedések kialakítása és végrehajtása, valamint a további intézkedéseket eredményező megfelelő döntéshozatali folyamat tekintetében, a szélesebb körű hibrid hadjárat részét képező rossz szándékú kibertevékenységek esetében összhangban a hibrid eszköztárral[14].

Reagálás olyan nagyszabású kiberbiztonsági eseményekre vagy olyan kiberválságokra, amelyek esetében az IPCR-t teljes körűen aktiválják

56. A fenti, *„Reagálás olyan nagyszabású kiberbiztonsági eseményekre vagy kiberválságokra, amelyek esetében az IPCR-t nem aktiválják teljes körűen”* címet viselő szakaszban felsorolt lépéseket végre kell hajtani.

57. Amikor az IPCR-t teljes körűen aktiválják, az integrált helyzetismereti és -elemzési jelentések célja, hogy biztosítsák politikai szinten a közös helyzetismeretet. Továbbra is az EU-CyCLONe és a CSIRT-hálózat helyzetjelentéseinek kell azon fő eszközöknek lenniük, amelyek áttekintést adnak az operatív, illetve a technikai szintre vonatkozó közös helyzetismeretről. Ezeket a jelentéseket be lehet építeni az integrált helyzetismereti és -elemzési jelentésekbe.

58. Olyan nagyszabású kiberbiztonsági esemény vagy olyan kiberválság esetén, amely az ICPR-t teljes körű aktiválását eredményezi, az összes szereplőnek szoros koordináció mellett, összkormányzati megközelítés keretében kell reagálnia az alábbiak szerint:

a) a reagálás uniós politikai szintű koordinációját a Tanács végzi az IPCR-mechanizmus felhasználásával;

---

14 A hibrid eszköztár az EU-t és tagállamait érintő hibrid hadjáratokra való koordinált reagálás kerete, amely például megelőző, együttműködési, stabilitási, korlátozó és helyreállítási intézkedéseket foglal magában, valamint támogatja a szolidaritást és a kölcsönös segítségnyújtást.

b) az EU-CyCLONe-nak a CSIRT-hálózattal együttműködve egyértelmű tájékoztatást kell nyújtania a politikai szint számára az esemény hatásáról, lehetséges következményeiről, valamint a reagálási és helyreállítási intézkedésekről, többek között azáltal, hogy hozzájárul az integrált helyzetismereti és -elemzési jelentéshez;

c) az integrált helyzetismereti és -elemzési képesség kiegészítéseként az Európai Unió Tanácsának elnöksége IPCR-kerekasztal-megbeszéléseket hívhat össze, hogy lehetővé tegye az uniós reagálásnak a kiberbiztonsági terv szerinti intézkedésekkel és az IPCR munkájához hozzájáruló érintett ágazati mechanizmusok munkájával való politikai és stratégiai összehangolását. Az IPCR-en belüli politikai és stratégiai koordináció elősegítése céljából a kerekasztal-megbeszélések során azonosítani lehet továbbá néhány konkrét hiányosságot a reagálás terén, meghatározott uniós szereplők pedig felkérését kaphatnak ezek kezelésére, valamint az erről való beszámolásra az elkövetkező kerekasztal-megbeszélések alkalmával;

d) az Európai Unió Tanácsa elnökségének fontolóra kell vennie, hogy meghívja az EU-CyCLONe-t releváns ülésekre, többek között az IPCR-mechanizmus keretében tartott kerekasztal-megbeszélésekre és a Tanács egyéb releváns üléseire;

e) a tagállamok válságkezelési hatóságainak – a kiberválságok kezelésével foglalkozó hatóságok támogatásával – biztosítaniuk kell, hogy a kiberválságra adott ágazati reagálás koherens és koordinált legyen;

f) a lehetséges diplomáciai intézkedéseket a IX. fejezettel összhangban kell megvizsgálni és végrehajtani.

VIII. A nyilvános kommunikációra irányuló erőfeszítések

59. Amellett, hogy valamely tagállam lakosságának egy folyamatban lévő nagyszabású kiberbiztonsági eseményről vagy kiberválságról való tájékoztatása – többek között a figyelemfelhívás részeként – nemzeti hatáskörbe tartozik, a tagállamoknak, a Bizottságnak és a főképviselőnek törekedniük kell arra, hogy a lehető legnagyobb mértékben összehangolják nyilvános kommunikációjukat. Adott esetben az IPCR válsághelyzeti kommunikátorok hálózata is bevonható.

60. A nagyszabású kiberbiztonsági eseményekre és a kiberválságokra való felkészülés céljából a tagállamok, valamint adott esetben a Bizottság és a CERT-EU felkérést kapnak arra, hogy folytassanak információcserét arról, milyen kommunikációs erőfeszítéseket tesznek az EU-CyCLONe keretében és a CSIRT-hálózaton belül, ideértve a bevált gyakorlatokat, például a figyelmeztetéseket vagy a figyelemfelkeltő kampányokat is. Az ENISA-nak eszközöket kell biztosítania az említett információcsere támogatásához és a könnyű hozzáférés lehetővé tételéhez.

61. Felkérjük a tagállamokat, hogy nagyszabású kiberbiztonsági esemény vagy kiberválság esetén – a közös tudatosság kiépítése és az intézkedések összehangolása érdekében – az EU-CyCLONe keretében osszanak meg információkat a nyilvános kommunikációra irányuló erőfeszítéseikről. Az EU-CyCLONe – saját kezdeményezésére vagy a Tanács kérésére – áttekintést adhat a Tanácsnak e megközelítésekről.

IX. Diplomáciai intézkedések és együttműködés stratégiai partnerekkel

62. A főképviselőnek a Bizottsággal és más érintett uniós szervezetekkel szoros együttműködésben:

    a) többek között elemzések, jelentések és javaslatok révén elő kell segítenie a tanácsi döntéshozatalt az uniós kiberdiplomáciai eszköztár részét képező lehetséges intézkedések alkalmazásával kapcsolatban. Ez lehetővé fogja tenni a rossz szándékú kibertevékenységek megelőzésére, az ilyen tevékenységektől való elrettentésre és az azokra való reagálásra rendelkezésre álló uniós eszközök teljes spektrumának felhasználását, megerősítve az Unió kiberbiztonsági pozícióját, valamint előmozdítva a nemzetközi békét, biztonságot és stabilitást a kibertérben;

b) releváns esemény azonosítása esetén elő kell segítenie a szükséges információk megosztását a stratégiai partnerekkel, többek között – adott esetben – a NATO-val;

c) fokoznia kell a stratégiai partnerekkel, többek között – adott esetben – a NATO-val való koordinációt a fenyegetést jelentő szereplők által folytatott, tartósan rossz szándékú kibertevékenységekre való reagálás terén, különösen az uniós kiberdiplomáciai eszköztár használata során, a végrehajtási iránymutatásokkal összhangban.

63. A tagállamoknak, a főképviselőnek, a Bizottságnak és más érintett uniós szervezeteknek együtt kell működniük a stratégiai partnerekkel és nemzetközi szervezetekkel a bevált gyakorlatok és a kibertérben tanúsított felelős állami magatartás előmozdítása, valamint a potenciális vagy nagyszabású kiberbiztonsági eseményekre való gyors és összehangolt reagálás biztosítása érdekében.

