EURÓPAI
BIZOTTSÁG

Strasbourg, 2022.10.18.
COM(2022) 551 final

2022/0338 (NLE)

Javaslat

A TANÁCS AJÁNLÁSA

a kritikus infrastruktúrák rezilienciájának megerősítését célzó összehangolt uniós megközelítésről

(EGT-vonatkozású szöveg)

INDOKOLÁS

1. A JAVASLAT HÁTTERE

• A javaslat indokai és céljai

A biztonság az Európai Unió egyik alapvető célja. Bár a polgárok védelme elsősorban a tagállamok felelőssége, az uniós szintű kollektív fellépés jelentős mértékben hozzájárul az EU egészének biztonságához. A koordináció elősegíti a reziliencia növelését, az éberség fokozását és kollektív válaszintézkedéseink megerősítését. Az európai biztonsági unióval összefüggésben fontos lépésekre került sor a számos biztonsági fenyegetés megelőzésére, felderítésére és az azokra való gyors reagálásra vonatkozó képességek és kapacitások kiépítése, valamint a köz- és a magánszektorbeli szereplők erőfeszítéseinek összevonása érdekében.

Ahhoz, hogy az EU képes legyen helytállni a folyamatosan változó fenyegetettségi helyzetben, szüntelen éberségre és alkalmazkodásra van szükség. Oroszország Ukrajna elleni agresszív háborúja új kockázatokat teremtett, amelyek együttesen gyakran hibrid fenyegetés formáját öltik. Ezek egyike az európai kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatások zavarának kockázata. Ez minden eddiginél egyértelműbbé vált az Északi Áramlat gázvezetékei ellen elkövetett nyilvánvaló szabotázs és más közelmúltbeli incidensek nyomán. A társadalom nagymértékben támaszkodik mind a fizikai, mind a digitális infrastruktúrára, és az alapvető szolgáltatások – akár hagyományos fizikai támadások, akár kibertámadások, vagy ezek kombinációja következtében kialakuló – zavarai súlyos következményekkel járhatnak a polgárok jóllétére, gazdaságainkra és a demokratikus rendszereinkbe vetett bizalomra nézve.

Az EU-nak ugyancsak kulcsfontosságú célja a belső piac zökkenőmentes működésének biztosítása, a kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatásokat is beleértve. Az EU ezért már számos intézkedést hozott a kritikus fontosságú szervezetek sebezhetőségének csökkentése és rezilienciájának növelése érdekében, mind a kiberkockázatok, mind a nem kiberjellegű kockázatok tekintetében.

Sürgősen meg kell erősíteni az EU arra vonatkozó kapacitását, hogy fel tudjon lépni a kritikus infrastruktúrák elleni esetleges támadásokkal szemben, elsősorban magán az EU-n belül, de adott esetben közvetlen szomszédságában is.

A javasolt tanácsi ajánlás fokozni kívánja a kritikus infrastruktúrák rezilienciájának növeléséhez és az uniós szintű koordináció biztosításához nyújtott, a felkészültségre és a reagálásra irányuló uniós támogatást. Célja, hogy kiterjessze és felgyorsítsa a gazdaság működéséhez szükséges eszközök, létesítmények és rendszerek védelmére, valamint a polgárok által igénybe vett alapvető belső piaci szolgáltatások nyújtására irányuló munkát, továbbá hogy a lehető leggyorsabb helyreállítást biztosítva enyhítse az esetleges támadások következményeit. Bár minden ilyen infrastruktúra védelmet igényel, a fő prioritás jelenleg az energia, a digitális infrastruktúra, a közlekedés, valamint az űrágazat, tekintettel rendkívül átfogó társadalmi és gazdasági jelentőségükre, valamint az aktuális kockázatértékelésekre.

Az EU-nak kiemelt szerepet kell vállalnia a szárazföldi vagy tengeri határokat átszelő és több tagállam érdekeit érintő, illetve a határokon átnyúló alapvető szolgáltatások nyújtására használt infrastruktúrák rezilienciájának biztosítása terén. A több tagállam számára releváns kritikus infrastruktúrák azonban egyetlen tagállamban, vagy akár a tagállamok területén kívül is elhelyezkedhetnek, például a tenger alatti kábelek vagy vezetékek esetében. A kritikus infrastruktúrák és az azokat üzemeltető szervezetek, valamint az azokat fenyegető kockázatok

egyértelmű azonosítása, és a védelmükre irányuló kollektív kötelezettségvállalás valamennyi tagállamnak és az EU egészének egyaránt érdeke.

Az Európai Parlament és a Tanács már politikai megállapodásra jutott az uniós jogszabályi keret elmélyítéséről a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának megerősítése érdekében. 2022 nyarán megállapodás született a kritikus fontosságú szervezetek rezilienciájáról szóló irányelvről (a továbbiakban: CER-irányelv)[1] és a hálózati és információs rendszerek biztonságáról szóló felülvizsgált irányelvről (a továbbiakban: NIS 2 irányelv)[2]. Ez a képességek lényeges megerősítését jelenti, összehasonlítva a meglévő jogszabályi kerettel, amelyet az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK irányelv (a továbbiakban: ECI-irányelv)[3] és a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai parlamenti és tanácsi irányelv (a továbbiakban: NIS-irányelv)[4] alkot. Az új jogi szabályozás várhatóan 2022 végén vagy 2023 elején lép hatályba, és az uniós joggal összhangban a tagállamoknak prioritásként kell kezelniük annak átültetését és alkalmazását.

Ilyen körülmények között, és tekintettel arra, hogy az Oroszország Ukrajna elleni agresszív háborújából eredő fenyegetések sürgős fellépést tehetnek szükségessé, az új jogszabályokban felvázolt lépéseket – amennyiben lehetséges és helyénvaló – a mai naptól kezdve előre kell ütemezni. A kölcsönös együttműködés azonnali fokozása segítene megteremteni az ahhoz szükséges lendületet, hogy az új jogi szabályozás teljes körű hatálybalépését hatékony végrehajtás kövesse.

Ennek eredményeként az együttműködés már most túllépne a jelenlegi kereteken, mind a fellépés mélysége, mind az érintett ágazatok köre tekintetében. Az új CER-irányelv új együttműködési keretet, valamint új kötelezettségeket irányoz elő a tagállamok és a kritikus fontosságú szervezetek számára azzal a céllal, hogy megerősítse a belső piacon alapvető szolgáltatásokat nyújtó szervezetek természeti és ember okozta fenyegetésekkel szembeni fizikai, nem kiberjellegű rezilienciáját, tizenegy konkrét ágazatban[5]. A NIS 2 irányelv kiterjeszti a kiberbiztonsági kötelezettségeket az ágazatok széles körére. Ez magában foglalja a tagállamokkal szembeni azon új követelményt, hogy adott esetben a tenger alatti kábeleket is belefoglalják kiberbiztonsági stratégiájukba.

