Az Európai Unió
Tanácsa

Brüsszel, 2022. december 9.
(OR. en)

15623/22

Intézményközi referenciaszám:
2022/0338(NLE)

PROCIV 149	**ATO 102**
ENV 1248	**CSC 561**
JAI 1617	**ECOFIN 1279**
SAN 650	**CSCI 189**
COSI 315	**DATAPROTECT 346**
CHIMIE 100	**MI 912**
ENFOPOL 619	**CODEC 1916**
RECH 645	**COPS 581**
CT 220	**JAIEX 103**
DENLEG 93	**COPEN 430**
COTER 297	**IND 533**
RELEX 1657	**POLMIL 297**
ENER 654	**IPCR 116**
HYBRID 116	**DIGIT 231**
TRANS 768	**DISINFO 102**
CYBER 397	**CSDP/PSDC 848**
TELECOM 512	**MARE 71**
ESPACE 125	**POLMAR 78**

AZ ELJÁRÁS EREDMÉNYE

Küldi:	a Tanács Főtitkársága
Címzett:	a delegációk
Előző dok. sz.:	13713/22, 15454/22
Tárgy:	A TANÁCS AJÁNLÁSA a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről

Mellékelten továbbítjuk a delegációknak a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről szóló tanácsi ajánlásnak a Tanács 2022. december 8-i, 3920. ülésén elfogadott szövegét.

MELLÉKLET

A TANÁCS (EU) 2022/… AJÁNLÁSA

(…)

a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről

(EGT-vonatkozású szöveg)

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unió működéséről szóló szerződésre és különösen annak 114. cikkére, valamint 292. cikkének első és második mondatára,

tekintettel az Európai Bizottság javaslatára,

mivel:

(1) A belső piac működésének biztosítása céljából valamennyi tagállamnak és az Unió egészének érdeke, hogy egyértelműen azonosítsa és megvédje az e piacon belül alapvető szolgáltatásokat nyújtó jelentős kritikus infrastruktúrákat – különösen a kulcsfontosságú ágazatokban, mint az energiaágazat, a digitális infrastruktúrák, a közlekedési ágazat és az űrágazat –, valamint a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrákat[1], amelyek zavarai jelentős hatással lehetnek más tagállamokra.

[1] A tagállamoknak a nemzeti gyakorlataiknak megfelelően kell értékelniük a jelentőséget, és ezt elvégezhetik – egyéb tényezők mellett – kockázatértékelés, valamint az esemény hatása és jellege alapján.

(2) Ezen ajánlás – mely egy nem kötelező erejű jogi aktus – bizonyítja a tagállamoknak az együttműködésre irányuló politikai akaratát, valamint az ajánlott – az Európai Bizottság elnöke által közreadott öt pontból álló tervben kiemelt – intézkedések iránti elkötelezettségüket, a tagállamok hatásköreinek teljes körű tiszteletben tartása mellett. Ezen ajánlás nem érinti a tagállamok alapvető nemzetbiztonsági, közbiztonsági, illetve védelmi érdekeinek védelmét, és egyik tagállammal szemben sem lehet elvárás az, hogy megosszon olyan információkat, amelyek károsak ezen érdekekre nézve.

(3) Bár a kritikus infrastruktúrák biztonságának és az általuk nyújtott alapvető szolgáltatásoknak a garantálása elsősorban a tagállamoknak és azok kritikusinfrastruktúra-üzemeltetőinek a felelőssége, az uniós szintű koordináció megerősítése helyénvaló, különösen az olyan folyamatosan változó fenyegetések fényében, amelyek egyidejűleg több tagállamot is érinthetnek – mint például Oroszország Ukrajna elleni agresszív háborúja, valamint a tagállamok ellen irányuló hibrid hadjáratok – vagy hatással lehetnek az Unió gazdaságának, belső piacának és teljes társadalmának a rezilienciájára és megfelelő működésére. Különös figyelmet kell fordítani a tagállamok területén kívül található kritikus infrastruktúrákra, például a tenger alatti kritikus infrastruktúrákra, illetve a tengeri energetikai infrastruktúrákra.

(4) Az Európai Tanács a 2022. október 20–21-i következtetéseiben határozottan elítélte a kritikus infrastruktúrák, például az Északi Áramlat földgázvezetékek ellen elkövetett szabotázscselekményeket, és kijelentette, hogy az Unió a kritikus infrastruktúrákat érintő, szándékosan előidézett zavarokra vagy az egyéb hibrid tevékenységekre egységes és határozott válaszintézkedésekkel fog reagálni.

(5) A gyorsan és folyamatosan változó fenyegetettségi helyzetre tekintettel prioritásnak minősül a rezilienciaerősítő intézkedések meghozatala a kulcsfontosságú ágazatokban – például az energiaágazatban, a digitális infrastruktúrák terén, a közlekedési ágazatban és az űrágazatban –, valamint a tagállamok által azonosított egyéb releváns ágazatokban. Az ilyen intézkedések középpontjában a kritikus infrastruktúrák rezilienciája erősítésének kell állnia, és figyelembe kell venni a releváns kockázatokat, különösen az áttételes hatásokat, az ellátási láncok zavarait, a függőséget, az éghajlatváltozás hatásait, a nem megbízható értékesítőket és partnereket, valamint a hibrid fenyegetéseket és hadjáratokat, beleértve a külföldi információmanipulációt és beavatkozást is. A nemzeti kritikus infrastruktúrák esetében, tekintettel a lehetséges következményekre, prioritásként kell kezelni a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrákat. A Tanács ösztönzi a tagállamokat, hogy – a folyamatosan alakuló jogi keretben meghatározott megközelítés fenntartása mellett és adott esetben sürgősen – hozzák meg ezeket a rezilienciaerősítő intézkedéseket.

(6) Az európai kritikus infrastruktúrák védelmét az energiaágazatban és a közlekedési ágazatban jelenleg a 2008/114/EK tanácsi irányelv[2] szabályozza, az uniós hálózati és információs rendszerek biztonságát pedig az (EU) 2016/1148 európai parlamenti és tanácsi irányelv[3] szavatolja, mely a kibertérben megjelenő fenyegetésekre összpontosít. A kritikus infrastruktúrák, a kiberbiztonság és a pénzügyi piac egységesen magasabb szintű rezilienciájának és védelmének biztosítása céljából a meglévő jogi keret módosításra és kiegészítésre kerül, mégpedig a kritikus fontosságú szervezetekre vonatkozó új szabályok (a CER-irányelv), a kiberbiztonságnak az egész Unióban biztosítandó egységesen magas szintjére vonatkozó megerősített szabályok (a NIS 2-irányelv) és a pénzügyi ágazat digitális működési rezilienciájára vonatkozó új szabályok (a DORA-rendelet) elfogadása által.