64. Az Európai Unió és a NATO közötti együttműködésnek az inkluzivitásra, a viszonosságra és az átláthatóságra vonatkozóan elfogadott vezérelvekkel összhangban és az Unió autonóm döntéshozatalának teljes körű tiszteletben tartása mellett kell megvalósulnia.

65. A Bizottságnak és a főképviselőnek – figyelembe véve a meglévő megállapodásokat, például a CERT-EU és a NATO közötti, 2016. évi technikai megállapodást – kiberválság esetén kapcsolattartó pontokat kell létrehoznia a NATO-val való koordináció céljából, hogy a reagálással kapcsolatos együttműködés és a reagálás fokozása érdekében megoszthassák egymással a helyzettel és a válságelhárítási mechanizmusok alkalmazásával kapcsolatos szükséges információkat. E célból az Uniónak meg kell vizsgálnia, hogy milyen módokon javítható a NATO-val való információmegosztás inkluzív, kölcsönös és megkülönböztetésmentes módon, különösen a biztonságos kommunikáció eszközeinek biztosítása révén, figyelembe véve ugyanakkor a különböző tagállamok információmegosztási normáit.

66. A fenti V. fejezetben említett, uniós kiberbiztonsági gyakorlatokból álló gördülő program részeként a Bizottság szolgálatainak és az EKSZ-nek fontolóra kell venniük, hogy személyzeti szinten gyakorlatot szervezzenek a NATO-val annak érdekében, hogy teszteljék a polgári és katonai szervezetek együttműködését olyan nagyszabású kiberbiztonsági események vagy olyan kiberválságok esetén, amikor a tagállamok vagy a NATO-szövetségesek célja a biztonságukat érintő kibertámadásokra való reagálás. A gyakorlatot inkluzív és megkülönböztetésmentes módon, valamint az EU–NATO együttműködés paramétereire vonatkozóan elfogadott elvek teljes körű tiszteletben tartása mellett kell megtartani. A gyakorlatot az „EU Integrated Resolve" gyakorlat (párhuzamos és koordinált gyakorlat, a továbbiakban: PACE) keretében kell lebonyolítani. Minden szükséges intézkedést meg kell tenni annak biztosítása érdekében, hogy a kiberbiztonsági tervben említett minden szereplő részt vegyen a gyakorlatban.

67. A Tanáccsal, a Bizottsággal és a főképviselővel konzultálva fontolóra kell venni olyan közös, uniós szintű kiberbiztonsági gyakorlatok megtartását is, amelyekben a nyugat-balkáni országok, a Moldovai Köztársaság, Ukrajna, valamint más stratégiai partnerek és hasonlóan gondolkodó harmadik országok is részt vesznek.

X. A kiberbiztonsági válságkezelés koordinálása katonai szereplőkkel uniós szinten

68. A tagállamoknak tovább kell erősíteniük a polgári és katonai kiberszereplők közötti, nemzeti szintű együttműködést.

69. A közös katonai és polgári perspektíva kiaknázásának érdekében az EU-CyCLONe-nak és a CSIRT-hálózatnak – elsősorban együttes ülések révén – meg kell határoznia az érintett uniós katonai szereplőkkel, például az uniós kibervédelmi parancsnokok konferenciájával és a katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok operatív hálózatával (MICNET) való együttműködés lehetséges módjait és eljárásait. Az EU-CyCLONe-nak és a CSIRT-hálózatnak tájékoztatnia kell a Tanácsot az említett együttműködés tekintetében elért eredményekről.

70. Az érintett tagállam felkérést kap, hogy tájékoztassa az EU-CyCLONe-t és az EKSZ-t, amennyiben egy nagyszabású kiberbiztonsági eseménnyel vagy egy válsággal összefüggésben releváns nemzeti vagy multinacionális katonai reagálási képességeket vesznek igénybe, és e tájékoztatásról az említett reagálási képességet igénybe vevő és biztosító fél közösen megállapodott.

71. A fenti V. fejezetben említett, uniós kiberbiztonsági gyakorlatokból álló gördülő program részeként a Bizottságnak és a főképviselőnek fontolóra kell venniük, hogy közös gyakorlatot szervezzenek annak érdekében, hogy teszteljék a polgári és katonai kiberszereplők együttműködését egy tagállamokat érintő nagyszabású kiberbiztonsági esemény esetén.

XI. Helyreállítás és a kiberválságból levont tanulságok

72. A tagállamoknak, valamint az érintett uniós szervezeteknek és hálózatoknak együtt kell működniük a kiberválságot követő helyreállítási szakaszban, hogy biztosítsák az alapvető funkciók gyors helyreállítását. Ebbe az együttműködésbe adott esetben a bűnüldöző területet is be kell vonni. Ebben a szakaszban döntő fontosságú a magánszektorral való együttműködés, különösen az adatvisszaállítás és a rendszerek helyreállításának elősegítése terén. Az érdekelt felek közötti hatékony koordináció keretében prioritásként kell kezelni a zavarok minimalizálását, valamint azt, hogy biztosított legyen az üzletmenet-folytonosság.

73. A tagállamoknak, valamint az érintett uniós szervezeteknek és hálózatoknak együtt kell működniük a helyreállítási szakaszban, a múltbéli kiberválságokból vagy kezelt kiberbiztonsági eseményekből levont tanulságokra, valamint az eseményekről szóló jelentésekre építve, különösen az (EU) 2025/38 rendelettel létrehozott, európai kiberbiztonsági események felülvizsgálati mechanizmusával összefüggésben.

74. Az EU-CyCLONe-nak átfogó jegyzéket kell a CSIRT-hálózat, a Kiberbiztonsági Együttműködési Csoport és a Tanács rendelkezésére bocsátania a kiberválságokból vagy a kezelt kiberbiztonsági eseményekből levont tanulságokról és a bevált gyakorlatokról. Az ENISA-nak gondoskodnia kell arról, hogy az említett tanulságokat megfelelően figyelembe vegyék a jövőbeli felkészültségi tevékenységekben, valamint a jövőbeli gyakorlatok tervezésekor.

XII. Biztonságos kommunikáció

75. A meglévő biztonságos kommunikációs eszközök feltérképezése[15] alapján a Bizottságnak 2026 végéig javaslatot kell tennie interoperábilis biztonságos kommunikációs megoldásokra. A Tanácsnak, a Bizottságnak, a főképviselőnek, az EU-CyCLONe-nak és a CSIRT-hálózatnak 2027 végéig meg kell állapodnia ezekről. Ezeknek a megoldásoknak támaszkodniuk kell az uniós intézmények által az EU felkészültségi unióról szóló stratégiája keretében a biztonságos kommunikáció területén hozható intézkedésekre, valamint ki kell terjedniük a szükséges kommunikációs módok teljes körére (hang, adat, videokonferencia, üzenetküldés, együttműködés, valamint dokumentummegosztás és -konzultáció). A megoldásoknak meg kell felelniük a nem minősített érzékeny adatok védelmére vonatkozó, közösen meghatározott követelményeknek. Olyan, nyílt protokollon alapuló megoldásokat kell használni, amelyek a valós idejű kommunikáció céljára alkalmas, nyílt forráskódú alkalmazásokat tartalmaznak, és amelyeket az Unióban letelepedett szervezet kezel.