A jogi előírások szerint a Bizottságnak fontos koordinációs szerepet kell betöltenie. A CER-irányelv értelmében a Bizottság támogató és elősegítő szerepet játszik, amelyet az említett irányelv alapján létrehozott, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport (CERG) támogatása és bevonása mellett kell végrehajtani, bevált gyakorlatok, iránymutatások és módszertanok kidolgozása révén kiegészítve a tagállami tevékenységeket. Ami a kiberbiztonságot illeti, a Tanács már az EU kiberbiztonsági helyzetéről szóló, 2022. nyári következtetéseiben felkérte a Bizottságot, a főképviselőt és a Kiberbiztonsági Együttműködési Csoportot, hogy ágyazzák be a kiberbiztonsági szempontokat a kockázatértékelésekbe és a forgatókönyvekbe. Ez a koordináció ösztönzőleg hathat az egyéb kulcsfontosságú kritikus infrastruktúrákkal kapcsolatos megközelítés kialakítására.

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 HL L 345., 2008.12.23.
4 HL L 194., 2016.7.19.
5 Energia, közlekedés, digitális infrastruktúra, banki szolgáltatások, pénzügyi piaci infrastruktúrák, egészségügy, ivóvíz, szennyvíz, közigazgatás, világűr és élelmiszeripar.

Ursula von der Leyen elnök 2022. október 5-én öt pontból álló tervet terjesztett elő, amely összehangolt megközelítésbe helyezi az előttünk álló munkát. A terv a következő fő elemekből áll: a felkészültség fokozása; együttműködés a tagállamokkal a kritikus infrastruktúráikra vonatkozó stressztesztek elvégzése céljából, kezdve az energiaágazattal, majd más, magas kockázatú ágazatokkal folytatva; a reagálási kapacitás növelése, különösen az uniós polgári védelmi mechanizmus révén; a műholdas kapacitás megfelelő kihasználása a potenciális fenyegetések felderítésére; valamint a kritikus infrastruktúrák rezilienciája terén a NATO-val és a kulcsfontosságú partnerekkel folytatott együttműködés megerősítése. Az öt pontból álló terv kiemelte a politikai támogatást élvező jogszabályok mielőbbi alkalmazásának jelentőségét.

A javasolt tanácsi ajánlás üdvözli ezt a megközelítést, amely a tagállamoknak nyújtott támogatás strukturálására és erőfeszítéseik összehangolására irányul a jelenlegi kockázatokkal összefüggő tudatosságnövelés, felkészültség és reagálás terén. Ennek kapcsán szakértői üléseket hívnak össze, hogy a CER-irányelv hatálybalépését és az annak alapján létrehozott CERG tevékenységének megkezdését előkészítve egyeztessenek a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájáról.

Elengedhetetlen lesz a kulcsfontosságú partnerekkel, valamint a szomszédos és más releváns harmadik országokkal a kritikus infrastruktúrát üzemeltető szervezetek rezilienciája terén folytatott megerősített együttműködés, különösen az EU és a NATO közötti, rezilienciáról szóló strukturált párbeszéd révén.

Ezen ajánlás középpontjában az Oroszország Ukrajna elleni agresszív háborújából eredő új fenyegetések előrejelzésére, megelőzésére és az azokra való reagálásra vonatkozó uniós kapacitás megerősítése áll. A javasolt ajánlások ezért a biztonsági vonatkozású kockázatok és a kritikus infrastruktúrákat fenyegető veszélyek kezelésére összpontosítanak. Mindazonáltal meg kell jegyezni, hogy a közelmúlt eseményei arra is rávilágítottak, hogy sürgősen fokozott figyelmet kell fordítani az éghajlatváltozás kritikus infrastruktúrákra és szolgáltatásokra gyakorolt hatásaira, például az atomerőművek hűtése, a vízenergia és a belvízi hajózás összefüggésében a szezonális ingadozásnak kitett és kiszámíthatatlan vízellátásra, vagy a közlekedési infrastruktúra súlyos károsodásának kockázatára, ami az alapvető szolgáltatások jelentős fennakadásait idézheti elő. Ezen aggályok kezelése továbbra is a megfelelő jogi eszközök és koordináció keretében zajlik.

- **Összhang a szabályozási terület jelenlegi rendelkezéseivel**

Ez a tanácsi ajánlásra irányuló javaslat teljes mértékben összhangban áll a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájára vonatkozó jelenlegi és jövőbeli jogi kerettel, az ECI-irányelvvel, illetve a CER-irányelvvel, mivel célja többek között az e területen megvalósuló, tagállamok közötti együttműködés előmozdítása, valamint az EU-ban kritikus infrastruktúrát üzemeltető szervezeteket érintő jelenlegi közvetlen fenyegetésekkel szembeni reziliencia javítását célzó konkrét intézkedések támogatása.

Emellett kiegészíti és előkészíti a CER-irányelvet, mivel már most felkéri a tagállamokat az irányelv időben történő átültetésének prioritásként kezelésére, együttműködést biztosít a Bizottság által bejelentett öt pontból álló terv alapján összehívott szakértői találkozók révén, valamint törekszik az EU-n belüli kritikus infrastruktúrák stressztesztjeinek elvégzésére vonatkozó közös megközelítés kialakítására.

A javaslat összhangban van továbbá a NIS-irányelvvel és az azt hamarosan felváltó NIS 2 irányelvvel, mivel szorgalmazza a végrehajtást és az átültetést célzó munka korai megkezdését. Tükrözi továbbá a 2022 márciusában Nevers-ben elfogadott közös felhívást, valamint az EU kiberbiztonsági helyzetéről szóló, 2022. májusi tanácsi következtetéseket a

tagállamok Bizottsághoz intézett, kockázatértékelések és kockázati forgatókönyvek kidolgozására irányuló kérését illetően.