(7) A tagállamoknak – az uniós és a nemzeti joggal összhangban – minden rendelkezésre álló eszközt fel kell használniuk az előrelépés és a fizikai és a kiberreziliencia megerősítése érdekében. E tekintetben a „kritikus infrastruktúrák” alatt értendők a tagállamok által nemzeti szinten azonosított, illetve a 2008/114/EK irányelv értelmében európai kritikus infrastruktúraként kijelölt jelentős kritikus infrastruktúrák, továbbá a CER-irányelv értelmében azonosítandó kritikus fontosságú szervezetek, illetve adott esetben a NIS 2-irányelv hatálya alá tartozó szervezetek. A reziliencia fogalmát úgy kell érteni mint a kritikus infrastruktúra megelőzésre, védekezésre, reagálásra, ellenállásra, enyhítésre, elnyelésre, alkalmazkodásra vagy helyreállításra való képességét az olyan események összefüggésében, amelyek jelentősen megzavarják vagy megzavarhatják az alapvető szolgáltatások – azaz a létfontosságú társadalmi és gazdasági funkciók, a közvédelem és a közbiztonság, a népegészség vagy a környezet fenntartása szempontjából kulcsfontosságú szolgáltatások – nyújtását a belső piacon.

---

2 A Tanács 2008/114/EK irányelve (2008. december 8.) az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről (HL L 345., 2008.12.23., 75. o.).

3 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről (HL L 194., 2016.7.19., 1. o.).

(8) Ahhoz, hogy össze lehessen hangolni azt a munkát, amely a kritikus infrastruktúrák – kritikus fontosságú szervezetekre vonatkozó új szabályok révén megvalósítandó – egységesen magasabb szintű rezilienciájának és védelmének az elérésére irányul, a nemzeti szakértők összefogására van szükség. Ezen összehangolt munka lehetővé tenné a tagállamok közötti együttműködést és az olyan tevékenységekkel kapcsolatos információmegosztást, mint a kritikus infrastruktúrák által nyújtott alapvető szolgáltatások azonosítására szolgáló módszertanok kidolgozása. A Bizottság már megkezdte a szakértői találkozók szervezését és munkájuk elősegítését, és a továbbiakban is folytatni kívánja ezt a munkát. Miután a CER-irányelv hatályba lépett és az irányelv értelmében megalakult a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport, a csoportnak – a feladataival összhangban – folytatnia kell az előkészítő munkát.

(9) A megváltozott fenyegetettségi helyzet tudatában tovább kell fejleszteni a kritikus infrastruktúrák stressztesztjei nemzeti szintű elvégzésének a lehetőségeit, mivel az ilyen tesztek hasznosak lehetnek a kritikus infrastruktúrák rezilienciájának erősítése szempontjából. Tekintettel az energiaágazat különös jelentőségére, és az ágazatban esetlegesen bekövetkező zavaroknak az Unió egészét érintő következményeire, ezen ágazat számára az járhat a legtöbb előnnyel, ha a stressztesztek közösen elfogadott elvek alapján végzik. Az ilyen stressztesztek a tagállamok hatáskörébe tartoznak, akiknek ösztönözniük kell a kritikus infrastruktúrák üzemeltetőit ilyen stressztesztek végzésére, és támogatniuk kell őket abban, amennyiben ezeket előnyösnek, valamint a nemzeti jogi keretükkel összhangban állónak értékelik.

(10) A jelenlegi és a várhatóan bekövetkező fenyegetésekre való összehangolt és hatékony reagálás biztosítása érdekében a Tanács ösztönzi a Bizottságot, hogy biztosítson további támogatást a tagállamoknak, különösen azáltal, hogy releváns információkat nyújt tájékoztatók, nem kötelező erejű kézikönyvek és iránymutatások formájában. Az Európai Külügyi Szolgálatnak (EKSZ) – különösen az Európai Unió Helyzetelemző Központján és annak a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoportján keresztül, az Európai Unió Katonai Törzse (EUKT) Hírszerzési Igazgatóságának támogatásával, az egységes információelemzési kapacitás (SIAC) kerete alapján – fenyegetésértékeléseket kell készítenie. A Tanács továbbá felkéri a Bizottságot, hogy a tagállamokkal együttműködésben mozdítsa elő az uniós finanszírozású kutatási és innovációs projektekben való részvételt.

(11) A fizikai és a digitális infrastruktúra egyre nagyobb mértékű kölcsönös függőségéből adódóan a kritikus területeket célba vevő, rossz szándékú kibertevékenységek zavart vagy kárt okozhatnak a fizikai infrastruktúrában, a fizikai infrastruktúra elleni szabotázs pedig hozzáférhetetlenné teheti a digitális szolgáltatásokat. A Tanács felkéri a tagállamokat, hogy gyorsítsák fel a kritikus fontosságú szervezetekre alkalmazandó új jogi keret és a kiberbiztonságra vonatkozó megerősített jogi keret átültetésének és alkalmazásának előkészítésére irányuló munkát, mégpedig az (EU) 2016/1148 irányelvvel létrehozott együttműködési csoportban (a továbbiakban: Kiberbiztonsági Együttműködési Csoport) szerzett tapasztalatokra építve és a lehető leghamarabb, szem előtt tartva az átültetésre vonatkozó határidőket és azt, hogy az említett előkészítő munkának párhuzamosan és koherens módon kell előrehaladnia.

(12) A felkészültség fokozása mellett fontos megerősíteni azokat a képességeket is, amelyek lehetővé teszik a gyors és hatékony reagálást a kritikus infrastruktúra által nyújtott alapvető szolgáltatásokban bekövetkező zavar esetén. Ezen ajánlás ezért uniós és tagállami szinten egyaránt meghozandó intézkedéseket tartalmaz, kiemelve többek között azt a támogató szerepet és hozzáadott értéket, mely a megerősített együttműködésnek és információcserének az 1313/2013/EU európai parlamenti és a tanácsi határozattal[4] létrehozott uniós polgári védelmi mechanizmus (UCPM) keretében történő bevezetése, valamint az (EU) 2021/696 európai parlamenti és tanácsi rendelettel[5] létrehozott uniós űrprogram releváns eszközeinek a felhasználása révén érhető el.

(13) A Bizottságnak, az Unió külügyi és biztonságpolitikai főképviselőjének (a továbbiakban: a főképviselő) és a Kiberbiztonsági Együttműködési Csoportnak az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a már működő hálózatokkal – köztük az Európai Kiberválságügyi Kapcsolattartó Szervezetek Hálózatával (EU-CyCLONe) – együttműködve kockázatértékelést kell végeznie, valamint kockázati forgatókönyveket kell kidolgoznia. A nevers-i közös miniszteri felhívás folyományaképp ezen a kockázatértékelésen dolgozik jelenleg a Kiberbiztonsági Együttműködési Csoport a Bizottság és az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) támogatásával, valamint az Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben. Ez a két feladat következetesen és összehangoltan fog igazodni a Bizottság és a tagállamok által jelenleg kidolgozás alatt álló, az UCPM keretében zajló forgatókönyv-kidolgozási munkához, többek között a kiberbiztonsági események és azok tényleges hatásai tekintetében. A hatékonyság, az eredményesség és a következetesség érdekében, valamint ezen ajánlás megfelelő végrehajtása céljából nemzeti szinten tükröződniük kell az említett feladatok elvégzése során kapott eredményeknek.

