Az Európai Unió
Tanácsa

Brüsszel, 2021. október 8.
(OR. en)

12534/21

CYBER 253
JAI 1064
TELECOM 361
CSC 340
CIS 110
RELEX 827
ENFOPOL 343
COPS 341
COSI 179
HYBRID 59
CSCI 127
POLGEN 172
DATAPROTECT 230

FELJEGYZÉS AZ „I/A” NAPIRENDI PONTHOZ

Küldi:	a Tanács Főtitkársága
Címzett:	az Állandó Képviselők Bizottsága (II. rész)/a Tanács
Tárgy:	A Tanács következtetései a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás kiegészítéseként szolgáló, a közös kiberbiztonsági egységre vonatkozó kezdeményezésben rejlő lehetőségek feltárásáról – Jóváhagyás

1. A Bizottság 2021. június 23-án közzétette a közös kiberbiztonsági egység létrehozásáról szóló ajánlását[1], amely a közszolgáltatásokat, valamint a vállalkozások és a polgárok életét az Európai Unióban mindenütt érintő, egyre növekvő számú súlyos kiberbiztonsági eseménnyel szembeni fellépésre irányul.

2. A Bizottság a kiberkérdésekkel foglalkozó horizontális munkacsoport 2021. június 28-i ülésén ismertette az ajánlást. Ezt követően a szlovén elnökség alatt további megbeszélésekre került sor a horizontális munkacsoport 2021. július 7-i és 14-i ülésén, ahol meghallgatták a tagállamok véleményét a bizottsági ajánlásról.

[1] C(2021) 4520 final (11155/21 és 11155/21 ADD1).

3. Az elnökség a kiberkérdésekkel foglalkozó horizontális munkacsoport tagjainak 2021. július 23-i nem hivatalos videokonferenciája keretében előterjesztette a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás kiegészítéseként szolgáló, a közös kiberbiztonsági egységre vonatkozó kezdeményezésben rejlő lehetőségek feltárásáról szóló tanácsi következtetések első tervezetét[2]. A horizontális munkacsoport a 2021. szeptember 8-i és 29-i ülésén további megbeszéléseket folytatott e következtetéstervezetről.

4. A munkacsoport a 2021. október 6-i ülésén jóváhagyta a mellékletben foglalt tanácsi következtetéstervezetet.

5. A fentiek alapján felkérjük az Állandó Képviselők Bizottságát, hogy nyújtsa be a tanácsi következtetések mellékletben foglalt tervezetét a Tanácsnak, és javasolja e következtetéstervezet „A” napirendi pontként történő elfogadását.

---

[2] 10975/21.

MELLÉKLET

Tervezet – A Tanács következtetései a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálás kiegészítéseként szolgáló, a közös kiberbiztonsági egységre vonatkozó kezdeményezésben rejlő lehetőségek feltárásáról

AZ EURÓPAI UNIÓ TANÁCSA,

EMLÉKEZTETVE a következőkre:

– a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról szóló tanácsi következtetések[3],

– a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt uniós reagálásról szóló tanácsi következtetések[4],

– a kiberdiplomáciáról szóló tanácsi következtetések[5],

– a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”) szóló tanácsi következtetések[6],

– a biztonságról és a védelemről szóló tanácsi következtetések[7],

– az uniós kibervédelmi szakpolitikai keret[8],

– az Európa digitális jövőjének alakításáról szóló tanácsi következtetések[9],

– az uniós politikai szintű integrált válságelhárítási mechanizmusról szóló, 2018. december 11-i (EU) 2018/1993 tanácsi végrehajtási határozat,

---

3 7290/21.
4 10086/18.
5 6122/15 + COR 1.
6 10474/17.
7 8396/21.
8 15585/14.
9 8711/20.