76. Az EU-CyCLONe-nak és a CSIRT-hálózatnak szükség esetén, a RESTREINT UE/EU RESTRICTED minősítésű adatok cseréje céljából képesnek kell lenniük arra, hogy az uniós intézmények, szervek és ügynökségek számára biztosított biztonságos kommunikációs csatornákat vegyenek igénybe a minősített adatok egymás közötti és a tagállamokkal való cseréjéhez.

[15] WK 862/2023.

77. Az (EU) 2021/887 rendelettel[16] létrehozott Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak (ECCC) – a jövőbeli többéves pénzügyi keret sérelme nélkül – fontolóra kell vennie a Digitális Európa programon keresztüli finanszírozást, hogy ezzel segítse a tagállamokat a biztonságos kommunikációs eszközök bevezetésében. El kell kerülni az interoperábilis biztonságos rendszerekbe történő párhuzamos beruházásokat.

78. Az uniós szervezeteknek és a tagállamoknak különösen olyan súlyos válságok esetére kell vészhelyzeti terveket kidolgozniuk, amikor az internetre vagy távközlési hálózatokra támaszkodó szokásos kommunikációs csatornákon zavar keletkezik vagy e csatornák nem állnak rendelkezésre.

79. A kiberválságokra való hatékony reagálás érdekében kommunikációs és információmegosztási mechanizmusokat kell létrehozni a bűnüldöző és a kiberbiztonsági hálózatok között, különösen technikai szinten. Ezeknek a mechanizmusoknak tiszteletben kell tartaniuk az egyes felek szerepét, és el kell kerülniük a folyamatban lévő műveletekbe való beavatkozást, valamint biztosítaniuk kell az összeköttetések redundanciáját. A jelenleg fejlesztés alatt álló európai kritikus kommunikációs rendszer (EUCCS) előnyös lehet az érintett kiberközösségekkel való közös reagálás szempontjából.

XIII. Záró rendelkezések

80. Az EU-CyCLONe-nak – a CSIRT-hálózattal és az uniós kiberbiztonsági válságkezelési ökoszisztéma más főbb szereplőivel együttműködve, valamint az ENISA támogatásával – az ajánlás közzétételét követő egy éven belül részletes folyamatábrákat kell kidolgoznia, amelyekben felvázolja az érintett szereplők közötti információáramlást, a döntéshozatali folyamatokat és az ezen ajánlás szerinti nagyszabású kiberbiztonsági események vagy kiberválságok kezelése során elkészített jelentéseket. A folyamatábráknak ki kell terjedniük a különböző együttműködési módokra és rétegekre. A folyamatábrákat szükség esetén naprakésszé kell tenni.

---

[16] 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.).

81. A Tanács szükség esetén – a felülvizsgált kiberbiztonsági terv hatékony alkalmazásának támogatása érdekében, valamint az annak megfelelően végzett közös kiberbiztonsági gyakorlatok során szerzett tapasztalatokra építve – végrehajtási iránymutatásokat dolgozhat ki. Ezekben az iránymutatásokban ki lehet térni a gyakorlatok során azonosított gyakorlati kihívások felszámolására, valamint a koordináció, a kommunikáció és az operatív interakció terén feltárt hiányosságok és hiányzó kapcsolatok orvoslására, illetve pótlására.

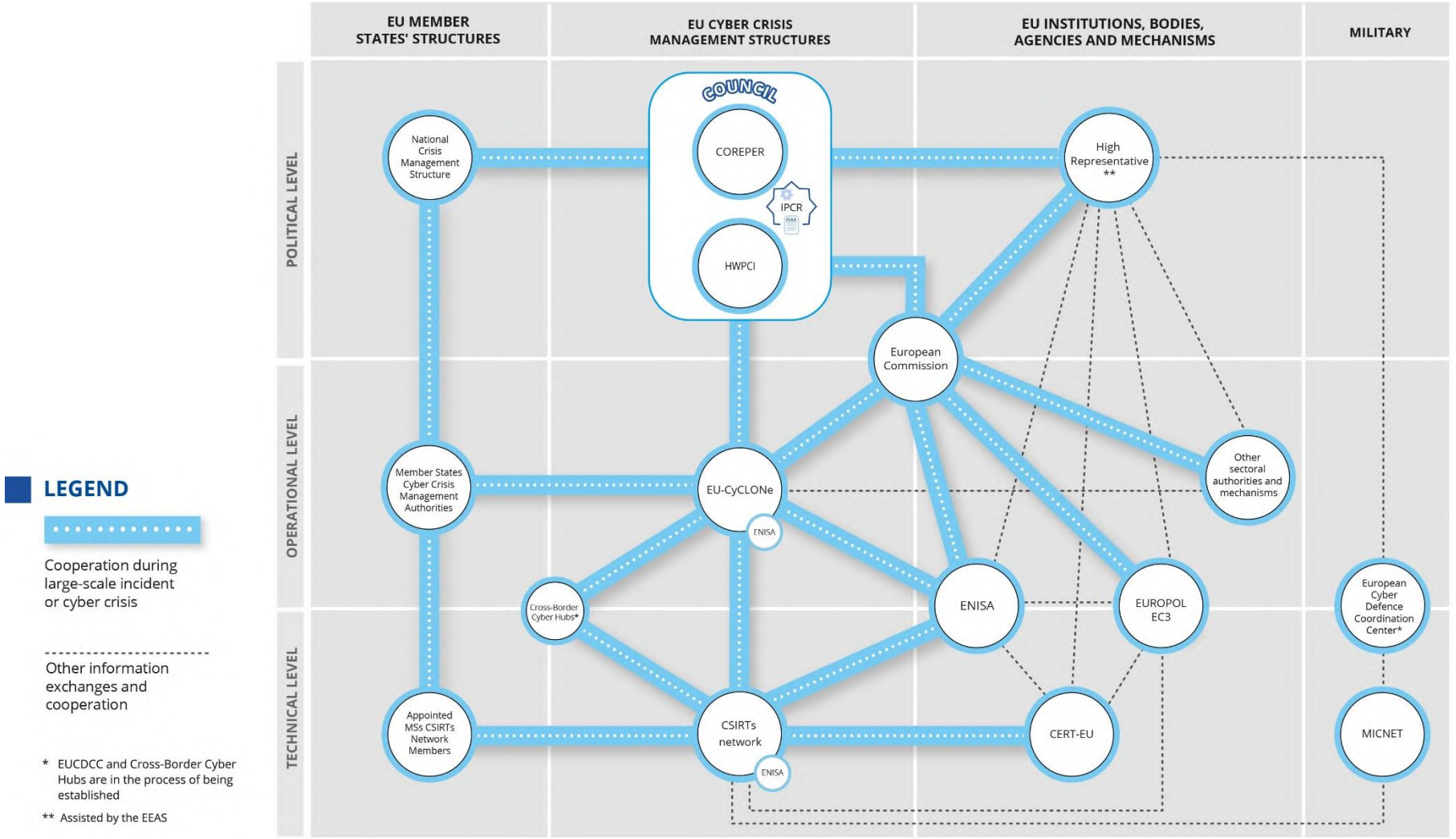
82. Ezt az ajánlást a Bizottságnak a tagállamokkal együttműködve, a közzétételt követően legalább négyévente felül kell vizsgálnia. A Bizottságnak minden felülvizsgálatot követően jelentést kell közzétennie, és azt be kell nyújtania a Tanácsnak. A Bizottságnak és a tagállamoknak figyelembe kell venniük mindenekelőtt a változó fenyegetettségi helyzet hatását, valamint a közös gyakorlatok és a jogszabályi változások eredményeit, különösen az (EU) 2019/881 rendelet felülvizsgálatából eredő esetleges változásokat.