---

4 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.).

5 Az Európai Parlament és a Tanács (EU) 2021/696 rendelete (2021. április 28.) az uniós űrprogram és az Európai Unió Űrprogramügynökségének a létrehozásáról, valamint a 912/2010/EU, az 1285/2013/EU és a 377/2014/EU rendelet és az 541/2014/EU határozat hatályon kívül helyezéséről (HL L 170., 2021.5.12., 69. o.).

(14) A nagyszabású kiberbiztonsági eseményekre való felkészültség és reagálási képesség azonnali megerősítése érdekében a Bizottság létrehozott egy rövid távú programot, amely az ENISA számára elkülönített további finanszírozás révén támogatást nyújt a tagállamoknak. A javasolt szolgáltatások között szerepelnek többek között felkészültségi intézkedések, például a szervezeteknél végzett behatolási tesztelés, melynek célja a sebezhetőségek azonosítása. A program emellett bővebb lehetőségeket biztosíthat a tagállamoknak való segítségnyújtásra a kritikus fontosságú szervezeteket érintő nagyszabású biztonsági események esetén. Ez egy első lépést jelent az Európai Unió kiberbiztonsági helyzetének javításáról szóló, 2022. május 23-i tanácsi következtetésekkel (a továbbiakban: az EU kiberbiztonsági helyzetéről szóló tanácsi következtetések) összhangban, amely következtetésekben a Tanács felszólította a Bizottságot, hogy terjesszen elő javaslatot egy kiberbiztonsági vészhelyzeti alapra vonatkozóan. A tagállamoknak az alkalmazandó követelményekkel összhangban teljes mértékben ki kell használniuk ezeket a lehetőségeket, és a Tanács arra ösztönzi őket, hogy folytassák a munkát az uniós kiberválság-kezelés területére vonatkozóan, különösen azáltal, hogy rendszeresen figyelemmel kísérik és áttekintik a Tanács keretében a közelmúltban kidolgozott kiberválság-kezelési ütemterv végrehajtásában elért eredményeket. Az említett ütemterv egy dinamikusan változó dokumentum, amelyet szükség szerint újra kell vizsgálni és aktualizálni kell.

(15) A tenger alatti kommunikációs kábelek globális hálózata alapvető fontosságú a globális és az EU-n belüli összekapcsoltság szempontjából. Mivel az ilyen kábelek rendkívül hosszúak és a tengerfenéken futnak, a legtöbb kábelszakasz esetében különösen nagy kihívást jelent a víz alatti vizuális felügyelet. A megosztott joghatóság és az ilyen kábelekkel kapcsolatos egyéb joghatósági nehézségek egyedi esetet képeznek, amely európai és nemzetközi együttműködést kíván az infrastruktúra védelmével és helyreállításával kapcsolatban. Ezért azokat a folyamatban lévő és tervezett kockázatértékeléseket, amelyek a digitális szolgáltatások alapját adó digitális és fizikai infrastruktúrára vonatkoznak, ki kell egészíteni a tenger alatti kommunikációs kábelekkel kapcsolatos külön kockázatértékeléssel és kockázatcsökkentő intézkedésekkel. A tagállamok felkérik a Bizottságot, hogy dolgozzon ki tanulmányokat e célból, és megállapításait ossza meg a tagállamokkal.

16. Az energia- és közlekedési ágazatot szintén érinthetik digitális infrastruktúrával kapcsolatos fenyegetések – például a digitális összetevőket tartalmazó energetikai technológiákkal összefüggésben. Az alapvető szolgáltatások folyamatossága és az energiaágazatbeli kritikus infrastruktúrák stratégiai ellenőrzése szempontjából fontos tényező a kapcsolódó ellátási láncok biztonsága. Ezeket a körülményeket figyelembe kell venni azon intézkedések meghozatalakor, amelyek ezen ajánlással összhangban a kritikus infrastruktúra rezilienciájának fokozására irányulnak.

17. Mivel a biztonsággal kapcsolatos tevékenységek szempontjából az űrinfrastruktúra, az űrtechnológiai eszközök földi elemei – többek között a különböző termelőlétesítmények –, valamint az űralapú szolgáltatások egyre növekvő jelentőségre tesznek szert, elengedhetetlenül fontos biztosítani az uniós űrtechnológiai eszközöknek és szolgáltatásoknak – valamint azok földi elemeinek – a védelmét és rezilienciáját az Unión belül. Ugyanezen okokból alapvető fontosságú ezen ajánlás keretében is, hogy strukturáltabban történjen azon űralapú adatok és szolgáltatások hasznosítása, amelyeket az űrrendszerek, valamint a más ágazatok kritikus infrastruktúrájának megfigyelését, nyomon követését és védelmét szolgáló programok biztosítanak. A hamarosan elfogadásra kerülő uniós biztonsági és védelmi űrstratégia megfelelő intézkedéseket fog javasolni e tekintetben, amelyeket figyelembe kell venni ezen ajánlás végrehajtása során.

18. A kritikus – többek között a nemzetközi vizeken üzemelő – infrastruktúrák rezilienciáját érintő kockázatok eredményes kezeléséhez nemzetközi szintű együttműködésre is szükség van. Ezért a Tanács felkéri a tagállamokat, hogy működjenek együtt a Bizottsággal és a főképviselővel annak érdekében, hogy sor kerüljön bizonyos lépésekre ezen együttműködés megvalósítása céljából, szem előtt tartva, hogy bármely ilyen jellegű lépés csak az uniós jog – különösen a Szerződések külkapcsolatokra vonatkozó rendelkezései – értelmében a tagállamokat terhelő feladatokkal és felelősségekkel összhangban tehető meg.

19. A Bizottság, amint azt „A Bizottság hozzájárulása az európai védelemhez” című, 2022. február 15-i közleményében leszögezte, „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” című cselekvési terv megvalósítása érdekében a főképviselővel és a tagállamokkal együttműködésben értékelni fogja az ágazati hibrid reziliencia alapértékeit, és ennek keretében azonosítani fogja a hiányosságokat és a szükségleteket, valamint az azok 2023-ig történő kezelése érdekében megteendő lépéseket. Az említett kezdeményezésnek információkkal kell szolgálnia az ezen ajánlás keretében folyó munkához, elősegítve a reziliencia – így többek között a kritikus infrastruktúrák rezilienciája – további megerősítésével kapcsolatos információmegosztás javítását és az ezt célzó intézkedések jobb összehangolását.

20. A 2014. évi uniós tengeri védelmi stratégia és az ahhoz kapcsolódó módosított cselekvési terv a kritikus tengeri infrastruktúrák – többek között a víz alatti, és különösen a tengeri közlekedési, energetikai és kommunikációs infrastruktúra – fokozott védelmét sürgette, többek között a tengerészeti ágazattal kapcsolatos tudatosságnak a jobb interoperabilitás és az észszerűbb (kötelező és önkéntes) információcsere révén történő javításával. Jelenleg folyamatban van az említett stratégia és cselekvési terv aktualizálása, melynek nyomán az ki fog bővülni a kritikus tengeri infrastruktúra védelmét célzó megerősített intézkedésekkel. Az említett intézkedéseknek ki kell majd egészíteniük ezt az ajánlást.