– az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése” című, az Európai Parlamenthez és a Tanácshoz intézett közös közleményről szóló tanácsi következtetések[10],

– az uniós kiberbiztonsági kapacitás és képességek megerősítéséről szóló tanácsi következtetések[11];

1. KIEMELI a kiberbiztonság fontosságát a reziliens, digitális és zöld Európa kialakítása szempontjából. HANGSÚLYOZZA, hogy a kiberbiztonság elengedhetetlen az EU és annak tagállamai, népei, vállalkozásai és intézményei jólétéhez és biztonságához, valamint szabad és demokratikus társadalmaink integritásának fenntartásához;

2. TUDATÁBAN VAN ANNAK, hogy számos kiberbiztonsági fenyegetés határokon és ágazatokon átnyúló jellegű, ahogy annak is, hogy milyen kockázatokkal és potenciális következményekkel járnak az egyre nagyobb hatást kiváltó, egyre kifinomultabb, célzottabb, összetettebb, kitartóbb és/vagy elterjedtebb rossz szándékú kibertevékenységek folyamatos kampányai[12]. A Covid19-világjárvány még inkább rávilágított társadalmaink sebezhetőségére, valamint arra, hogy a nagyszabású kiberbiztonsági események milyen károkat okozhatnak a gazdaságra, a demokráciára, az alapvető szolgáltatásokra és a kritikus infrastruktúrára nézve, különösen az egészségügyi ágazatban. Emellett a járvány növelte a konnektivitás fontosságát és a társadalom függőségét a megbízható, bizalomra érdemes és biztonságos hálózati és információs rendszerektől. Végezetül pedig rávilágított arra, hogy globális, nyitott, szabad, stabil és biztonságos internetre van szükség, és fontos az információs és kommunikációs technológiai (IKT) termékekbe, folyamatokba és szolgáltatásokba, valamint az azok biztonságába vetett bizalom, ideértve a reziliens ellátási lánc biztosításának szükségességét is;

---

10 14435/17 + COR 1.
11 7737/19.
12 Az ENISA fenyegetettségi helyzetjelentése (2020).

3. ÚJÓLAG HANGSÚLYOZZA a kiberrezilienciának és az uniós kiberbiztonsági válságkezelési keret továbbfejlesztésének a fontosságát[13], amelynek célja, hogy uniós szinten hatékonyan és időben lehessen reagálni a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre, és fontos annak további integrálása a meglévő horizontális és ágazati uniós válságelhárítási mechanizmusokba. KIEMELI a Tanács és a politikai szintű integrált válságelhárítási mechanizmus szerepét abban, hogy a széles körű hatással járó vagy politikai jelentőséggel bíró válságok esetén biztosított legyen az uniós politikai szintű, időben történő koordináció és reagálás, függetlenül attól, hogy az Unión belülről vagy kívülről eredő válságról van-e szó. KIEMELI, hogy fontos ezeket a kereteket és mechanizmusokat rendszeres gyakorlatok keretében tesztelni;

4. EMLÉKEZTET arra, hogy a nagyszabású kiberbiztonsági eseményekkel és válsághelyzetekkel kapcsolatos uniós szintű tevékenységekre a szubszidiaritás, az arányosság, a kiegészítő jelleg, az átfedésektől való mentesség és a bizalmas jelleg elvével összhangban kerül sor. ÚJÓLAG HANGSÚLYOZZA, hogy elsődlegesen a tagállamok felelőssége az őket érintő nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való reagálás. EMLÉKEZTET arra, hogy az Európai Unióról szóló szerződés 4. cikkének (2) bekezdésével összhangban tiszteletben kell tartani a tagállamok hatásköreit és a nemzetbiztonsággal kapcsolatos kizárólagos felelősségüket, a kiberbiztonság területén is;

5. EMLÉKEZTET ugyanakkor arra, hogy tiszteletben kell tartani az uniós intézmények, szervek és hivatalok hatásköreit és megbízatását. A főképviselő, a Bizottság és más uniós intézmények, szervek és hivatalok az uniós jogból eredően szintén lényeges szerepet töltenek be, többek között a nagyszabású kiberbiztonsági események és válsághelyzetek által az egységes piacra, valamint maguknak az uniós intézményeknek, szerveknek és hivataloknak a működésére gyakorolt potenciális hatás miatt;

[13] 10086/18.