Kelt Brüsszelben, -án/-én.

a Tanács részéről

az elnök

I. MELLÉKLET – A kiberbiztonsági válságkezelésre vonatkozó uniós terv



II. MELLÉKLET – AZ ÉRINTETT UNIÓS SZINTŰ SZEREPLŐK (SZERVEZETEK ÉS HÁLÓZATOK) ÉS VÁLSÁGKEZELÉSI MECHANIZMUSOK

(1) A főbb szereplők bevonása a kiberbiztonsági válságkezelés teljes ciklusa során (nagyszabású kiberbiztonsági események és kiberválságok)

	Felkészültség	Észlelés	Reagálás nagyszabású kiberbiztonsági eseményre vagy kiberválságra			Nyilvános kommunikáció	Helyreállítás és levont tanulságok
			technikai szinten	operatív szinten	politikai szinten		
Tagállamok	X	X	X	X	X	X	X
Bizottság	X			X	X	X	
Főképviselő, akinek munkáját az EKSZ segíti	X			X	X	X	
Tanács	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
CSIRT-hálózat	X	X	X				X
EU-CyCLONe	X			X	X		X

(2) Az érintett uniós szintű szereplők és mechanizmusok szerepe és hatásköre (betűrendi sorrendben) a kiberbiztonsági válságkezeléssel összefüggésben

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
CERT-EU	Technikai / Operatív	Koordinálja az uniós szervezeteket érintő súlyos eseményekre való, technikai szintű válságreagálást, és az említett események kezelését. Nyilvántartást vezet azon rendelkezésre álló technikai szakértelemről, amelyre súlyos események esetén az eseményekre való reagáláshoz szükség lehet, és segíti az IICB-t az uniós szervezetek súlyos eseményekre vonatkozó kiberbiztonsági válságkezelési terveinek koordinálásában. A CSIRT-hálózat tagja. Az EU-CyCLONe keretei között támogatja a Bizottságot a nagyszabású kiberbiztonsági események és válságok összehangolt kezelésében. A kiberbiztonsági információcsere és az eseményekre való reagálás koordinációs központjaként működik, amely megkönnyíti az eseményekkel, kiberfenyegetésekkel, sebezhetőségekkel és majdnem bekövetkezett (near miss)	(EU, Euratom) 2023/2841 rendelet (EU) 2025/38 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		eseményekkel kapcsolatos információcserét az uniós szervezetek és partnerek között. Kérelmezi az uniós kiberbiztonsági tartalék szolgáltatásait az uniós szervezetek nevében. Technikai megállapodásuk alapján együttműködik a NATO Kiberbiztonsági Központjával.	
Az Európai Unió Tanácsa	Politikai	Szakpolitikai döntéshozatali és koordinációs feladatok. Az uniós politikai szintű koordinációra és reagálásra vonatkozó IPCR-rel megbízott szereplő.	Az Európai Unióról szóló szerződés 16. cikke.
Az Európai Unió Tanácsának elnöksége	Politikai	Eldönti (kivéve, ha az Európai Unió működéséről szóló szerződés 222. cikke alapján alkalmazzák a szolidaritási klauzulát), hogy aktiválja-e az IPCR-t, és erről konzultál adott esetben az érintett tagállamokkal, valamint a Bizottsággal és a főképviselővel.	Az Európai Unióról szóló szerződés 16. cikke. A Tanács (EU) 2018/1993 végrehajtási határozata
Határokon átnyúló kiberközpontok	Technikai	A határokon átnyúló kiberközpontok írásbeli konzorciummegállapodással létrehozott, több országra	(EU) 2025/38 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		kiterjedő platformok, amely összehangolt hálózati struktúrába tömörítik legalább három tagállam nemzeti kiberközpontjait, és amelyek célja a kiberfenyegetések nyomon követésének, észlelésének és elemzésének javítása az események megelőzése és a kiberfenyegetettséggel kapcsolatos információk előállításának támogatása érdekében, különösen a releváns – és adott esetben anonimizált – adatok és információk cseréje, valamint a legkorszerűbb eszközök megosztása és kiberészlelési, -elemzési, valamint -megelőzési és -védelmi képességek megbízható környezetben való közös fejlesztése révén. Szorosan együttműködnek a CSIRT-hálózattal az információk megosztása érdekében. Az EU-CyCLONe-on és a CSIRT-hálózaton keresztül tájékoztatást nyújtanak a tagállami hatóságoknak és a Bizottságnak egy potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményről.	