21. A kritikus infrastruktúrák rezilienciájának megerősítése hozzájárul azokhoz a szélesebb körű erőfeszítésekhez, amelyek az Unióval és tagállamaival szembeni hibrid fenyegetések és hadjáratok elleni fellépésre irányulnak. Ez az ajánlás épít „A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz” című, az Európai Parlamentnek és a Tanácsnak címzett közös közleményben foglaltakra. A közös keret 1. intézkedése – nevezetesen a hibrid kockázatokra vonatkozó felmérés – kulcsfontosságú szerepet játszik a nemzeti és a páneurópai struktúrákat és hálózatokat potenciálisan érintő sebezhetőségek azonosításában. Emellett a hibrid hadjáratokra való koordinált uniós reagálásra vonatkozó keretről szóló, 2022. június 21-i tanácsi következtetések végrehajtása – az uniós hibrid eszköztár valamennyi érintett területen történő alkalmazása révén – lehetővé fogja tenni az erőteljesebb koordinált fellépést.

ELFOGADTA EZT AZ AJÁNLÁST:

I. FEJEZET: CÉL, ALKALMAZÁSI KÖR ÉS A PRIORITÁSOK MEGHATÁROZÁSA

1. Ez az ajánlás egy sor olyan célzott uniós és nemzeti szintű intézkedést határoz meg, amelynek célja a kritikus infrastruktúrák rezilienciájának önkéntes alapon történő támogatása és fokozása, és amelyek középpontjában a számottevő határokon átnyúló jelentőséggel bíró, illetve az egyes meghatározott kulcsfontosságú ágazatokbeli kritikus infrastruktúrák – például az energetikai infrastruktúrák, a digitális infrastruktúrák, a közlekedési infrastruktúrák és az űrinfrastruktúrák – állnak. Az említett célzott intézkedések a felkészültség és a reagálás megerősítésére, valamint nemzetközi együttműködésre irányulnak.

2. Az ezen ajánlásban foglalt célok megvalósítása érdekében megosztott, az uniós és a nemzeti szabályok, valamint az üzleti titoktartásra vonatkozó szabályok értelmében bizalmasnak minősülő információkat csak abban az esetben kell megosztani a Bizottsággal és más érintett hatóságokkal, ha ez az információmegosztás ezen ajánlás megfelelő alkalmazásához szükséges. Ez az ajánlás nem érinti a tagállamok alapvető nemzetbiztonsági, közbiztonsági, illetve védelmi érdekeinek védelmét, és egyik tagállammal szemben sem elvárás az, hogy megosszon olyan információkat, amelyek ellentétesek ezen érdekekkel.

II. FEJEZET FOKOZOTT FELKÉSZÜLTSÉG

Tagállami szintű intézkedések

3. A tagállamoknak kockázatértékeléseik vagy meglévő egyenértékű elemzéseik aktualizálása során mérlegelniük kell az összes veszélyre kiterjedő megközelítés alkalmazásának lehetőségét, összhangban a kritikus infrastruktúráikat fenyegető aktuális veszélyek változó jellegével – különösen az azonosított kulcsfontosságú ágazatokban –, és ha lehetséges, a kritikus fontosságú szervezetekre alkalmazandó, készülő új jogi keret hatálya alá tartozó valamennyi ágazatban.

4. A Tanács felkéri a tagállamokat, hogy a kritikus fontosságú szervezetekre alkalmazandó, rövidesen elfogadandó jogi keretnek megfelelően – amennyiben lehetséges – gyorsítsák fel az előkészítő munkát és fogadjanak el rezilienciát fokozó intézkedéseket, kiemelt figyelmet fordítva a számottevő határokon átnyúló jelentőséggel bíró kritikus fontosságú szervezetek azonosításával, valamint az azonosított kritikus fontosságú szervezetek rezilienciájának javítása érdekében nyújtott támogatás fokozásával kapcsolatos, egyfelől a tagállamok közötti, másfelől a Bizottsággal történő együttműködésre és releváns információmegosztásra.

5. A tagállamoknak támogatniuk kell a szakértők képzését és gyakorlatait, valamint a bevált gyakorlatok és a levont tanulságok szakértők közötti megosztását. A tagállamoknak ösztönözniük kell a szakértőket a meglévő nemzeti és nemzetközi képzési platformokon való részvételre, például az uniós polgári védelmi mechanizmus keretében.

6. A tagállamoknak ösztönözniük és támogatniuk kell legalább az energiaágazatbeli kritikus infrastruktúrák üzemeltetőit abban, hogy – amennyiben ez előnyös – az uniós szinten közösen elfogadott elveket követve stressztesztek végezzenek. E stressztesztek során értékelni kell a kritikus infrastruktúra ember okozta ellenséges fenyegetésekkel szembeni rezilienciáját. Ezért a tagállamoknak törekedniük kell arra, hogy a lehető leghamarabb, de legkésőbb 2023 első negyedévének végéig azonosítsák a tesztelendő, érintett kritikus infrastruktúrákat, és konzultáljanak ezeknek a kritikus infrastruktúráknak az üzemeltetőivel. Emellett a tagállamoknak a nemzeti joggal összhangban támogatniuk kell a kritikus infrastruktúrák üzemeltetőit abban, hogy a lehető leghamarabb megkezdjék az említett teszteket, törekedve azok 2023 végéig történő lezárására. A Tanács 2023. április végéig értékelni kívánja a stressztesztekkel kapcsolatos helyzetet.

7. A kritikus infrastruktúrákat érintő, gyorsan változó fenyegetések miatt létfontosságú ezen infrastruktúrák magas szintű védelmének a fenntartása. A Tanács arra ösztönzi a tagállamokat, hogy különítsenek el elegendő pénzügyi forrást illetékes nemzeti hatóságaik kapacitásainak a megerősítésére, és biztosítsák számukra az ahhoz szükséges támogatást, hogy fokozni tudják a kritikus infrastruktúrák rezilienciáját. A Tanács arra bátorítja továbbá a tagállamokat, hogy különítsenek el elegendő pénzügyi forrást a nagyszabású kiberbiztonsági események kezeléséért felelős hatóságok számára azok támogatása érdekében, és biztosítsák, hogy a számítógép-biztonsági eseményekre reagáló csoportjaik (CSIRT) és illetékes hatóságaik teljes mértékben részt vegyenek a CSIRT-ek hálózatában, illetve az EU-CyCLONe-ban.