6. HANGSÚLYOZZA, hogy el kell kerülni a felesleges átfedéseket, és kiegészítő jellegre, illetve hozzáadott értékre kell törekedni az uniós kiberbiztonsági válságkezelési keret továbbfejlesztése során, valamint biztosítani kell a meglévő nemzeti és európai szintű mechanizmusokkal, kezdeményezésekkel, hálózatokkal, folyamatokkal és eljárásokkal való összhangot. HANGSÚLYOZZA, hogy észszerűsíteni kell a meglévő folyamatokat és struktúrákat azért, hogy azok kevésbé legyenek összetettek, és az Unión belüli kohézió érdekében hozzáférhetőbbek és reagálóképesebbek legyenek azok számára, akik segítséget kérnek vagy szolidaritást igényelnek;

7. ELISMERI a nemzetközi jognak – többek között az Egyesült Nemzetek teljes Alapokmányának –, a nemzetközi humanitárius jognak és az emberi jogok nemzetközi jogának a kibertérben való alkalmazandóságát, és SZORGALMAZZA az ENSZ valamennyi tagállama által jóváhagyott, a kibertérben tanúsított felelősségteljes állami magatartás önkéntes, nem kötelező erejű normáinak, szabályainak és elveinek betartását;

8. ÜDVÖZLI azt az előrelépést, amelyet az elmúlt években a Tanácson belül sikerült elérni különösen a kiberkérdésekkel foglalkozó horizontális munkacsoportban és más releváns tanácsi munkacsoportokban, illetve a tagállamok közötti egyéb együttműködési és információmegosztási kezdeményezések, hálózatok és mechanizmusok létrehozása terén, ideértve nevezetesen a 2016. július 6-i (EU) 2016/1148 európai parlamenti és tanácsi irányelv által létrehozott Kiberbiztonsági Együttműködési Csoportot és CSIRT-hálózatot, az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatát (CyCLONe), az állandó strukturált együttműködés (PESCO) keretében indított, kibervédelemmel kapcsolatos releváns projekteket[14], a kiberbűnözés elleni közös fellépés munkacsoportját (J-CAT), a számítástechnikai bűnözés elleni európai igazságügyi hálózatot (EJCN), a tagállamok által az Európai Unió Helyzetelemző Központjának (EU INTCEN) nyújtott önkéntes hozzájárulásokat, valamint a kiberdiplomáciai eszköztár keretében megvalósított koordinációt és együttműködést;

---

[14] Különösen a „kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok, valamint kölcsönös segítségnyújtás a kiberbiztonság területén” elnevezésű, Litvánia által koordinált projekt, „A Kiber- és az Információs Terület Koordinációs Központja”, amelynek koordinátora Németország, illetve „a kiberfenyegetésekre és kiberbiztonsági eseményekre való reagálással kapcsolatos információmegosztási platform”, amelyet Görögország koordinál.

9. EMLÉKEZTET az uniós intézmények, szervek és hivatalok közötti együttműködés meglévő kereteire, például az ENISA és a CERT-EU közötti strukturált együttműködésre, valamint az ENISA, az Európai Védelmi Ügynökség (EDA), az Europol Kiberbűnözés Elleni Európai Központja (EC3) és a CERT-EU közötti egyetértési megállapodásra. HANGSÚLYOZZA, hogy az ezen együttműködési kereteket érintő további fejleményekre vonatkozó információkat folyamatosan és rendszeresen meg kell osztani a Tanáccsal;

10. KIEMELI, hogy minden szükséges – technikai, operatív és stratégiai/politikai – szinten fokozni kell az együttműködést és az információmegosztást az EU-n és a tagállamain belüli különböző kiberközösségek között, valamint össze kell kapcsolni a meglévő válságkezelési mechanizmusokat, hálózatokat, struktúrákat, folyamatokat és eljárásokat, amennyiben ez támogatja és javítja a nagyszabású kiberbiztonsági események és válsághelyzetek kezelését;

11. NYUGTÁZZA, hogy a tagállamok egy csoportja előrelépést ért el a PESCO keretében a „kiberbiztonsági eseményekkel foglalkozó gyorsreagálású csoportok” elnevezésű, közös operatív kiberkapacitás létrehozása terén, aminek a célja, hogy elmélyítsék a kiberterületen folytatott önkéntes együttműködést kölcsönös segítségnyújtás formájában, többek között a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való reagálás terén is;