A javaslat összhangban van a polgári védelemre vonatkozó uniós politikával is, amely szerint a kritikus infrastruktúrák/szervezetek működésének jelentős zavara esetén a tagállamok és harmadik országok segítséget kérhetnek az uniós polgári védelmi mechanizmus (UCPM) keretében működő Veszélyhelyzet-reagálási Koordinációs Központon (ERCC) keresztül. Az uniós polgári védelmi mechanizmus aktiválása esetén az ERCC képes koordinálni és társfinanszírozni a tagállamokban (részben az európai polgári védelmi eszköztár keretében) és a rescEU keretében rendelkezésre álló alapvető felszerelések, anyagok és szakértők érintett országba való telepítését. A kérésre rendelkezésre bocsátható segítségnyújtás magában foglalja például az üzemanyagot, a generátorokat, a villamosenergia-infrastruktúrát, a menedékhelyeket, a víztisztító kapacitást, valamint a sürgősségi orvosi kapacitást.

A javaslat szintén összhangban van az energiaellátás biztonságával kapcsolatos uniós vívmányokkal.

Az atomenergia-ágazat nem szerepel kifejezetten a javasolt tanácsi ajánlásban, kivéve például az ellátásbiztonságot adott esetben befolyásoló, kapcsolódó infrastruktúrákat (például az atomerőművekbe vezető átviteli vezetékeket). A kifejezetten nukleáris elemek az Euratom-Szerződés, illetve a nukleáris energiára vonatkozó releváns nemzeti jogi jogszabályok hatálya alá tartoznak[6]. A fukusimai balesetből tanulva az EU megerősítette a nukleáris biztonságra vonatkozó európai jogszabályokat, és következésképpen a nemzeti hatóságoknak minden egyes létesítmény esetében rendszeres időszakos biztonsági felülvizsgálatot kell végezniük a legszigorúbb biztonsági követelményeknek való folyamatos megfelelés garantálása és a biztonság fokozására vonatkozó további lehetőségek azonosítása érdekében, ezen túlmenően pedig uniós szinten hatévenként tematikus partneri felülvizsgálatra kerül sor.

Az EU tengeri védelmi stratégiája[7] és a kapcsolódó cselekvési terv[8] kiemeli a tengeri színtéren jelentkező fenyegetések változó jellegét, és sürgeti a kritikus tengeri infrastruktúrák – köztük a víz alatti, és különösen a tengeri közlekedési, energetikai és kommunikációs infrastruktúra – védelme iránti elkötelezettség megújítását, többek között a tengeri helyzetismeretnek a jobb interoperabilitás és az észszerűbb információcsere révén történő fokozása révén.

A javaslat összhangban van más vonatkozó ágazati jogszabályokkal is. Ezért ezen ajánlást azokkal az egyedi intézkedésekkel összhangban kell végrehajtani, amelyek szabályozzák vagy a jövőben szabályozhatják az érintett ágazatokban – például a közlekedésben – működő szervezetek rezilienciájának bizonyos szempontjait. Ide tartoznak más releváns kezdeményezések is, például a közlekedési vészhelyzeti terv[9] vagy az élelmiszer-ellátás és az élelmezésbiztonság válság idején történő biztosítása érdekében kidolgozott vészhelyzeti terv[10], valamint a kapcsolódó európai élelmezésbiztonsági válságfelkészültségi és -reagálási mechanizmus. Általánosabban fogalmazva, az ajánlást magától értetődően az uniós jog valamennyi alkalmazandó szabályának – köztük az ECI-irányelv és a NIS-irányelv rendelkezéseinek – teljes körű tiszteletben tartása mellett kell végrehajtani.

---

6 A 2008/114/EK tanácsi irányelv (ECI-irányelv) (9) preambulumbekezdése.
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.

A javaslat ezenkívül összhangban van a biztonságra és védelemre vonatkozó stratégiai iránytűvel, amely hangsúlyozta, hogy jelentősen fokozni kell a hibrid fenyegetésekkel és a kibertámadásokkal szembeni rezilienciát és az elhárításukra vonatkozó képességet, valamint meg kell erősíteni a partnerországok rezilienciáját és együtt kell működni a NATO-val. Összhangban van továbbá az EU-t, a tagállamokat és a partnereket érintő hibrid fenyegetésekre és hadjáratokra való koordinált uniós reagálásra vonatkozó kerettel[11].

2. JOGALAP, SZUBSZIDIARITÁS ÉS ARÁNYOSSÁG

• Jogalap

A javaslat jogalapját az Európai Unió működéséről szóló szerződés (a továbbiakban: EUMSZ) 114. cikke képezi, amely előirányozza a jogszabályok közelítését a belső piac továbbfejlesztése céljából, az EUMSZ 292. cikkével együtt. Ezt az indokolja, hogy a javasolt tanácsi ajánlás elsősorban az új CER-irányelvben és a NIS 2 irányelvben foglalt intézkedések mielőbbi alkalmazását célozza, amely két jogszabály szintén az EUMSZ 114. cikkén alapul. Azzal a megfontolással összhangban, amely szerint az említett irányelvek jogalapját az említett cikknek kell képeznie, uniós fellépésre van szükség a belső piac zavartalan működésének biztosítása érdekében, különös tekintettel az érintett szolgáltatások határokon átnyúló jellegére és hatókörére, a zavarok lehetséges következményeire, valamint az alapvető belső piaci szolgáltatások nyújtásához használt kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozását célzó jelenlegi és kidolgozás alatt álló nemzeti intézkedésekre.

• Szubszidiaritás (nem kizárólagos hatáskör esetén)

A kritikus infrastruktúrát üzemeltető szervezetek rezilienciája terén indokolt az európai szintű előrelépés, tekintettel a kritikus infrastruktúrák működése és a nyújtott alapvető szolgáltatások közötti kapcsolatok egymástól függő, határokon átnyúló jellegére, valamint arra, hogy a jelenlegi geopolitikai helyzetben az érintett szervezetek kellő mértékű rezilienciájának biztosításához közös és összehangoltabb európai megközelítésre van szükség. Mivel számos közös kihívást – például az Északi Áramlat gázvezetékei ellen elkövetett nyilvánvaló szabotázst – elsősorban nemzeti intézkedések vagy kritikus infrastruktúrát üzemeltető szervezetek kezelnek, a reziliencia növeléséhez, az éberség fokozásához és az EU kollektív reagálásának megerősítéséhez az EU és adott esetben az érintett ügynökségek támogatására van szükség.

• Arányosság

Ez a javaslat összhangban van az Európai Unióról szóló szerződés 5. cikkének (4) bekezdésében meghatározott arányosság elvével.

A javasolt tanácsi ajánlás sem tartalmilag, sem formailag nem lépi túl a benne foglalt célkitűzések eléréséhez szükséges mértéket. A javasolt intézkedések arányosak a kitűzött célokkal, mivel tiszteletben tartják a tagállamok nemzeti jogban foglalt előjogait és kötelezettségeit.