8. A Tanács felkéri a tagállamokat, hogy az alkalmazandó követelményekkel összhangban egyrészről maguk is használják fel az uniós kritikus infrastruktúrák rezilienciájának fokozása céljából az uniós és nemzeti szintű finanszírozási lehetőségeket, másrészről bátorítsák a kritikus infrastruktúrák üzemeltetőit is e finanszírozási lehetőségek igénybevételére, többek között például a transzeurópai hálózatoknak a jelentős fenyegetések teljes körével szembeni védelme érdekében, különösen az (EU) 2021/1149 európai parlamenti és tanácsi rendelettel[6] létrehozott Belső Biztonsági Alap, az 1301/2013/EU európai parlamenti és tanácsi rendelettel[7] létrehozott Európai Regionális Fejlesztési Alap, az UCPM és a Bizottság REPowerEU terve által finanszírozott programok keretében. A Tanács arra is ösztönzi a tagállamokat, hogy a lehető leghatékonyabban használják fel a kutatási programok – például az (EU) 2021/695 európai parlamenti és tanácsi rendelettel[8] létrehozott Horizont Európa – releváns projektjeinek eredményeit.

---

6 Az Európai Parlament és a Tanács (EU) 2021/1149 rendelete (2021. július 7.) a Belső Biztonsági Alap létrehozásáról (HL L 251., 2021.7.15., 94. o.).

7 Az Európai Parlament és a Tanács 1301/2013/EU rendelete (2013. december 17.) az Európai Regionális Fejlesztési Alapról és a „Beruházás a növekedésbe és munkahelyteremtésbe” célkitűzésről szóló egyedi rendelkezésekről, valamint az 1080/2006/EK rendelet hatályon kívül helyezéséről (HL L 347., 2013.12.20., 289. o.).

8 Az Európai Parlament és a Tanács (EU) 2021/695 rendelete (2021. április 28.) a Horizont Európa kutatási és innovációs keretprogram létrehozásáról, valamint részvételi és terjesztési szabályainak megállapításáról, továbbá az 1290/2013/EU és az 1291/2013/EU rendelet hatályon kívül helyezéséről (HL L 170., 2021.5.12., 1. o.).

(9) Ami az Unióban található kommunikációs és hálózati infrastruktúrát illeti, a Tanács felkéri a Kiberbiztonsági Együttműködési Csoportot, hogy – az (EU) 2016/1148 irányelv 11. cikkével összhangban eljárva – gyorsítsa fel a célzott kockázatértékelésre irányuló, a nevers-i közös miniszteri felhívás alapján jelenleg végzett munkáját, és a lehető leghamarabb terjessze elő az első ajánlásokat. Ebben a kockázatértékelésben információkkal kell szolgálni a kiberkockázatok folyamatban lévő ágazatközi értékeléséhez és a forgatókönyvekhez, amelyek kidolgozását a Tanács az Európai Unió kiberbiztonsági helyzetéről szóló tanácsi következtetésekben szorgalmazta. Biztosítani kell, hogy ez a munka koherensen és kiegészítő jelleggel illeszkedjen ahhoz a munkához, amelyet a Kiberbiztonsági Együttműködési Csoport az információs és kommunikációs technológiák ellátási láncának biztonságával kapcsolatban végez, valamint más érintett csoportok munkájához.

10. A Tanács felkéri továbbá a Kiberbiztonsági Együttműködési Csoportot, hogy – a Bizottság és az ENISA támogatásával – folytassa a digitális infrastruktúra biztonságával kapcsolatos munkáját, többek között a tenger alatti infrastruktúra, nevezetesen a tenger alatti kommunikációs kábelek tekintetében. Felkéri továbbá, hogy kezdje meg az űrágazattal kapcsolatos munkáját, mégpedig többek között azáltal, hogy szükség esetén olyan szakpolitikai iránymutatást és kiberbiztonsági kockázatkezelési módszereket dolgoz ki az űrágazati szereplők számára, amelyek az űralapú szolgáltatások nyújtását támogató földi infrastruktúra rezilienciájának növelését célozzák, és egy összes veszélyre kiterjedő megközelítésen és egy kockázatalapú megközelítésen alapulnak.

11. A tagállamoknak teljes mértékben ki kell használniuk a Bizottságnak az ENISA-val közösen végrehajtott rövid távú támogatási programjában kínált kiberbiztonsági felkészültségi szolgáltatásokat, például a sebezhetőségek azonosítására szolgáló behatolási tesztelést, és ezzel összefüggésben a Tanács arra ösztönzi a tagállamokat, hogy kezeljék prioritásként az energia-, a digitálisinfrastruktúra- és a közlekedési ágazatban kritikus infrastruktúrát üzemeltető szervezeteket.

12. A tagállamoknak teljes mértékben ki kell használniuk az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont (ECCC) jelentette lehetőségeket. A tagállamoknak ösztönözniük kell nemzeti koordinációs központjaikat, hogy az alapvető szolgáltatásokat nyújtó szereplők megfelelőbb támogatását célzó uniós és nemzeti szintű kapacitásépítés érdekében proaktívan működjenek együtt a kiberbiztonsági közösségük tagjaival.

13. Fontos, hogy a tagállamok sürgősen végrehajtsák az 5G kiberbiztonsággal kapcsolatos eszköztárban ajánlott intézkedéseket, és kiváltképp, hogy a tagállamok korlátozásokat léptessenek életbe a magas kockázatú beszállítók esetében, figyelembe véve, hogy az időveszteség növelheti az uniós hálózatok sebezhetőségét, továbbá fontos, hogy megerősítsék az 5G-hálózatok kritikus és érzékeny részeinek fizikai és nem fizikai védelmét, többek között szigorú hozzáférés-ellenőrzés révén. Emellett a tagállamoknak a Bizottsággal együttműködve fel kell mérniük, hogy szükség van-e kiegészítő intézkedésekre az 5G-hálózatok egységes szintű biztonságának és rezilienciájának biztosításához.

14. A tagállamoknak a Bizottsággal és az ENISA-val közösen az IKT-ellátási lánc biztonságáról szóló 2022. október 17-i tanácsi következtetések végrehajtására kell összpontosítaniuk.

15. A tagállamoknak figyelembe kell venniük a határokon átnyúló villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó, hamarosan hatályba lépő üzemi és kereskedelmi szabályzatot [...], az (EU) 2016/1148 irányelv végrehajtása során szerzett tapasztalatokra és a Kiberbiztonsági Együttműködési Csoport vonatkozó iránymutatásaira, és különösen az alapvető szolgáltatásokat nyújtó szereplőkre vonatkozó biztonsági intézkedésekről szóló referenciadokumentumára építve.

16. A tagállamoknak fejleszteniük kell a Kopernikusz, a Galileo és az európai geostacionárius navigációs lefedési szolgáltatás (EGNOS) megfigyelési célú használatát annak érdekében, hogy releváns információkat tudjanak megosztani a 15. pont szerint bevont szakértőkkel. Megfelelően ki kell használni a kritikus infrastruktúra megfigyelésére és a válságok előrejelzésének, valamint a válságokra való reagálásnak a támogatására szolgáló, az Unió űrprogramja keretében létrehozott állami műholdas kommunikációs program (GOVSATCOM) kínálta lehetőségeket.