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
A CSIRT-hálózat	Technikai	Hozzájárul a bizalomteremtéshez, és előmozdítja a tagállamok közötti gyors operatív együttműködést. A legfontosabb olyan hálózat, amely releváns információkat oszt meg az eseményekről, a majdnem bekövetkezett (near miss) eseményekről, a kiberfenyegetésekről, a kockázatokról és a sérülékenységekről. Az esemény által potenciálisan érintett tag kérésére a hálózat megosztja és megvitatja az adott eseménnyel és a kapcsolódó kiberfenyegetésekkel kapcsolatos információkat. A hálózat a koordinált reagálást is elősegítheti a kérelmező tag joghatóságán belül azonosított eseményre. Segítséget nyújt a tagállamoknak a határokon átnyúló események kezelésében, és feltérképezi az együttműködés további formáit, ideértve a kölcsönös segítségnyújtást is. Tájékoztatást kap a tagállamoktól az uniós	(EU) 2022/2555 irányelv (EU) 2025/38 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		kiberbiztonsági tartalék iránti kérelmeikről.	
A kibervédelmi parancsnokok konferenciája		A kibervédelmi parancsnokok nemzeti szintű fóruma a tagállamokon belül a folyamatban lévő kibertér-műveletekkel és a nagyszabású kiberbiztonsági események mérséklésére irányuló stratégiákkal kapcsolatos alapvető információk megosztása és cseréje céljából. A konferenciát az Európai Unió Tanácsának soros elnöksége szervezi az Európai Védelmi Ügynökség (EDA) és az Európai Külügyi Szolgálat (EKSZ) – beleértve az Európai Unió Katonai Törzsét (EUKT) –támogatásával.	Közös közlemény az EU kibervédelmi politikájáról (2022)
Bizottság	Operatív/Politikai	Az Európai Unió végrehajtó szerve. Biztosítja a belső piac zavartalan működését. Elősegíti a kapcsolódó uniós szintű válságelhárítási intézkedések közötti koherenciát és koordinációt. Meghoz az uniós polgári védelmi mechanizmusról szóló határozat szerinti, bizonyos általános uniós szintű felkészültséget célzó intézkedéseket, beleértve a	Az Európai Unióról szóló szerződés 17. cikke. (EU) 2018/1993 végrehajtási határozat 1313/2013/EU határozat (EU) 2022/2555 irányelv (EU) 2025/38 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		Veszélyhelyzet-reagálási Koordinációs Központ (ERCC) és a közös veszélyhelyzeti kommunikációs és tájékoztatási rendszer (CECIS) irányítását. Megfigyelő az EU-CyCLONe-ban, és az EU-CyCLONe tagja olyan, potenciális vagy folyamatban lévő nagyszabású események esetében, amelyek jelentős hatást gyakorolnak vagy gyakorolhatnak az (EU) 2022/2555 irányelv hatálya alá tartozó szolgáltatásokra és tevékenységekre. Megfigyelő a CSIRT-hálózatban. Általános felelősséggel tartozik az uniós kiberbiztonsági tartalék végrehajtásáért. Az Intézményközi Kiberbiztonsági Testületben a súlyos biztonsági eseményekkel kapcsolatos releváns információk EU-CyCLONe-nal való megosztásáért felelős kapcsolattartó. A Tanács elnöksége konzultál vele az IPCR aktiválására, illetve alkalmazásának megszüntetésére vonatkozó döntésekről (kivéve az EUMSZ 222. cikke szerinti szolidaritási	(EU, Euratom) 2023/2841 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		klauzula alkalmazása iránti kérés esetén). A Bizottság szolgálatai – az EKSZ-szel – elkészítik az integrált helyzetismereti és -elemzési jelentéseket.	
Európai Uniós Kiberbiztonsági Ügynökség (ENISA)	Technikai/Operatív	Feladatokat lát el a magas szintű kiberbiztonság Unión belüli elérése céljából, többek között azáltal, hogy aktívan támogatja a tagállamokat és az uniós intézményeket. Biztosítja a CSIRT-hálózat és az EU-CyCLONe titkárságát. Az eseményekről és a kiberfenyegetésekről rendszeres uniós kiberbiztonsági technikai helyzetjelentést készít (az EC3-mal és a CERT-EU-val, valamint szoros együttműködésben a tagállamokkal). Hozzájárul a határokon átnyúló nagyszabású eseményekre vagy válságokra való közös reagálás kialakításához elsősorban az alábbiak révén: - a nemzeti forrásokból származó jelentések összesítése és elemzése,	(EU) 2022/2555 irányelv (EU) 2019/881 rendelet (EU) 2025/38 rendelet (EU) 2024/2847 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		- a technikai, operatív és politikai szintek közötti információáramlás biztosítása, - kérésre az események kezelésének megkönnyítése, - az uniós szervezetek támogatása a nyilvános kommunikáció terén, - kérésre a tagállamok támogatása a nyilvános kommunikáció terén, - az eseményekre való reagálási képességek tesztelése és kiberbiztonsági gyakorlatok rendszeres szervezése. Ajánlatkérő szervként jár el, amennyiben részben vagy egészben megbízták az uniós kiberbiztonsági tartalék működtetésével és igazgatásával. Kétévente nagyszabású, átfogó kiberbiztonsági gyakorlatot szervez uniós szinten, technikai, operatív vagy stratégiai elemekkel. Az érintett tagállammal és más érdekelt felekkel együttműködésben eseményértékelési jelentést készít az adott esemény	

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		okainak, hatásának és mérséklésének értékelése céljából (a Bizottság vagy az EU-CyCLONe kérésére és az érintett tagállam jóváhagyásával). Tájékoztatja az EU-CyCLONe-t, ha a kiberrezilienciáról szóló rendelet szerinti jelentéstételi kötelezettségek keretében szolgáltatott információk relevánsak a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelése szempontjából.	
Az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózata (EU-CyCLONe)	Operatív	Támogatja a nagyszabású kiberbiztonsági események és válságok operatív szintű összehangolt kezelését. Biztosítja a releváns információk rendszeres cseréjét a tagállamok és az uniós intézmények, szervek, hivatalok és ügynökségek között. Összehangolja a nagyszabású kiberbiztonsági események és válságok kezelését, és támogatja az ilyen eseményekkel és válságokkal kapcsolatos politikai szintű döntéshozatalt.	(EU) 2022/2555 irányelv (EU) 2025/38 rendelet

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		Értékeli a releváns nagyszabású kiberbiztonsági események és válságok következményeit és hatását, valamint javaslatot tesz a lehetséges mérséklési intézkedésekre. Megvitatja – valamely érintett tagállam kérésére – a nagyszabású kiberbiztonsági eseményekre és válságok elhárítására szolgáló nemzeti terveket. Az ENISA-val és a Bizottsággal közösen kidolgozza az uniós kiberbiztonsági tartalékból származó támogatás iránti kérelmek benyújtásának megkönnyítésére szolgáló sablont. Tájékoztatást kap a tagállamoktól az uniós kiberbiztonsági tartalék iránti kérelmeikről. Potenciális vagy folyamatban lévő nagyszabású kiberbiztonsági eseményekkel kapcsolatos információkat fogad a határokon átnyúló kiberközpontoktól vagy a CSIRT-hálózattól.	
Az Unió külügyi és biztonságpolitikai főképviselője,	Politikai	Irányítja és koordinálja a külső kiber- és hibrid biztonsági	2010/427/EU tanácsi határozat

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
akinek munkáját az Európai Külügyi Szolgálat segíti		fenyegetések kezelésére irányuló uniós erőfeszítéseket. Felelős a külső fenyegetésektől való elrettentést és az azokra való reagálást célzó uniós kiberdiplomáciai és kibervédelmi eszközökért, többek között az Unió hibrid eszköztárának és kiberdiplomáciai eszköztárának használata révén. Együttműködik a külső partnerekkel, többek között KBVP-szerepvállalás révén is. Felkészültséget biztosít az Unió és a tagállamok számára a hibrid és kiberfenyegetésekre vonatkozó helyzetismeret és reagálási képesség tekintetében, például gyakorlatok, képzések és hálózatok révén. Kezeli az Unió űrtechnológiai eszközeinek biztonsági és védelmi vonatkozásait, különösen az Unió közös biztonság- és védelempolitikája (KBVP) keretében. Támogatja az uniós kibervédelmi parancsnokok konferenciáját. Támogatja a katonai hálózatbiztonsági vészhelyzeteket elhárító	

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
		csoportok uniós operatív hálózatát (MICNET). A Tanács elnöksége konzultál vele az IPCR aktiválására, illetve alkalmazásának megszüntetésére vonatkozó döntésekről (kivéve az EUMSZ 222. cikke szerinti szolidaritási klauzula alkalmazása iránti kérés esetén). Az EKSZ – a Bizottság szolgálataival – elkészíti az integrált helyzetismereti és -elemzési jelentéseket.	
Az EU kibervédelmi koordinációs központja	Horizontális	Eredeti célja elsősorban az Unió és tagállamai közös helyzetismeretének javítása a kibertérben folytatott rossz szándékú tevékenységekkel kapcsolatban, különös tekintettel a katonai KBVP-missziókra és -műveletekre.	Közös közlemény az EU kibervédelmi politikájáról (2022)
Europol	Operatív	Operatív és technikai támogatást nyújt a tagállamok illetékes hatóságainak a kiberbűnözés megelőzéséhez és az attól való elrettentéshez. Kérésükre segítséget nyújt a tagállamok illetékes hatóságainak a gyaníthatóan bűncselekményhez kötődő kibertámadásokra való reagálásban.	(EU) 2016/794 rendelet, beleértve annak összes módosítását