Végezetül a javaslat a differenciálást lehetővé tevő megközelítést alkalmaz, tükrözve a tagállamok eltérő belső realitásait a kritikus infrastruktúrákat fenyegető fizikai veszélyekre való felkészültség és reagálás tekintetében.

[11] Az Európai Unió Tanácsa 10016/22, 2022. június 21.

- **A jogi aktus típusának megválasztása**

A fent említett célkitűzések elérése érdekében az EUMSZ előírja – konkrétan a 292. cikkben –, hogy a Tanácsnak a Bizottság javaslata alapján ajánlásokat kell elfogadnia. A tanácsi ajánlás a jelen esetben megfelelő eszköz, figyelembe véve a fent ismertetett aktuális jogi környezetet is. A tanácsi ajánlás – bár nem kötelező erejű – jogi aktusként jelzi a benne foglalt intézkedések iránti tagállami elkötelezettséget, és szilárd politikai alapot biztosít az e területeken folytatott együttműködéshez, miközben teljes mértékben tiszteletben tartja a tagállamok hatáskörét.

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

- **Az érdekelt felekkel folytatott konzultációk**

E javaslat kidolgozása során a Bizottság figyelembe vette a tagállami szakértők által a 2022. október 12-i ülésen kifejtett nézeteket. Széles körű egyetértés övezte azt a nézetet, hogy az uniós szintű koordináció fokozása a jelenlegi fenyegetésekre való felkészültség és reagálás szempontjából hasznos, valamint hogy a CER-irányelv egyes elemeit már a jogszabály hivatalos elfogadását megelőzően helyénvaló alkalmazni. A tagállamok jelezték, hogy nyitottak a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozására irányuló intézkedésekkel és módszerekkel kapcsolatos tapasztalatok és bevált gyakorlatok megosztására. A tagállamok emellett kifejezték, hogy nyitottak a kritikus infrastruktúrát üzemeltető szervezetek stressztesztjeire vonatkozó, közös elveken alapuló összehangolt megközelítés önkéntes alkalmazására. A tagállamok úgy vélték, hogy ezen ajánlás alkalmazásában prioritást kell élvezniük az energetikai, a digitális és a közlekedési ágazatban kritikus infrastruktúrát üzemeltető szervezeteknek, különös tekintettel azokra, amelyek több tagállam számára is relevánsak. A tagállamok üdvözölték továbbá a Bizottság azon szándékát, hogy az elkövetkező hetekben további üléseket hívjon össze tagállami szakértők részvételével.

- **A javaslat egyes rendelkezéseinek részletes magyarázata**

A tanácsi ajánlásra irányuló javaslat a következőket tartalmazza:

– Az I. fejezet meghatározza a javaslat célját, alkalmazási körét és az ajánlott intézkedések prioritási sorrendjét.

– A II. fejezet azokra az intézkedésekre összpontosít, amelyeket uniós és tagállami szinten meg kell hozni a felkészültség fokozása érdekében.

– A III. fejezet a megerősített reagálással foglalkozik, uniós és tagállami viszonylatban egyaránt.

– A IV. fejezet témája a nemzetközi együttműködés és a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozása érdekében meghozandó intézkedések.

2022/0338 (NLE)

Javaslat

A TANÁCS 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. és 292. cikkére,

tekintettel az Európai Bizottság javaslatára,

mivel:

(1) Az EU-nak kiemelt szerepet kell vállalnia a szárazföldi vagy tengeri határokon átnyúló és több tagállam érdekeit érintő, illetve a határokon átnyúló alapvető szolgáltatások nyújtása céljából a szervezetek által más módon használt infrastruktúrák rezilienciájának biztosítása terén. A több tagállam számára releváns ilyen szolgáltatásnyújtás és kritikus infrastruktúra azonban egyetlen tagállamban, vagy a tagállamok területén kívül is elhelyezkedhet, például a tenger alatti kábelek vagy vezetékek esetében. Az ilyen infrastruktúrák és szervezetek, valamint az azokat fenyegető kockázatok egyértelmű azonosítása, csakúgy mint a védelmükre irányuló kollektív kötelezettségvállalás valamennyi tagállamnak és az Unió egészének egyaránt érdeke.

(2) A kritikus infrastruktúrák védelmét két ágazatban jelenleg a 2008/114/EK tanácsi irányelv[12] szabályozza. Az említett irányelv eljárást hoz létre az európai kritikus infrastruktúrák azonosítására és kijelölésére, valamint közös megközelítést alakít ki annak értékelésére vonatkozóan, hogy a személyek védelméhez való hozzájárulás érdekében szükséges-e javítani ezen infrastruktúrák védelmét. Az irányelv az energetikai és a közlekedési ágazatot fedi le. A kritikus fontosságú szervezetek és az általuk nyújtott alapvető szolgáltatások, valamint az általuk igénybe vett kritikus infrastruktúrák rezilienciájának javítása érdekében folyamatban van a kritikus fontosságú szervezetek rezilienciájáról szóló új irányelv[13] (a továbbiakban: CER-irányelv) uniós jogalkotó általi elfogadása. Az új jogszabály a 2008/114/EK irányelv helyébe fog lépni, és több ágazatra, köztük a digitális infrastruktúrára is kiterjed majd.

(3) Emellett a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről szóló (EU) 2016/1148 európai

[12] 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.).

[13] COM(2020) 829.

parlamenti és tanácsi irányelv[14] a kibertérben megjelenő fenyegetésekre összpontosít. Ezt az irányelvet az Unió egész területén magas szintű kiberbiztonságot biztosító intézkedésekről szóló új irányelv[15] (a továbbiakban: NIS 2 irányelv) fogja felváltani, amelynek az uniós jogalkotó általi elfogadása szintén folyamatban van.

(4) Tekintettel a gyorsan változó fenyegetettségi helyzetre – különösen az Északi Áramlat 1 és 2 gázinfrastruktúrája ellen elkövetett nyilvánvaló szabotázzsal összefüggésben – a kritikus infrastruktúrát üzemeltető szervezetek sajátos kihívásokkal szembesülnek az ellenséges cselekményekkel és más ember okozta fenyegetésekkel szembeni rezilienciájukat tekintve, miközben a természeti tényezőkből és az éghajlatváltozásból eredő kihívások egyre súlyosbodnak, és kölcsönhatásba léphetnek az ellenséges cselekményekkel. Ezért e szervezeteknek a tagállamok támogatásával megfelelő intézkedéseket kell hozniuk rezilienciájuk megerősítése érdekében. Ezeket az intézkedéseket végre kell hajtani, és ehhez már az új CER- és NIS 2 irányelv elfogadása, hatálybalépése és átültetése előtt a 2008/114/EK irányelv és az (EU) 2016/1148 irányelv szerinti intézkedéseken túlmutató támogatást kell biztosítani.