Uniós szintű intézkedések

17. A kritikus infrastruktúra fizikai rezilienciájának megerősítése céljából, mindenekelőtt az alábbiak révén meg kell erősíteni tagállamok kijelölt szakértői közötti, valamint a Bizottsággal folytatott párbeszédet és együttműködést:

a) hozzájárulás a tagállamokat e reziliencia fokozásában támogató közös önkéntes eszközök – többek között módszertanok és kockázati forgatókönyvek – előkészítéséhez, kidolgozásához és népszerűsítéséhez;

b) a tagállamok támogatása a kritikus fontosságú szervezetekre vonatkozó új jogi keret végrehajtásában, többek között a Bizottság arra való ösztönzésével, hogy időben fogadja el a felhatalmazáson alapuló jogi aktust;

c) a 6. pontban említett stressztesztek közös elvek alapján történő elvégzésének támogatása, kezdve az energiaágazatot érintő, ellenséges, ember okozta fenyegetésekre összpontosító tesztekkel, majd folytatva a más kulcsfontosságú ágazatokat érintő ilyen tesztekkel, továbbá egy tagállam kérésére az ilyen stressztesztek elvégzésével kapcsolatos támogatás és tanácsadás;

d) a Bizottság általi létrehozását követően bármely biztonságos platform biztosítása a bevált gyakorlatok, a nemzeti tapasztalatokból levont tanulságok és az ilyen jellegű rezilienciával kapcsolatos egyéb információk önkéntes jellegű összegyűjtéséhez, számbavételéhez és megosztásához.

E kijelölt szakértők munkája során különleges figyelmet kell fordítani az ágazatközi függőségekre és a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrára, és e munka nyomán adott esetben a Tanácson és a Bizottságon belül további lépéseket kell tenni.

18. A Tanács ösztönzi a tagállamokat, hogy minden olyan támogatást használjanak ki, amelyet a Bizottság nyújt például kézikönyvek és iránymutatások – így a kritikus infrastruktúrák és nyilvános terek pilóta nélküli légijármű-rendszerekkel szembeni védelméről szóló kézikönyv –, valamint kockázatértékelési eszközök elkészítése révén. A Tanács felkéri az EKSZ-t, hogy a helyzetismeret javítása érdekében – különösen az Európai Unió Helyzetelemző Központján és annak hibrid fenyegetésekkel foglalkozó információs csoportján keresztül, továbbá az EUKT-nek az egységes információelemzési kapacitás (SIAC) keretébe tartozó Hírszerzési Igazgatósága támogatásával – tartson tájékoztatókat az Unió kritikus infrastruktúráit fenyegető veszélyekről.

19. A tagállamoknak támogatniuk kell a Bizottság által a kritikus infrastruktúrák rezilienciájával kapcsolatos, az uniós kutatási és innovációs programok keretében finanszírozott projektek eredményeinek alkalmazása érdekében végzett tevékenységeket. A Tanács nyugtázza a Bizottság azon szándékát, hogy a 2021–2027-es időszakra vonatkozó többéves pénzügyi keretben a Horizont Európa számára elkülönített költségvetésen belül növelje az ilyen jellegű reziliencia finanszírozását, mégpedig anélkül, hogy ez negatív hatást gyakorolna a Horizont Európa keretében a polgári biztonsággal kapcsolatos egyéb kutatási és innovációs projektek számára nyújtott finanszírozásra.

20. Az Európai Unió kiberbiztonsági helyzetéről szóló tanácsi következtetésekben szereplő megbízások alapján a Tanács felkéri a Bizottságot, a főképviselőt és a Kiberbiztonsági Együttműködési Csoportot, hogy az uniós jog szerinti feladataikkal és hatásköreikkel összhangban fokozzák az érintett hálózatokkal és polgári és katonai szervekkel és ügynökségekkel a kockázatértékelések elvégzése és a kiberbiztonsági kockázati forgatókönyvek kidolgozása terén folytatott munkát, figyelembe véve különösen az energia, a digitális infrastruktúra, a közlekedés és az űrinfrastruktúra jelentőségét, valamint az ágazatok és a tagállamok közötti kölcsönös függőségeket. Ennek során figyelembe kell venni az említett ágazatok alapját adó infrastruktúrát érintő kapcsolódó kockázatokat. Amennyiben ez hasznos, rendszeresen kockázatértékelést lehet végezni és forgatókönyveket lehet kidolgozni, de ügyelni kell arra, hogy e tevékenységek a szóban forgó ágazatokban már meglévő vagy tervezett kockázatértékeléseket kiegészítsék, azokra épüljenek és azokkal ne legyenek átfedésben, valamint hogy információval szolgáljanak azon megbeszélésekhez, amelyek témája, hogy miként lehet megerősíteni a kritikus infrastruktúrát üzemeltető szervezetek általános rezilienciáját és kezelni a sebezhetőségeket.

21. A Tanács felkéri a Bizottságot, hogy a kiberválság-kezelés szerinti vonatkozó feladataival összhangban gyorsítsa fel a nagyszabású kiberbiztonsági eseményekre való tagállami felkészültség és reagálás támogatását célzó tevékenységeit, így mindenekelőtt:

a) készítsen átfogó tanulmányt[9] a hálózat- és információbiztonság összefüggésében végzett releváns kockázatértékelések kiegészítése érdekében, amely tanulmányban számba veszi a tagállamokat, továbbá Európát a világ többi részével összekötő tenger alatti infrastruktúrát, nevezetesen a tenger alatti kommunikációs kábeleket, és a tanulmány megállapításait ossza meg a tagállamokkal;

b) a megerősített kiberbiztonsági jogi kerettel és más releváns alkalmazandó szabályokkal összhangban támogassa a tagállamoknak, valamint az uniós intézményeknek, szerveknek és ügynökségeknek a nagyszabású kiberbiztonsági eseményekre és a jelentős eseményekre való felkészültségét és az ezekre való reagálásukat[10];

c) a tagállamokkal folytatott megfelelő megbeszélések révén gyorsítsa fel a kiberbiztonsági vészhelyzeti alap fő koncepciójának kidolgozását.

22. A Tanács arra ösztönzi a Bizottságot, hogy fokozza az előretekintő megelőző intézkedésekkel kapcsolatos munkát, többek között az 1313/2013/EU határozat 6. és 10. cikke értelmében a tagállamokkal folytatott együttműködést, továbbá hogy vészhelyzeti tervezés formájában támogassa az Európai Veszélyhelyzet-reagálási Központnak a kritikus infrastruktúra zavaraira való operatív felkészültségét és reagálását; növelje a preventív megközelítésekre és a lakosság felkészültségére irányuló beruházásokat; valamint az uniós polgári védelmi tudáshálózat keretében növelje a kapacitásépítéssel kapcsolatos támogatást.

---

9 E tanulmányban fel kell térképezni ezen infrastruktúra kapacitásait és tartalékkapacitásait, a szolgáltatás rendelkezésre állását fenyegető sebezhetőségeket, veszélyeket és kockázatokat, a (transzatlanti) tenger alatti kábelek leállása által a tagállamokra és az Unió egészére gyakorolt hatásokat, valamint a kockázatcsökkentést, figyelembe véve az ilyen információk érzékenységét és azt, hogy ezeket védeni kell.