12. NYUGTÁZZA, hogy a bűnüldöző közösség tapasztalattal és a hét minden napján 24 órában rendelkezésre álló reagálási képességgel rendelkezik a határokon átnyúló jelentős kibertámadások elhárítása érdekében – az uniós bűnüldözési vészhelyzet-elhárítási protokoll keretében – folytatott operatív együttműködés és biztonságos információcsere terén;

13. ELISMERI a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretének (a „kiberdiplomáciai eszköztárnak”) a folyamatos alkalmazását. EMLÉKEZTET arra, hogy minden tagállam szabadon hozhatja meg saját szuverén döntését – eseti alapon – valamely rossz szándékú kibertevékenység attribúciójával kapcsolatban. EMLÉKEZTET arra, hogy a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretében hozott intézkedéseknek a tagállamok által elfogadott közös helyzetismereten kell alapulniuk. Az EU INTCEN kulcsszerepet tölt be mint olyan központ, amely helyzetismerettel és fenyegetésértékeléssel segíti az EU-t a kiberkérdésekkel kapcsolatban, a tagállamok önkéntes hírszerzési hozzájárulásai alapján és hatásköreik sérelme nélkül;

14. ÚJÓLAG HANGSÚLYOZZA a kölcsönös segítségnyújtás és szolidaritás fontosságát, összhangban az Európai Unióról szóló szerződés 42. cikkének (7) bekezdésével és az Európai Unió működéséről szóló szerződés 222. cikkével, és további, kiberdimenzióval bíró gyakorlatokat SÜRGET. EMLÉKEZTET arra, hogy át kell gondolni, hogy nagyszabású kiberbiztonsági események vagy válsághelyzetek esetén hogyan érdemes ötvözni az uniós kiberbiztonsági válságkezelési keretet, a kiberdiplomáciai eszköztárat és a fent említett cikkek rendelkezéseit. EMLÉKEZTET továbbá arra, hogy az Európai Unióról szóló szerződés 42. cikkének (7) bekezdéséből fakadó tagállami kötelezettségek nem sértik bizonyos tagállamok biztonság- és védelempolitikájának sajátos jellegét. EMLÉKEZTET emellett arra is, hogy továbbra is a NATO képezi a kollektív védelem alapját azon államok számára, amelyek NATO-tagok;

15. ELISMERI az EU és a NATO között a kibervédelem és -biztonság terén folytatott együttműködést – ideértve a CERT-EU és a NATO kiberbiztonsági eseményeket kezelő képessége (NCIRC) közötti információmegosztást is –, amely az átláthatóság, a kölcsönösség és az inkluzivitás elveinek, valamint a két szervezet döntéshozatali autonómiájának a teljes körű tiszteletben tartása mellett megy végbe;

16. ELISMERI a magánszektorral való együttműködés fontosságát a megfelelő esetekben, az információmegosztás, a szükséges szakértelem, valamint a megbízható megoldások és szolgáltatások biztosítása terén, többek között például a kiberbiztonsági eseményekre való reagálás támogatása és a különböző kiberközösségek között a helyzetismeret javítása céljából;

17. HANGSÚLYOZZA a minősített és érzékeny információk cseréjére igénybe vett kommunikációs csatornák biztonságosságának fontosságát. RÁMUTAT, hogy további előrelépésre van szükség;

E tekintetben és a fentiek figyelembevételével,

18. ELISMERI, hogy a közös kiberbiztonsági egység létrehozásáról szóló bizottsági ajánlás olyan kezdeményezés, amelyet az uniós kiberbiztonsági válságkezelési keret továbbfejlesztése során figyelembe kell venni[15];