(5) Az említett új irányelvek elfogadásáig, hatálybalépéséig és átültetéséig a Tanács arra ösztönzi az Uniót és a tagállamokat, hogy az uniós joggal összhangban használjanak fel minden rendelkezésre álló eszközt az előrelépés érdekében, és erősítsék meg az érintett szervezetek, valamint a belső piaci alapvető szolgáltatások – azaz az alapvető társadalmi funkciók, a gazdasági tevékenységek, a népegészségügy és a közbiztonság, illetve a környezet fenntartása szempontjából kulcsfontosságú szolgáltatások – nyújtása érdekében általuk üzemeltetett kritikus infrastruktúrák fizikai és kiberrezilienciáját. E tekintetben a reziliencia fogalmát úgy kell érteni mint a szervezet megelőzésre, védekezésre, reagálásra, ellenállásra, enyhítésre, elnyelésre, alkalmazkodásra és helyreállításra vonatkozó képességét az olyan események összefüggésében, amelyek jelentősen megzavarhatják vagy ténylegesen megzavarják a szóban forgó alapvető szolgáltatások nyújtását.

(6) A hatékony és az új CER-irányelvhez a lehető legnagyobb mértékben illeszkedő megközelítés biztosítása érdekében az ezen ajánlásban foglalt intézkedéseknek a tagállamok által kritikus infrastruktúraként kijelölt infrastruktúrákra kell vonatkozniuk, a nemzeti és az európai kritikus infrastruktúrákat is beleértve, függetlenül attól, hogy a kritikus infrastruktúrát üzemeltető szervezetet az új irányelv alapján már kijelölték-e kritikus fontosságú szervezetként. Ezen ajánlás alkalmazásában a „kritikus infrastruktúra” kifejezés ennek megfelelően értendő.

(7) A fennálló fenyegetésekre tekintettel prioritásnak minősül a rezilienciaerősítő intézkedések meghozatala a kulcságazatokban, vagyis az energia, a digitális infrastruktúra, a közlekedés és az űrkutatás területén, és ezeknek az intézkedéseknek a kritikus infrastruktúrát üzemeltető szervezetek ember okozta kockázatokkal szembeni rezilienciájának fokozására kell irányulniuk. A nemzeti kritikus infrastruktúrák esetében, tekintettel a kockázatok bekövetkezésének lehetséges következményeire, prioritásként kell kezelni a határokon átnyúló jelentőségű infrastruktúrákat.

(8) Ennek megfelelően az ezen ajánlásban meghatározott intézkedések elsődleges célja az Európai Unió működéséről szóló szerződés (EUMSZ) 114. cikkén alapuló új CER- és

[14] 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.).

[15] COM(2020) 823.

NIS 2 irányelv kiegészítése az e két új irányelv által előírt intézkedések előrevetítése és megerősítése révén. Mindezért, továbbá tekintettel a szóban forgó alapvető szolgáltatások és kritikus infrastruktúrák határokon átnyúló jellegére és jelentőségére, valamint a nemzeti jogszabályok jelenlegi és kialakulóban lévő, a belső piacot torzító eltéréseire, helyénvaló ezt az ajánlást szintén az EUMSZ 114. cikkére és az EUMSZ 292. cikkére alapozni.

(9) Ezen ajánlás végrehajtása nem értendő úgy, mint amely érinti az érintett szervezetek rezilienciájának bizonyos szempontjaira vonatkozó, jelenlegi és jövőbeli uniós jogi követelményeket, és azokkal összhangban kell állnia. Ezeket a követelményeket olyan általános eszközök határozzák meg, mint a 2008/114/EK irányelv és az (EU) 2016/1148 irányelv, valamint az ezeket felváltó új CER- és NIS 2 irányelv, de bizonyos ágazatspecifikus eszközök is, például a közlekedés területén, ahol a Bizottság többek között a közlekedési vészhelyzeti tervre vonatkozó kezdeményezést indított[16]. A lojális együttműködés elvével összhangban ezen ajánlást a teljes körű kölcsönös tisztelet és segítségnyújtás szellemében kell végrehajtani.

(10) A Bizottság 2022. október 5-én öt pontból álló tervet terjesztett elő, amely összehangolt megközelítésbe helyezi az előttünk álló kihívások kezelését. Kiterjed egyrészt a felkészültséggel kapcsolatos munkára, az új CER-irányelv elfogadását és hatálybalépését megelőlegezve, illetve arra építve, másrészt pedig a tagállamokkal való együttműködésre a kritikus infrastruktúrát üzemeltető szervezetek közös elveken alapuló stressztesztjeinek elvégzése céljából, az energiaágazattal kezdve. Ez az ajánlás, amely hozzá fog járulni az említett tervhez, üdvözli a javasolt megközelítést, és felvázolja, hogy az hogyan ültethető át a gyakorlatba.

(11) Tekintettel a gyorsan változó fenyegetettségi helyzetre és az ember okozta kockázatokkal fémjelzett jelenlegi kockázati környezetre – különösen ami a határokon átnyúló jelentőségű kritikus infrastruktúrákat illeti –, elengedhetetlen, hogy pontos, naprakész és teljes kép álljon rendelkezésre a kritikus infrastruktúrát üzemeltető szervezeteket érintő fő kockázatokról. Ezért a tagállamoknak meg kell tenniük a szükséges intézkedéseket e kockázatok értékelésének elvégzése vagy az értékelés naprakésszé tétele érdekében. Bár ez az ajánlás a biztonsági vonatkozású kockázatokra összpontosít, az éghajlatváltozás és a környezeti kockázatok kezelésére irányuló erőfeszítéseket is fenn kell tartani, különösen akkor, ha természeti események tovább súlyosbíthatják az ember okozta kockázatokat.

(12) Tekintettel a fenyegetettségi helyzetre, fel kell kérni a tagállamokat arra, hogy a lehető leghamarabb hozzanak megfelelő intézkedéseket a kritikus infrastruktúrák rezilienciájának fokozása érdekében, az említett kockázatértékeléseken túlmenően is, amelyek elvégzése az új CER-irányelv hatálybalépésével kötelezővé válik.