10 Különös figyelmet kell fordítani minden olyan tevékenységre is, amely a digitális működési rezilienciáról szóló új jogi szabályozással összhangban a határokon átnyúló olyan jelentős kiberbiztonsági események vagy kapcsolódó fenyegetések esetén uniós szintű koordinált reagálás előkészítésére irányul, amelyek rendszerszintű hatást gyakorolhatnak az Unió pénzügyi ágazatára.

23. A Bizottságnak elő kell mozdítania az Unió megfigyelési eszközeinek (Kopernikusz, Galileo és EGNOS) használatát a következők érdekében: a tagállamoknak a kritikus infrastruktúrák és adott esetben azok közvetlen környezetének megfigyeléséhez nyújtott támogatás, továbbá az Unió űrprogramja keretében biztosított egyéb megfigyelési lehetőségeknek – például a világűr-megfigyelés, valamint az uniós űrmegfigyelés és a Föld körüli pályán haladó objektumok nyomon követése keretének – támogatása.

24. A Tanács felkéri az uniós ügynökségeket és más érintett szerveket, hogy – adott esetben és megbízatásukkal összhangban – nyújtsanak támogatást a kritikus infrastruktúrák rezilienciájával kapcsolatos kérdésekben, különösen az alábbiak szerint:

a) a Bűnüldözési Együttműködés Európai Uniós Ügynöksége (Europol) nyújtson támogatást a határokon átnyúló bűnüldözési tevékenységekhez kapcsolódó információgyűjtés, bűnügyi elemzés és nyomozati támogatás terén, valamint adott esetben ossza meg az eredményeket a tagállamokkal;

b) az Európai Tengerészeti Biztonsági Ügynökség (EMSA) nyújtson támogatást az uniós tengerhasznosítási ágazat biztonságával és védelmével kapcsolatos ügyekben, beleértve a tengeri védelemmel és biztonsággal kapcsolatos tengerfelügyeleti szolgáltatásokat is;

c) az Európai Unió Űrprogramügynöksége (EUSPA) és az Európai Unió Műholdközpontja (SatCen) képes lehet segítséget nyújtani az uniós űrprogram keretében végzett műveletekhez;

d) a kiberbiztonsággal kapcsolatos tevékenységeket illetően az ECCC – akár az ENISA-val együttműködve – támogatást nyújthat a kiberbiztonsággal kapcsolatos innovációs és iparpolitikához.

III. FEJEZET: MEGERŐSÍTETT REAGÁLÁS

Tagállami szintű intézkedések

25. A Tanács felkéri a tagállamokat, hogy:

a) adott esetben továbbra is koordinálják reagálásukat, és továbbra is kísérjék figyelemmel a kritikus infrastruktúrák által nyújtott alapvető szolgáltatásokban bekövetkező akut zavarokra való ágazatközi reagálást. Ez a következők keretében végezhető: a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák zavaraira való koordinált reagálásról szóló jövőbeli terv; a politikai reagálás koordinálására szolgáló, már meglévő, politikai szintű integrált válságelhárítási mechanizmus (IPCR), amennyiben határokon átnyúló jelentőséggel bíró kritikus infrastruktúrákról van szó; az (EU) 2017/1584 bizottsági ajánlás[11] szerinti, a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre vonatkozó tervezet; az EU-CyCLONe; a hibrid hadjáratokra való koordinált uniós reagálás kerete és az uniós hibrid eszköztár hibrid fenyegetések és hadjáratok esetén; valamint a riasztási rendszer dezinformáció esetén;

b) fokozzák az UCPM-mel összefüggésben folytatott operatív szintű információcserét a Veszélyhelyzet-reagálási Koordinációs Központtal, egyrészt a korai előrejelzés javítása, másrészt a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák zavarai esetén az UCPM keretében való reagálásuk koordinálása érdekében, hogy ezáltal szükség esetén gyorsabban sor kerülhessen az Unió segítségével történő reagálásra;

c) fokozzák az említett jelentős zavarokra való reagálási felkészültségüket, adott esetben az a) pontban említett, már meglévő vagy még kialakítandó eszközökön keresztül;

[11] 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.).

d) működjenek közre az európai polgári védelmi eszköztár (ECPP) és a rescEU releváns reagálási képességeinek továbbfejlesztésében;

e) ösztönözzék a kritikus infrastruktúrák üzemeltetőit és a releváns tagállami hatóságokat arra, hogy fokozzák azon kapacitásaikat, amelyek révén gyorsan helyre tudják állítani az említett kritikus infrastruktúrák üzemeltetői által nyújtott alapvető szolgáltatások alapszintű biztosítását;

f) ösztönözzék a kritikus infrastruktúrák üzemeltetőit, hogy amennyiben a kritikus infrastruktúrájuk újjáépítésére kerül sor, azt úgy építsék meg – figyelembe véve az intézkedések arányosságát a kockázatértékelések és a költségek tekintetében –, hogy a rá veszélyt jelentő valamennyi jelentős kockázattal szemben a lehető leginkább reziliens legyen, beleértve a kedvezőtlen éghajlati forgatókönyveket is.

26. A Tanács felkéri a tagállamokat, hogy amennyiben lehetséges, a kiberbiztonsággal kapcsolatos megerősített jogi keretben előírtaknak megfelelően, gyorsítsák fel az előkészítő munkát azáltal, hogy – tekintettel a CSIRT-ek új feladataira, valamint az új ágazatokban tevékenykedő szervezetek megnövekedett számára – törekednek a tagállami CSIRT-ek képességeinek fokozására, megfelelő időben felülvizsgálják és naprakésszé teszik kiberbiztonsági stratégiáikat, valamint a lehető leghamarabb kiberbiztonsági eseményekre és válságokra vonatkozó nemzeti reagálási terveket fogadnak el, amennyiben még nem rendelkeznek ezekkel.

27. A Tanács felkéri a tagállamokat, hogy nemzeti szinten mérlegeljék, hogy melyek a leginkább releváns eszközök annak biztosítására, hogy az érintett érdekelt felek tudatában legyenek annak, hogy fokozni kell a kritikus infrastruktúrák rezilienciáját azáltal, hogy megbízható értékesítőkkel és partnerekkel működnek együtt. Fontos további kapacitásokba beruházni, különösen azokban az ágazatokban, amelyekben a jelenlegi infrastruktúra az élettartama végéhez közelít (például a tenger alatti kommunikációs kábelek infrastruktúrája), az alapvető szolgáltatások zavarok esetén való folyamatos nyújtásának biztosítása, valamint a nem kívánt függőségek csökkentése érdekében.

28. A Tanács arra ösztönzi a tagállamokat, hogy nemzeti szinten fordítsanak figyelmet a proaktív stratégiai kommunikációra a hibrid fenyegetések és hadjáratok elleni küzdelem összefüggésében, valamint tekintettel annak a lehetőségére, hogy az ellenfelek törekedhetnek a külföldi információmanipulációra és beavatkozásra, a kritikus infrastruktúrákat célzó incidensekkel kapcsolatos narratívák alakítása révén.