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
Intézményközi Kiberbiztonsági Testület		Kiberbiztonsági válságkezelési tervet hoz létre az uniós szervezeteket érintő súlyos események koordinált kezelésének operatív szintű támogatása, valamint a releváns információk rendszeres cseréjéhez való hozzájárulás céljából. Koordinálja az egyes uniós szervezetek kiberbiztonsági válságkezelési terveinek elfogadását. A CERT-EU javaslata alapján iránymutatásokat vagy ajánlásokat fogad el az uniós szervezeteket érintő jelentős eseményekre való reagálással kapcsolatos együttműködésről.	(EU, Euratom) 2023/2841 rendelet
Katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok operatív hálózata (MICNET)	Technikai	Előmozdítja az EU-n belüli védelmi rendszereket – többek között a katonai KBVP-missziókban és -műveletekben alkalmazott rendszereket – érintő kiberbiztonsági fenyegetésekre való erőteljesebb és összehangoltabb reagálást; az Európai Védelmi Ügynökség támogatja.	Közös közlemény az EU kibervédelmi politikájáról (2022)

Szereplő	Szint	Szerep és hatáskör	Hivatkozás
Egységes információelemzési kapacitás (SIAC)		A következőkből áll: (1) az Európai Unió Helyzetelemző Központja (EU INTCEN) és (2) az Európai Unió Katonai Törzsének Hírszerzési Igazgatósága (EUMS INT). Stratégiai hírszerzést biztosít a külpolitikával, a terrorizmussal és a hibrid fenyegetésekkel kapcsolatban, továbbá Kezeli a KBVP-missziók katonai hírszerzését, és támogatja az uniós védelmi és válságkezelési műveleteket. A főképviselő irányítása alá tartozik.	Az Európai Unióról szóló szerződés 38. és 42–46. cikke.

(3) Releváns uniós szintű válságkezelési mechanizmusok és platformok

Mechanizmus	Horizontális /ágazati / kiberspecifikus	Leírás	Hivatkozás
ARGUS	Horizontális	A Bizottság koordinációs folyamata és általános riasztórendszere az uniós szintű fellépést igénylő, határokon átnyúló súlyos válságokra való koherens reagálás céljából. Összefogja az összes érintett szolgálatot és kabinetet, annak érdekében, hogy döntsenek az intézkedésekről és koordinálják azokat. Lehetővé teszi a Bizottság számára a kialakuló, több ágazatot érintő válságokra, illetve az uniós szintű fellépést igénylő, előre látható vagy közvetlen fenyegetésekre vonatkozó releváns információk cseréjét.	A Bizottság közleménye, COM(2005)662 végleges
Az EKSZ Válságelhárítási Központja (CRC)	Horizontális	Egyedüli kapcsolattartó pontként szolgál az EKSZ-nél a válságokkal kapcsolatos valamennyi kérdésben, valamint a hét minden napján, napi 24 órában működő állandó válságreagálási kapacitást biztosít az Unió küldöttségei személyzetének biztonságát fenyegető vészhelyzetekre és/vagy az uniós polgárokat külföldön érintő válsághelyzetekre való reagálás során. Biztonsági, konzuli és	A biztonság és a védelem területére vonatkozó stratégiai iránytű – Egy, a polgárait, az értékeit és az érdekeit megvédő Európai Unióért, amely hozzájárul a nemzetközi béke és biztonság

Mechanizmus	Horizontális /ágazati / kiberspecifikus	Leírás	Hivatkozás
		helyzetismereti szakértőket tömörít, miközben a helyszínen az Unió küldöttségeinek elkötelezett szakembereire támaszkodik.	megvalósításához (2022. március 21.)
A kritikus infrastruktúrákra vonatkozó terv	Horizontális	Koordinálja a kritikus infrastruktúrák számottevő mértékben határokon átnyúló jelentőségű zavaraira való uniós szintű reagálást.	A Tanács C/2024/4371 ajánlása
Kiberbiztonsági Riasztási Rendszer	Kiberspecifikus	Fejlett uniós képességeket biztosít a kiberfenyegetésekkel kapcsolatos észlelési, elemzési és adatkezelési képességek javítása, valamint az Unión belüli események megelőzése érdekében.	(EU) 2025/38 rendelet
Kiberdiplomáciai eszköztár (a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések kerete)	Kiberspecifikus	Lehetővé teszi a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedéseket, hozzájárulva a konfliktusmegelőzéshez, a kiberbiztonsági fenyegetések mérsékléséhez és a nemzetközi kapcsolatok nagyobb stabilitásához.	A Tanács következtetései, 2017. június 19. Felülvizsgált végrehajtási iránymutatások, 10289/23, 2023. június 8.
Uniós kiberbiztonsági tartalék	Kiberspecifikus	Kiberbiztonsági szakértőket és erőforrásokat mozgósít válságok idején a tagállamok, az uniós intézmények, szervek vagy ügynökségek reagálási erőfeszítéseinek támogatása érdekében.	(EU) 2025/38 rendelet

Mechanizmus	Horizontális /ágazati / kiberspecifikus	Leírás	Hivatkozás
A határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó ágazatspecifikus szabályokról szóló üzemi és kereskedelmi szabályzat	Ágazati	Ismétlődő kiberbiztonsági kockázatértékelési folyamatot hoz létre a villamosenergia-ágazatban uniós, tagállami, regionális és szervezeti szinten. Kifejezetten a válságkezelésre, valamint a CSIRT-ekkel és az EU-CyCLONe-nal való együttműködésre vonatkozó rendelkezéseket tartalmaz azokra az esetekre, amikor egy nagyszabású kiberbiztonsági esemény hatással van egyéb, a villamosenergia-ellátás biztonságától függő ágazatokra.	A Bizottság (EU) 2024/1366 felhatalmazáson alapuló rendelete
Hibrid eszköztár	Horizontális	A benne foglalt rendelkezések célja a következők biztosítása: annak áttekintése, hogy mi áll rendelkezésre uniós szinten a hibrid fenyegetések valamennyi típusára való reagálás tekintetében és a koordinált alkalmazásuk, gondoskodva fellépéseink koherenciájáról a különböző területeken. A hibrid eszköztár segít biztosítani, hogy a döntéshozatal átfogó helyzetismereten és a levont tanulságokon alapuljon.	A Tanács következtetései a hibrid hadjáratokra való koordinált uniós reagálásra vonatkozó keretről, 2022. június 22. Végrehajtási iránymutatások a hibrid hadjáratokra való koordinált uniós reagálásra vonatkozó kerethez, 2022. december 14.