(13) A Bizottság által bejelentett öt pontból álló terv végrehajtásának részeként össze kell hangolni a munkát a nemzeti szakértők összefogása révén, ezáltal előkészítve az új CER-irányelv szerint létrehozandó, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport tevékenységét, hogy lehetővé váljon a tagállamok közötti együttműködés és a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájával kapcsolatos információcsere. Ennek ki kell terjednie az olyan tevékenységekkel kapcsolatos együttműködésre és információcserére, mint a kritikus fontosságú szervezetek és infrastruktúrák azonosítása, a stressztesztek elvégzésére vonatkozó közös elvek kidolgozásának és érvényesítésének előkészítése, a stressztesztek közös

[16] COM(2022) 211.

tanulságainak levonása, valamint a sebezhetőségek és a lehetséges képességek azonosítása. Ezek a folyamatok várhatóan a kritikus infrastruktúrát üzemeltető szervezetek éghajlati és környezeti kockázatokkal szembeni rezilienciája szempontjából is előnyösek lesznek. Ezek az erőfeszítések lehetővé tennék továbbá a stressztesztekkel kapcsolatos munka közös prioritásainak kijelölését, kiemelt hangsúlyt fektetve az energiára, a digitális infrastruktúrára, a közlekedésre és az űrágazatra. A Bizottság már megkezdte a szakértői találkozók szervezését és munkájuk elősegítését, és a továbbiakban is folytatni kívánja ezt a munkát. Az új CER-irányelv hatálybalépését és a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport megalakulását követően a csoportnak kell folytatnia az előkészítő munkát, a CER-irányelvben meghatározott feladataival összhangban.

(14) A stressztesztek kiegészítéseként ki kell dolgozni a kritikus infrastruktúrákat érintő biztonsági eseményekre és válságokra vonatkozó tervet, amely leírja és meghatározza a kritikus infrastruktúrákat érintő biztonsági eseményekre való reagálás terén a tagállamok, valamint az uniós intézmények, szervek, hivatalok és ügynökségek között megvalósuló együttműködés céljait és módjait, különösen a belső piacon nyújtott alapvető szolgáltatások jelentős zavara esetében. A tervnek a reagálás koordinálása érdekében a meglévő politikai szintű integrált válságelhárítási mechanizmusra (IPCR) kell támaszkodnia, a nagyszabású kiberbiztonsági eseményekre vonatkozó tervvel összhangban és azt kiegészítve kell működnie, továbbá rendelkeznie kell a nyilvánosságnak szóló kulcsfontosságú üzenetekkel kapcsolatos megállapodásról is, mivel a válságkommunikáció fontos szerepet játszik a kritikus infrastruktúrákat érintő események és válságok negatív hatásainak enyhítésében.

(15) A jelenlegi és a várhatóan bekövetkező fenyegetésekre való összehangolt és hatékony reagálás biztosítása érdekében a Bizottság további támogatást fog biztosítani a tagállamoknak, hogy e fenyegetések fényében fokozza a rezilienciát, különösen azáltal, hogy releváns információkat nyújt tájékoztatók, kézikönyvek és iránymutatások formájában, előmozdítja az uniós finanszírozású kutatási és innovációs projektekben való részvételt, megteszi a szükséges megelőző intézkedéseket és optimalizálja az uniós felügyeleti eszközök alkalmazását. Az EKSZ-nek – különösen az Európai Unió Helyzetelemző Központján keresztül – fenyegetésértékeléseket kell készítenie.

(16) Az ágazatspecifikus uniós ügynökségeknek és más érintett szerveknek szintén támogatást kell nyújtaniuk a rezilienciával kapcsolatos kérdésekben, amennyiben a vonatkozó uniós jogi eszközökben meghatározott megbízatásuk ezt lehetővé teszi. Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) segítséget nyújthat a kiberbiztonsági kérdésekben, az Európai Tengerészeti Biztonsági Ügynökség (EMSA) tengerfelügyeleti szolgálatán keresztül szakértelmével járulhat hozzá a tagállamok támogatásához a tengerbiztonsággal és -védelemmel kapcsolatos kérdésekben, a Bűnüldözési Együttműködés Európai Uniós Ügynöksége (EUROPOL) támogatást nyújthat a határokon átnyúló bűnüldözési tevékenységek keretében folytatott információgyűjtéshez és nyomozásokhoz, míg az Európai Unió Űrprogramügynöksége (EUSPA) és az Európai Unió Műholdközpontja (SatCen) az uniós űrprogram keretében végrehajtott műveletek révén nyújthat segítséget.

(17) A kritikus infrastruktúrák és az érintett szervezetek biztonságának garantálása elsősorban a tagállamok felelőssége, mindazonáltal az uniós szintű koordináció megerősítése helyénvaló, különösen az olyan fenyegetések fényében, amelyek egyszerre több tagállamot is érinthetnek – mint például Oroszország Ukrajna elleni

agresszív háborúja – vagy hatással lehetnek az Unió gazdaságának, egységes piacának és a társadalmainak rezilienciájára és megfelelő működésére.

(18) Ez az ajánlás nem irányozza elő olyan információk átadását, amelyek közlése ellentétes a tagállamok alapvető nemzetbiztonsági, közbiztonsági vagy védelmi érdekeivel.

(19) A fizikai és digitális infrastruktúrák 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. Tekintettel a kifinomult hibrid támadások jelentette fokozott fenyegetésre, a tagállamoknak a jelen ajánlás végrehajtása során figyelembe kell venniük ezeket a megfontolásokat. Tekintettel a kiberbiztonság és az üzemeltetők fizikai biztonsága közötti összefüggésekre, fontos, hogy az új NIS 2 irányelv átültetésének és alkalmazásának előkészítésére irányuló munka a lehető leghamarabb megkezdődjön, és hogy az új CER-irányelvvel összefüggő hasonló munka ezzel párhuzamosan haladjon.

(20) A felkészültség fokozása mellett fontos javítani azokat a képességeket is, amelyek lehetővé teszik a gyors és hatékony reagálást abban az esetben, ha valóban zavar állna be a kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatásokban. Ezért ennek az ajánlásnak tartalmaznia kell a tagállami és uniós szinten egyaránt meghozandó intézkedéseket, ideértve az uniós polgári védelmi mechanizmus keretében folytatandó megerősített együttműködést és információcserét, valamint az uniós űrprogram releváns eszközeinek felhasználását.

(21) Az EU kiberbiztonsági helyzetéről szóló tanácsi következtetésekben[17] foglalt felkérés nyomán a Bizottság, az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: a főképviselő) és az (EU) 2016/1148 irányelvvel létrehozott együttműködési csoport (a továbbiakban: Kiberbiztonsági Együttműködési Csoport) az érintett polgári és katonai szervekkel és ügynökségekkel, valamint a létrehozott hálózatokkal – köztük az EU CyCLONe-nal – együttműködve kockázatértékelést végeznek és kiberbiztonsági szemléletű kockázati forgatókönyveket dolgoznak ki a tagállamok vagy partnerországok elleni fenyegetés vagy esetleges támadás esetére. E tevékenységük során olyan kritikus ágazatokra összpontosítanak, mint az energia, a digitális infrastruktúra, a közlekedés és az űrkutatás ágazata.