Uniós szintű intézkedések

29. A Tanács felkéri a Bizottságot, hogy szorosan működjön együtt a tagállamokkal a releváns szervek, eszközök és reagálási kapacitások továbbfejlesztése érdekében, azzal a céllal, hogy fokozza a kritikus infrastruktúrák által nyújtott releváns alapvető szolgáltatások jelentős zavarai által okozott azonnali és közvetett hatások kezelésére vonatkozó operatív felkészültséget, ideértve különösen az ECPP-n és a rescEU-n keresztül az UCPM vagy a hibrid fenyegetéseket kezelő jövőbeli uniós gyorsreagálású csapatok keretében rendelkezésre álló szakértőket és erőforrásokat.

30. A Tanács felkéri a Bizottságot, hogy figyelembe véve a változó fenyegetettségi helyzetet, a tagállamokkal együttműködve, az UCPM keretében:

a) folyamatosan elemezze és tesztelje a meglévő reagálási kapacitások megfelelőségét és operatív felkészültségét;

b) rendszeresen kísérje figyelemmel az ECPP és a rescEU kapacitásait, és azonosítsa az azokban mutatkozó potenciálisan jelentős reagálási képességbeli hiányosságokat;

c) tegye még intenzívebbé az ágazatközi együttműködést a megfelelő uniós szintű reagálás biztosítása érdekében, és egy vagy több tagállammal közösen szervezzen rendszeres képzést és gyakorlatokat ezen együttműködés tesztelésére;

d) fejlessze tovább az ERCC-t mint az érintett tagállamoknak nyújtott támogatás koordinálásáért felelős uniós szintű ágazatközi veszélyhelyzeti központot.

31. A Tanács elkötelezett amellett, hogy megkezdje a munkát egy olyan, a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák zavaraira való koordinált reagálásról szóló terv jóváhagyása érdekében, amely leírja és meghatározza az említett kritikus infrastruktúrákat érintő biztonsági eseményekre való reagálás terén a tagállamok, valamint az uniós intézmények, szervek, hivatalok és ügynökségek között megvalósuló együttműködés céljait és módjait. A Tanács várakozással tekint az elé, hogy a Bizottság benyújtsa az említett tervre vonatkozó tervezetét, a releváns uniós ügynökségek által nyújtott támogatásra és hozzájárulásokra építve. A tervnek teljes mértékben koherensnek és interoperábilisnak kell lennie a hibrid fenyegetésekkel szembeni fellépés felülvizsgált uniós operatív protokolljával (EU Playbook), valamint figyelembe kell vennie a nagyszabású határokon átnyúló kiberbiztonsági eseményekre és válsághelyzetekre való koordinált reagálásról szóló, már meglévő tervezetet[12] és az EU-CyCLONe-nak a NIS 2 irányelvben meghatározott megbízatását, továbbá el kell kerülnie a struktúrák és tevékenységek megkettőzését. Az említett tervnek teljeskörűen tiszteletben kell tartania a már meglévő IPCR-t a reagálás koordinálása érdekében.

[12] A Bizottság (EU) 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról.

32. A Tanács felkéri a Bizottságot, hogy folytasson konzultációt az érintett érdekelt felekkel és szakértőkkel a tenger alatti infrastruktúrákat érintő potenciális jelentős biztonsági eseményekkel kapcsolatos – a 20. pont a) alpontjában említett helyzetfelmérő tanulmánnyal együtt előterjesztendő – megfelelő intézkedésekről, valamint részletesebben dolgozza ki az 1313/2013/EU határozatban meghatározott vészhelyzeti tervezést, kockázati forgatókönyveket és uniós katasztrófavédelmi rezilienciacélokat.

IV. FEJEZET: NEMZETKÖZI EGYÜTTMŰKÖDÉS

Tagállami szintű intézkedések

33. A tagállamoknak – adott esetben és az uniós joggal összhangban – együtt kell működniük az érintett harmadik országokkal a számottevő határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák rezilienciáját érintő kérdésekben.

34. A Tanács arra ösztönzi a tagállamokat, hogy működjenek együtt a Bizottsággal és a főképviselővel annak érdekében, hogy hatékonyan tudják kezelni a nemzetközi vizeken található kritikus infrastruktúrákat érintő kockázatokat.

35. A Tanács felkéri a tagállamokat, hogy a Bizottsággal és a főképviselővel együttműködve járuljanak hozzá az uniós hibrid eszköztár, valamint a hibrid hadjáratokra való koordinált uniós reagálás keretéről szóló, 2022. június 21-i tanácsi következtetésekben említett végrehajtási iránymutatások felgyorsított kifejlesztéséhez és végrehajtásához, valamint azok későbbi alkalmazásához, hogy teljeskörűen érvényt szerezzenek a hibrid hadjáratokra való koordinált uniós reagálási keretnek, különösen a hibrid hadjáratokra és hibrid fenyegetésekre való uniós szinten koordinált reagálás fontolóra vétele és előkészítése során, ideértve azokat a hadjáratokat vagy fenyegetéseket is, amelyek kritikus infrastruktúrát üzemeltető szervezetek ellen irányulnak.

Uniós szintű intézkedések

36. A Tanács felkéri a Bizottságot és a főképviselőt, hogy – adott esetben, az uniós jog szerinti feladat- és felelősségi körükkel összhangban – támogassák az érintett harmadik országokat a területükön lévő kritikus infrastruktúrák rezilienciájának fokozásában, különös tekintettel azokra a kritikus infrastruktúrákra, amelyek fizikailag kapcsolódnak a területükhöz és valamely tagállam területéhez.

37. A Bizottság és a főképviselő – az uniós jog szerinti feladat- és felelősségi körükkel összhangban – a rezilienciáról szóló EU–NATO strukturált párbeszéd keretében fokozni fogják a NATO-val való koordinációt a közös érdekű kritikus infrastruktúrák rezilienciájával kapcsolatban, az Unió és a tagállamok Szerződések szerinti hatásköreinek, valamint az Európai Tanács által jóváhagyott, az EU–NATO együttműködésre irányadó kulcsfontosságú elveknek, különösen a viszonosság, az inkluzivitás és a döntéshozatali autonómia elvének teljes körű tiszteletben tartása mellett. Ezzel összefüggésben az említett együttműködést a rezilienciáról szóló EU–NATO strukturált párbeszéd keretében fogják előmozdítani, az együttes nyilatkozatok végrehajtását segítő, személyzeti szintű, már meglévő mechanizmusba integrálva, a teljes körű átláthatóságnak és valamennyi tagállam bevonásának a biztosítása mellett.

38. A Tanács felkéri a Bizottságot, hogy – amennyiben szükséges és megfelelő – mérlegelje az érintett harmadik országok képviselőinek részvételét a tagállamok közötti együttműködés és információcsere keretében az olyan kritikus infrastruktúrák rezilienciáját illetően, amelyek fizikailag kapcsolódnak valamely tagállam, illetve valamely harmadik ország területéhez.

Kelt …-ban/-ben, …-án/-én.

a Tanács részéről

az elnök