Mechanizmus	Horizontális /ágazati / kiberspecifikus	Leírás	Hivatkozás
Hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatok	Horizontális	Az uniós hibrid eszköztár részeként a hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatok a vonatkozó ágazati nemzeti és uniós polgári és katonai szakértelemre támaszkodnak annak érdekében, hogy testre szabott és célzott, rövid távú segítséget nyújtsanak a tagállamoknak, a közös biztonság- és védelempolitika hatálya alá tartozó missziónak és műveleteknek, valamint a partnerországoknak a hibrid fenyegetések és hadjáratok elleni küzdelemben.	A hibrid fenyegetéseket kezelő uniós gyorsreagálású csapatok gyakorlati létrehozására vonatkozó irányadó keret (2024. május 21.) A hibrid fenyegetéseket kezelő gyorsreagálású csapatok telepítésére vonatkozó operatív iránymutatás, a Coreper által 2024. december 4-én jóváhagyva
IPCR	Horizontális	Támogatja a gyors és koordinált uniós politikai szintű döntéshozatalt a súlyos és összetett válsághelyzetek esetén. Az aktiválására és az alkalmazásának megszüntetésére vonatkozó döntést a Tanács elnöksége hozza meg, amely konzultál az érintett tagállamokkal, a Bizottsággal és a főképviselővel (kivéve a szolidaritási klauzula alkalmazása iránti kérés esetén). A Tanács Főtitkársága, a Bizottság szolgálatai és az EKSZ az	A Tanács (EU) 2018/1993 végrehajtási határozata

Mechanizmus	Horizontális /ágazati / kiberspecifikus	Leírás	Hivatkozás
		elnökséggel konzultálva megállapodhatnak abban is, hogy az IPCR-t információmegosztási módban aktiválják. Az IPCR munkájának alapjául a Bizottság szolgálatai és az EKSZ által készített integrált helyzetismereti és -elemzési jelentések szolgálnak. E jelentések a tagállamok (például az érintett nemzeti válságközpontok), valamint az uniós ügynökségek és szervek által szolgáltatott releváns információkra és elemzésekre támaszkodnak.	
Uniós bűnüldözési vészhelyzet-elhárítási protokoll	Horizontális	Olyan eszköz, amely gyors értékelés, a kritikus információk biztonságos és időben történő megosztása, valamint nyomozásaik nemzetközi vonatkozásainak hatékony koordinálása révén támogatja az uniós bűnüldöző hatóságokat a súlyos, határokon átnyúló kibertámadásokra való azonnali reagálásban.	A Tanács következtetései (2018. június 26.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról
PESCO kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok (CRRT)	Kiberspecifikus	A PESCO CRRT-k az uniós tagállamok azzal a céllal közösen kifejlesztett polgári-katonai kibervédelmi képessége, hogy gyorsan reagáljanak a kiberbiztonsági eseményekre és a	Az Európai Unióról szóló szerződés 42. cikkének (6) bekezdése, 46. cikke és 10. jegyzőkönyve

Mechanizmus	Horizontális /ágazati / kiberspecifikus	Leírás	Hivatkozás
		kiberválságokra, valamint megelőző intézkedéseket – például sebezhetőségi értékeléseket és választási megfigyelést – végezzenek. A PESCO CRRT-k megbízatása az, hogy kérésre kibertámogatást nyújtsanak az uniós tagállamoknak, az uniós intézményeknek, szerveknek és ügynökségeknek, az uniós katonai KBVP-missziónak és -műveleteknek, valamint a partnerországoknak.	

Űrfenyegetés-elhárítási architektúra (STRA)	Ágazati (Űrfenyegetések, beleértve a kiber vonatkozásúakat is)	Az űrfenyegetés-elhárítási architektúra (STRA) az uniós űrprogram keretében létrehozott rendszerek és nyújtott szolgáltatások kiépítéséből, üzemeltetéséből vagy használatából eredő fenyegetések elhárításával kapcsolatos, a Tanács és a főképviselő által ellátandó feladatköröket foglalja magában.	A Tanács (KKBP) 2021/698 határozata
A rendszerszintű kiberbiztonsági események koordinációs kerete (EU-SCICF)	Ágazati	Kidolgozás alatt álló olyan kommunikációs és koordinációs keret, amely a pénzügyi ágazat potenciális rendszerszintű kibereseményeire vonatkozik és kezeli azokat. A keret az európai felügyeleti hatóságoknak az (EU) 2022/2554 rendelet szerinti egyik tervezett szerepére fog épülni, amely szerint fokozatosan lehetővé kell tenniük az eredményes, koordinált uniós szintű reagálást annak érdekében, hogy kezelhessék az információs és kommunikációs technológiákkal (IKT) kapcsolatos jelentős, határokon átnyúló eseményeket vagy az azokhoz kapcsolódó fenyegetéseket, amelyek rendszerszintű hatással lehetnek az uniós pénzügyi ágazat egészére.	Az Európai Rendszerkockázati Testület ajánlása (2021. december 2.) a rendszerszintű kiberbiztonsági események érintett hatóságok számára létrehozandó páneurópai koordinációs keretéről (ERKT/2021/17)
Uniós polgári védelmi	Horizontális	Polgári védelmi együttműködést biztosít a katasztrófamegelőzés, -	1313/2013/EU határozat

mechanizmus (UCPM)		felkészültség és -reagálás javítása érdekében.	
CISE – Közös információmegosztási környezet	Tengeri vonatkozású, és hét ágazatra terjed ki.	A CISE olyan hálózat, amely összeköti az EU/EGT tengerfelügyeletért felelős hatóságainak rendszereit. A CISE lehetővé teszi a releváns információk határokon és különböző ágazatokon átnyúló, zökkenőmentes és automatizált cseréjét.	A biztonság és a védelem területére vonatkozó stratégiai iránytű – Egy, a polgárait, az értékeit és az érdekeit megvédő Európai Unióért, amely hozzájárul a nemzetközi béke és biztonság megvalósításához (2022. március 21.)

(4) Az (EU) 2022/2555 irányelv szerinti kiemelten kritikus ágazatok és egyéb kritikus ágazatok, valamint uniós szintű ágazati válságkezelési mechanizmusok (adott esetben)		
Ágazatok	**Alágazat**	**Alkalmazandó ágazati válságkezelési mechanizmusok**
Energia	Villamos energia	Villamosenergia-ügyi koordinációs csoport
	Távfűtés és -hűtés	n. a.
	Olaj	Olajkoordinációs csoport Európai Uniós Tengerhatósági Csoport (EUOAG)
	Gáz	Gázkoordinációs csoport
	Hidrogén	n. a.
Szállítás	Légi	Európai Légiközlekedési Válságkoordinációs Egység (EACCC)
	Vasúti	n. a.
	Vízi	Európai Halászati Ellenőrző Hivatal (EFCA) SafeSeaNet (SSN) Integrált tengeri szolgáltatások (IMS) A nagy hatókörű hajóazonosító és nyomon követő rendszer adatközpontja (LRIT) EMSA tengeri támogató szolgáltatások

	Közúti	n. a.
	Horizontális	A közlekedési kapcsolattartó pontok hálózata, amelyet a közlekedésre vonatkozó vészhelyzeti terv (COM(2022) 211) hozott létre
Banki szolgáltatások		EU-SCICF
Pénzügyi piaci infrastruktúrák		EU-SCICF Európai pénzügyi stabilizációs mechanizmus

Egészségügy		Korai figyelmeztető és gyorsreagáló rendszer (EWRS) Az egészségügyi szükséghelyzeti műveleti központ (HEOF) szövetekkel és sejtekkel, illetve vérkomponensekkel kapcsolatos riasztási rendszere (RATC/RAB) Közegészségügyi szükséghelyzeti keret Vegyi incidensek riasztási rendszere (RASCHEM) A fertőző betegségek európai felügyeleti portálja Egészségügyi Szükséghelyzet-felkészültségi és -reagálási Hatóság (HERA) Orvosi egészségügyi információs rendszer (MediSys) Az orvostechnikai eszközök hiányával foglalkozó ügyvezető irányítócsoport (MDSSG) Farmakovigilanciai riasztási rendszer Uniós egészségügyi munkacsoport (EUHTF) Egészségügyi Biztonsági Bizottság
Ivóvíz		n. a.