(22) A nevers-i közös miniszteri felhívás[18] és az EU kiberbiztonsági helyzetéről szóló tanácsi következtetések egyaránt az Unióban található kommunikációs infrastruktúrák és hálózatok rezilienciájának megerősítésére szólítottak fel a tagállamoknak és a Bizottságnak címzett, kockázatértékelésen alapuló ajánlások révén. Ezen a kockázatértékelésen dolgozik jelenleg a Kiberbiztonsági Együttműködési Csoport a Bizottság és az ENISA támogatásával, valamint az Európai Elektronikus Hírközlési Szabályozók Testületével (BEREC) együttműködésben. A kockázatértékelés és a hiányelemzés megvizsgálja a kommunikációs infrastruktúrák különböző alágazatait – többek között a helyhez kötött és mobil infrastruktúrákat, a műholdakat, a tenger alatti kábeleket és az internetes útvonal-meghatározást – érintő kibertámadások kockázatát, ezáltal alapul szolgálva az ezen ajánlás keretében végzett munkához. Ez a kockázatértékelés információkkal szolgál majd a kiberkockázatok folyamatban lévő

[17] Kiberbiztonsági helyzet: A Tanács jóváhagyja a következtetéseket – Tanács (europa.eu) (angol nyelven)

[18] https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

ágazatközi értékeléséhez és a forgatókönyvekhez, amelyek kidolgozására a Tanács a 2022. május 23-i tanácsi következtetésekben szólított fel.

(23) Ez a két gyakorlat következetesen és összehangoltan fog igazodni ahhoz a jelenleg is folyó gyakorlathoz, amelynek keretében a Bizottság és a tagállamok az 1313/2013/EU európai parlamenti és tanácsi határozat[19] alapján a polgári védelemre összpontosító forgatókönyveket dolgoznak ki a természeti és ember okozta katasztrófák széles körére vonatkozóan, többek között a kiberbiztonsági eseményekkel és azok valós életre gyakorolt hatásaival összefüggésben. A hatékonyság, az eredményesség és a következetesség érdekében ezen ajánlás végrehajtása során figyelembe kell venni az említett gyakorlatok eredményeit.

(24) Az 5G kiberbiztonsággal kapcsolatos uniós eszköztár[20] releváns intézkedéseket és kockázatcsökkentési terveket határoz meg az 5G hálózatok biztonságának megerősítése céljából. Tekintettel arra, hogy számos alapvető szolgáltatás függ 5G hálózatoktól, és a digitális ökoszisztémák összekapcsolt jellegűek, alapvető fontosságú, hogy valamennyi tagállam sürgősen végrehajtsa az eszköztárban ajánlott intézkedéseket, és alkalmazza különösen a koordinált uniós kockázatértékelésben kritikusnak és érzékenynek minősített kulcsfontosságú eszközök magas kockázatú beszállítóira vonatkozó releváns korlátozásokat.

(25) A súlyos kiberbiztonsági eseményekre való felkészültség és reagálási képességek azonnali megerősítése érdekében a Bizottság létrehozott egy rövid távú programot, amely az ENISA számára elkülönített további finanszírozás révén támogatást nyújt a tagállamoknak. A program keretében nyújtott szolgáltatások között szerepelni fognak felkészültségi intézkedések, például a kritikus fontosságú szervezeteknél végzett behatolási tesztelés, melynek célja a sebezhetőségek azonosítása. A program emellett bővebb lehetőségeket fog biztosítani a tagállamoknak való segítségnyújtásra a kritikus fontosságú szervezeteket érintő súlyos biztonsági események esetén. Ez az első lépés a kiberbiztonság helyzetéről szóló tanácsi következtetésekkel összhangban, amely következtetésekben a Tanács felszólítja 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.

(26) A tenger alatt futó adat- és elektronikus hírközlési kábelek világméretű hálózata nélkülözhetetlen a globális és az EU-n belüli összekapcsoltság szempontjából. Mivel ezek a kábelek rendkívül hosszúak és a tengerfenéken futnak, a legtöbb kábelszakasz esetében a víz alatti vizuális felügyelet különösen nagy kihívást jelent. A megosztott joghatóság és az e kábelekkel kapcsolatos egyéb joghatósági nehézségek olyan különleges 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 infrastruktúrákra vonatkoznak, ki kell egészíteni a tenger alatti kábelekkel kapcsolatos külön kockázatértékeléssel és kockázatcsökkentő intézkedésekkel. A Bizottság ezért e célból tanulmányokat fog készíteni, és megállapításait megosztja a tagállamokkal.

---

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

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(27) Az ezen ajánlásban kiemelt ágazatként meghatározott energia- és közlekedési ágazatot a digitális infrastruktúrával kapcsolatos kockázatok is érinthetik. Ilyen hatás például a digitális összetevőket tartalmazó energetikai technológiákkal összefüggésben is jelentkezhet. Az alapvető szolgáltatások folyamatossága és az energiaágazatban működő szervezetek által működtetett kritikus infrastruktúrák stratégiai ellenőrzése szempontjából fontos tényező a kapcsolódó ellátási láncok biztonsága. Figyelembe kell venni ezeket a körülményeket azon intézkedések meghozatalakor, amelyek ezen ajánlással összhangban a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozására irányulnak.

(28) Ahogy a biztonsággal kapcsolatos tevékenységek szempontjából az űrinfrastruktúra és az űralapú szolgáltatások egyre növekvő jelentőséggel bírnak, elengedhetetlenül fontos biztosítani az uniós űrtechnológiai eszközök és szolgáltatások védelmét és rezilienciáját az Unión belül és ezen ajánlás keretében egyaránt, hogy strukturáltabban történjen azon űralapú adatok és szolgáltatások hasznosítása, amelyeket az űrrendszerek és a más ágazatok kritikus infrastruktúrájának megfigyelését 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.