19. FELSZÓLÍTJA az EU-t és tagállamait, hogy a már meglévő mechanizmusokra és elért eredményekre építve folytassák az átfogóbb és hatékonyabb uniós kiberbiztonsági válságkezelési keret kialakítására irányuló erőfeszítéseiket, és gondolják át, milyen lehetőségek rejlenek a közös kiberbiztonsági egységre irányuló kezdeményezésben e mechanizmusok – fokozatos megközelítés keretében való – kiegészítésére. HANGSÚLYOZZA, hogy a bizalom növeléséhez csak egy fokozatos, átlátható és inkluzív folyamat vezethet el, amely éppen ezért kritikus fontosságú az uniós kiberbiztonsági válságkezelési keret továbbfejlesztése szempontjából. E folyamat során tiszteletben kell tartani a tagállamok és az uniós intézmények, szervek és hivatalok meglévő szerepét, hatásköreit és megbízatását, valamint az e következtetésekben megállapított elveket, ideértve az arányosságot, a szubszidiaritást, az inkluzivitást, a kiegészítő jelleget, az átfedések elkerülését és az információk bizalmas jellegét. HANGSÚLYOZZA ugyanakkor, hogy a tagállamoknak az esetleges közös kiberbiztonsági egységben való részvétele vagy az ahhoz való hozzájárulásuk önkéntes lehetőség;

[15] C(2021)4520 final (11155/21 és 11155/21 ADD1).

20. HANGSÚLYOZZA, hogy annak érdekében, hogy valamennyi tagállam részt vehessen az uniós kiberbiztonsági válságkezelési kerettel – többek között az előirányzott közös kiberbiztonsági egységre irányuló kezdeményezéssel – kapcsolatos tanácskozásokban, annak fejlesztésében és a hatékony döntéshozatali folyamatokban, megfelelő munkamódszereket és irányítási struktúrát kell kialakítani. A Tanács Szerződések szerinti előjogainak és a lojális együttműködés elvének tiszteletben tartására SZÓLÍT FEL;

21. KIEMELI annak fontosságát, hogy az EU-n és tagállamain belüli valamennyi érintett kiberközösséget feltérképezzük és bevonjuk a munkába, figyelembe véve a nagyszabású kiberbiztonsági események és válsághelyzetek tekintetében betöltött eltérő szerepüket és felelősségi körüket. ALÁHÚZZA, hogy az uniós kiberbiztonsági válságkezelési keret továbbfejlesztése terén a Tanács – különösen a kiberkérdésekkel foglalkozó horizontális munkacsoport révén – döntő szerepet játszik a szakpolitikai döntéshozatal és a koordináció tekintetében. FELKÉRI ezért a tagállamokat, a Bizottságot, az Európai Külügyi Szolgálatot (EKSZ), az EU INTCEN-t, a CERT-EU-t, az ENISA-t, az Europolt (EC3), az Eurojustot (EJCN), az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontot (ECCC), valamint a CSIRT-hálózat, a CyCLONe, a Kiberbiztonsági Együttműködési Csoport, az EDA és a releváns PESCO-projektek képviselőit és más lehetséges érdekelt feleket, hogy vegyenek részt ebben a folyamatban. Megfontolandó a bizottsági ajánlásban foglalt azon javaslat, hogy jöjjön létre egy munkacsoport, mely ideiglenes fórumként szolgálna a tagállamokon és az Unión belüli minden érintett kiberközösség képviselői számára; e munkacsoport keretében biztosítani kellene az összes tagállam megfelelő képviseletét, és annak a Tanács politikai iránymutatását követve kellene eljárnia. E munkacsoportnak rendszeresen jelentést kellene tennie a tevékenységeiről, és esetlegesen javaslatokat kellene benyújtania a Tanácshoz megvitatás, jóváhagyás és további iránymutatás céljából. Ezen túlmenően a párbeszéd más formáit is ki lehetne alakítani a közösségeken belül és között, egyebek mellett műhelytalálkozók, szemináriumok, közös képzések és gyakorlatok keretében;

22. RÁMUTAT az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak (ECCC) és a nemzeti koordinációs központok hálózatának a potenciális közös kiberbiztonsági egységgel kapcsolatban betöltendő szerepére, különös tekintettel azon szerepre, hogy a kiberbiztonság területén számottevően növelje az Unió technológiai kapacitásait, technológiai megoldásait, képességeit és készségeit;