Szennyvíz		n. a.
Digitális infrastruktúra		n. a.
IKT-szolgáltatások irányítása		n. a.
Közigazgatás		n. a.
Világűr		Űrfenyegetés-elhárítási architektúra (STRA)
Postai és futárszolgáltatások		n. a.
Hulladékgazdálkodás		n. a.
Vegyszerek gyártása, előállítása és forgalmazása		Vegyi incidensek riasztási rendszere (RASCHEM)

Élelmiszer-termelés, -feldolgozás és -forgalmazás		Európai terméshozam-megfigyelési rendszer Mezőgazdasági termelési rendellenességek helyszíneinek globális észlelése (ASAP) Európai növényegészségügyi értesítési rendszer (EUROPHYT) Uniós állategészségügyi sürgősségi csoport (EUVET) Élelmiszer- és takarmánybiztonsági riasztási rendszer (RASFF) Az élelmezésbiztonsági válságokra való felkészültségre és reagálásra vonatkozó európai mechanizmus (EFSCM) A belső piaci szükséghelyzetről és rezilienciáról szóló rendelet (IMERA)
Gyártás	Orvostechnikai eszközök	n. a.
	Számítógépek, elektronikai és optikai termékek	n. a.
	Gépek és gépi berendezések	n. a.
	Gépjárművek, pótkocsik és félpótkocsik gyártása	n. a.
	Egyéb szállítóeszközök gyártása	n. a.

Digitális szolgáltatók		n. a.
Kutatás		n. a.

III. MELLÉKLET – Uniós kiberbiztonsági válságkezelési keret és kapcsolódó eszközök

2017 óta az Unió több olyan, az alábbiakban felsorolt eszköz révén alakította ki kiberbiztonsági keretét, amelyek a kiberbiztonsági válságkezelés szempontjából releváns rendelkezéseket tartalmaznak:

- az (EU) 2019/881 európai parlamenti és tanácsi rendelet[1],
- az (EU) 2022/2555 európai parlamenti és tanácsi irányelv[2],
- az (EU) 2024/2690 bizottsági végrehajtási rendelet[3], az (EU, Euratom) 2023/2841 európai parlamenti és tanácsi rendelet[4],
- az (EU) 2021/887 európai parlamenti és tanácsi rendelet[5],
- az (EU) 2024/2847 európai parlamenti és tanácsi rendelet[6], valamint
- az (EU) 2025/38 európai parlamenti és tanácsi rendelet (a kiberszolidaritásról szóló rendelet)[7].

A kiberbiztonsági válsággal kapcsolatos konkrét ágazati intézkedések közé tartozik az (EU) 2024/1366 felhatalmazáson alapuló bizottsági rendelet[8] és az (EU) 2022/2554 európai parlamenti és tanácsi rendelettel[9] összefüggésben a rendszerszintű kiberbiztonsági események koordinációs kerete (EU-SCICF).

A 2013/40/EU irányelv[10] hivatkozásként szolgál a kibertámadásokkal kapcsolatos bűnözői tevékenységek fogalmának meghatározásához, valamint az elektronikus bizonyítékokhoz való határokon átnyúló hozzáférésre vonatkozó uniós szabályokhoz, az (EU) 2023/1543 európai parlamenti és tanácsi rendelet pedig különösen [11] – a végrehajtását követően – jelentősen megkönnyíti majd a bűnüldözési intézkedéseket ezen a területen.

Az EU kibervédelmi politikája[12] felvázolja a katonai hálózatbiztonsági vészhelyzeteket elhárító csoportok uniós operatív hálózatának (MICNET) és az uniós kibervédelmi parancsnokok konferenciájának szerepét, és előirányozza az EU kibervédelmi koordinációs központjának (EUCDCC) létrehozását.

Az (EU) 2022/2555 irányelv I. és II. mellékletében felsorolt egyes kritikus ágazatokban léteznek más, nem kiberbiztonsági vonatkozású helyzetismereti és válságelhárítási mechanizmusok.

A kritikus infrastruktúrák számottevő mértékben határokon átnyúló jelentőségű zavaraira való uniós szintű reagálás koordinálására szolgáló tervről szóló tanácsi ajánlás[13] rendelkezik az érintett szereplők közötti együttműködésről arra az esetre, ha egy adott esemény a kritikus infrastruktúra fizikai vonatkozásait és kiberbiztonságát egyaránt érinti.

[1] 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., ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 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., ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] A Bizottság (EU) 2024/2690 végrehajtási rendelete (2024. október 17.) az (EU) 2022/2555 irányelvnek a kiberbiztonsági kockázatkezelési intézkedések technikai és módszertani követelményei, valamint a DNS-szolgáltatók, a legfelső szintű doménnév-nyilvántartók, a felhőszolgáltatók, az adatközpont-szolgáltatók, a tartalomszolgáltató hálózati szolgáltatók, az irányított szolgáltatók, az irányított biztonsági szolgáltatók, az online piacterek, online keresőprogramok vagy közösségimédia-szolgáltatási platformok szolgáltatói és a bizalmi szolgáltatók tekintetében jelentősnek minősülő biztonsági események eseteinek további pontosítása tekintetében történő alkalmazására vonatkozó szabályok megállapításáról (HL L, 2024/2690, 2024.10.18.). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

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

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

[6] Az Európai Parlament és a Tanács (EU) 2024/2847 rendelete (2024. október 23.) a digitális elemeket tartalmazó termékekre vonatkozó horizontális kiberbiztonsági követelményekről, valamint a 168/2013/EU és az (EU) 2019/1020 rendelet, és az (EU) 2020/1828 irányelv módosításáról (a kiberrezilienciáról szóló rendelet) (HL L, 2024/2847, 2024.11.20., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Az Európai Parlament és a Tanács (EU) 2025/38 rendelete (2024. december 19.) a kiberfenyegetések és -események észlelése, valamint az azokra való felkészülés és reagálás érdekében az Unión belüli szolidaritás és

képességek megerősítését célzó intézkedések meghatározásáról, és az (EU) 2021/694 rendelet módosításáról (a kiberszolidaritásról szóló rendelet) (HL L, 2025/38, 2025.1.15., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] A Bizottság (EU) 2024/1366 felhatalmazáson alapuló rendelete (2024. március 11.) az (EU) 2019/943 európai parlamenti és tanácsi rendeletnek a határkeresztező villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó ágazatspecifikus szabályokról szóló üzemi és kereskedelmi szabályzat létrehozása révén történő kiegészítéséről (HL L, 2024/1366, 2024.5.24., ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

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

[10] 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., ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Az Európai Parlament és a Tanács (EU) 2023/1543 rendelete (2023. július 12.) a büntetőeljárás során az elektronikus bizonyítékokkal kapcsolatban, valamint a büntetőeljárást követően a szabadságvesztés-büntetések végrehajtása céljából kibocsátott, közlésre kötelező európai határozatokról és megőrzésre kötelező európai határozatokról, valamint Az Európai Parlament és a Tanács (EU) 2023/1544 irányelve (2023. július 12.) a büntetőeljárásban az elektronikus bizonyítékok gyűjtése céljából a kijelölt telephelyek kijelöléséről és a jogi képviselők kinevezéséről szóló harmonizált szabályok meghatározásáról (HL L 191., 2023.7.28., 118. o., ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52022JC0049

[13] *HL C, C/2024/4371, 2024.7.5.* https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:C_202404371