23. FELKÉRI az EU-t és tagállamait, hogy vegyenek részt az uniós kiberbiztonsági válságkezelési keret továbbfejlesztésében, többek között azáltal, hogy feltérképezik a közös kiberbiztonsági egységre irányuló kezdeményezésben rejlő lehetőségeket, kijelölik és meghatározzák a folyamatot, beleértve a mérföldköveket és az ütemtervet, valamint tisztázzák a célokat és a lehetséges szerepeket és felelősségi köröket. HANGSÚLYOZZA, hogy elsődleges fontosságú az egyes közösségeken belül kialakult hálózatok és kapcsolatok megszilárdítása, valamint hogy alaposan fel kell térképezni a kiberközösségeken belüli és közötti, valamint az európai intézményeken, szerveken és hivatalokon belüli és azok közötti információmegosztási hiányosságokat és szükségleteket, és ezt követően meg kell állapodni a potenciális közös kiberbiztonsági egység lehetséges elsődleges célkitűzéseiről és prioritásairól. A végkimenetel megelőlegezése nélkül HANGSÚLYOZZA, hogy az információmegosztási szükségletek meghatározására kell összpontosítani annak érdekében, hogy közös helyzetismeret alakulhasson ki az összes érintett közösség között. Az információmegosztási hiányosságok és szükségletek megállapításakor – többek között a virtuális platformok lehetséges használatának tekintetében is – továbbra is kellő figyelmet kell fordítani a minősített és érzékeny információk cseréjére szolgáló biztonságos kommunikációs csatornákra, ugyanakkor HANGSÚLYOZZA a már meglévő infrastruktúra használatának fontosságát. A fokozatos megközelítés bevezetésének célja, hogy kialakuljon a bizalom, valamint megteremtődjön a felkészültség és az operatív együttműködés fokozásával kapcsolatos lehetséges további lépések alapja. TISZTÁBAN VAN AZZAL, hogy különböző célkitűzések különböző megoldásokat, illetve az Unión és tagállamain belüli érintett kiberközösségek különböző képviselőinek bevonását tehetik szükségessé;

24. A teljes folyamat során az előirányzott közös kiberbiztonsági egység jogalapjának további vizsgálatára SZÓLÍT FEL, többek között az egység feladatainak és szerepének az értékelésére az ajánlásban az ENISA-ra ruházott feladatokhoz és szerepekhez viszonyítva, a 2019. április 17-i (EU) 2019/881 európai parlamenti és tanácsi rendelet 7. cikkének fényében. A közös kiberbiztonsági egységről szóló ajánlás egyes elemeinek további vizsgálatát SÜRGETI, ideértve az uniós kiberbiztonsági gyorsreagálású csoportokra vonatkozó elképzelést, valamint a kiberbiztonsági események és válságok elhárítására irányuló uniós tervet. HANGSÚLYOZZA, hogy a lehetséges közös kiberbiztonsági egységnek tiszteletben kell tartania a lehetséges jövőbeli résztvevők hatásköreit, megbízatásait és jogköreit;

25. FELSZÓLÍTJA az EU-t és tagállamait, hogy vizsgálják meg a közös kiberbiztonsági egységre irányuló kezdeményezésben rejlő lehetőségeket – az uniós intézmények, szervek és hivatalok nézőpontjából is – a tagállamok szintjén folytatott erőfeszítések kiegészítése érdekében. ÜDVÖZLI a Bizottság azon szándékát, hogy az uniós intézmények, szervek és hivatalok számára kötelező közös kiberbiztonsági szabályokról szóló, a közeljövőben benyújtandó rendeletjavaslata révén megerősítse az érintett uniós intézmények, szervek és hivatalok rezilienciáját;

26. Végezetül, ÚJÓLAG MEGERŐSÍTI elkötelezettségét a kiberreziliencia fokozása és az uniós kiberbiztonsági válságkezelési keret továbbfejlesztése iránt, és RENDSZERESEN NYOMON FOGJA KÖVETNI az elért előrehaladást, illetve további iránymutatást fog nyújtani az uniós kiberbiztonsági válságkezelési keret kiegészítéséhez.