(29) A kritikus infrastruktúrát üzemeltető szervezetek rezilienciáját érintő kockázatok eredményes kezeléséhez nemzetközi szintű együttműködésre is szükség van, legyen szó akár az Unióban, akár az érintett harmadik országokban, akár nemzetközi vizeken üzemelő infrastruktúrákról. Ezért a tagállamokat fel kell kérni, hogy az e cél felé vezető egyes lépések tekintetében működjenek együtt a Bizottsággal és a főképviselővel, azzal a kikötéssel, hogy bármely ilyen jellegű lépés csak az uniós jog – nevezetesen az uniós szerződések külkapcsolatokra vonatkozó rendelkezései – értelmében a tagállamokat terhelő feladatokkal és felelősségekkel összhangban tehető meg.

(30) Az „A Bizottság hozzájárulása az európai védelemhez” című közleményben[21] foglaltak szerint a Bizottság a főképviselővel és a tagállamokkal együttműködésben értékelni fogja az ágazati hibrid reziliencia alapértékeit az „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[22] támogatása érdekében, és ennek keretében azonosítani fogja a hiányosságokat és a szükségleteket, valamint az azok 2023-ig történő kezelése érdekében megteendő lépéseket. Ennek a kezdeményezésnek információkkal kell szolgálnia az ezen ajánlás keretében folyó munkához, elősegítve az információmegosztás javítását és a fellépések jobb összehangolását a reziliencia – így többek között a kritikus infrastruktúrák rezilienciájának – további megerősítésével kapcsolatban.

(31) A 2014. évi uniós tengeri védelmi stratégia és az ahhoz kapcsolódó cselekvési terv sürgette a kritikus tengeri infrastruktúrák – többek között a víz alatti, és különösen a tengeri közlekedési, energetikai és kommunikációs infrastruktúra – fokozott védelmét, többek között a tengeri tudatosságnak a jobb interoperabilitás és az észszerűbb (kötelező és önkéntes) információcsere révén történő javításával. Jelenleg folyamatban

---

21 https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52022DC0060&qid=1666010202682&from=HU

22 Az Európai Unió Tanácsa 7371/22, 2022. március 21.

van az említett stratégia és cselekvési terv aktualizálása, és az aktualizált változat tartalmazni fog a kritikus tengeri infrastruktúra védelmét célzó megerősített intézkedéseket. Ezeknek az intézkedéseknek információval kell szolgálniuk ehhez az ajánláshoz és ki kell egészíteniük azt.

(32) A tagállamoknak az uniós biztonsági kutatási programban rejlő összes lehetőséggel számolniuk kell: maradéktalanul ki kell aknázniuk a programnak a kritikus infrastruktúrákra vonatkozó célzott prioritását, különösen a Belső Biztonsági Alap által finanszírozott programok keretében, valamint amennyiben az egyedi intézkedések teljesítik a vonatkozó támogathatósági követelményeket, ki kell használniuk az egyéb – nevezetesen az Európai Regionális Fejlesztési Alap kínálta – potenciális uniós szintű finanszírozási lehetőségeket. A REPowerEU is lehetőséget kínálhat a rezilienciaépítés finanszírozására. Az uniós finanszírozás által kínált lehetőségeket az alkalmazandó jogi követelményekkel összhangban lehet kihasználni.

ELFOGADTA EZT AZ AJÁNLÁST:

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

(1) Ez az ajánlás felkéri a tagállamokat, hogy hozzanak sürgős és hatásos intézkedéseket, valamint folytassanak lojális, hatékony, szolidáris és összehangolt együttműködést egymással, a Bizottsággal, más illetékes hatóságokkal és az érintett szervezetekkel az alapvető szolgáltatások belső piacon való nyújtásához használt kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozása érdekében.

(2) Az ezen ajánlásban meghatározott intézkedések azokra a kritikus infrastruktúrákra vonatkoznak, amelyeket valamely tagállam kritikus infrastruktúrának minősített, ideértve az európai kritikus infrastruktúrákat is.

(3) Ezen ajánlás végrehajtása során prioritásként kell kezelni az energia, a digitális infrastruktúra, a közlekedés és az űrkutatás ágazatában működő szervezetek, valamint az általuk üzemeltetett, határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák ember okozta kockázatokkal szembeni rezilienciájának növelését.

II. FEJEZET FOKOZOTT FELKÉSZÜLTSÉG

Tagállami szintű fellépések

(4) A Tanács felkéri a tagállamokat, hogy végezzék el vagy aktualizálják a 2008/114/EK irányelv által kijelölt, a közlekedési és energiaágazatban európai kritikus infrastruktúrát üzemeltető szervezetek rezilienciájára vonatkozó kockázatértékeléseket, és – adott esetben és az említett irányelvvel összhangban – működjenek együtt egymással az ilyen kockázatértékelések és az azokból eredő rezilienciafokozó intézkedések terén.

(5) Emellett annak érdekében, hogy a kritikus infrastruktúrát üzemeltető szervezetek rezilienciája magas szintet érjen el, a tagállamoknak az új CER-irányelv mielőbbi átültetése és alkalmazása érdekében fel kell gyorsítaniuk az előkészítő munkát a következő intézkedések révén:

(a) a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozását célzó nemzeti stratégiák elfogadásának vagy aktualizálásának felgyorsítása. E stratégia releváns részeiről tájékoztatni kell a Bizottságot;

(b) a jelenlegi fenyegetések változó jellegéhez igazodva kockázatértékelések elvégzése vagy aktualizálása azon szervezetek rezilienciájára vonatkozóan, amelyek az energia,

a digitális infrastruktúra, valamint a közlekedés és az űrkutatás ágazatán kívül eső ágazatokban üzemeltetnek kritikus infrastruktúrákat, valamint lehetőség szerint az új CER-irányelv hatálya alá tartozó ágazatok – nevezetesen a banki ágazat, a pénzügyi piaci infrastruktúra, a digitális infrastruktúra, az egészségügy, az ivóvíz, a szennyvíz, a közigazgatás, az űrkutatás, valamint az élelmiszer-termelés, -feldolgozás és -elosztás – tekintetében, figyelembe véve a releváns fenyegetések potenciálisan hibrid jellegét, beleértve az áttételes hatásokat és az éghajlatváltozás hatásait;

(c) a Bizottság tájékoztatása az egyes ágazatokban és alágazatokban azonosított kockázatok típusáról, valamint a kockázatértékelések eredményéről, amely megtehető a Bizottság által a tagállamokkal együttműködésben kidolgozott közös jelentéstételi sablon használatával;

(d) a kritikus fontosságú szervezetek azonosítására és kijelölésére irányuló folyamat felgyorsítása, prioritásként kezelve azon kritikus fontosságú szervezetek azonosítását és kijelölését, amelyek:

(a) olyan kritikus infrastruktúrákat használnak, amelyek között két vagy több tagállamon átívelő fizikai kapcsolat áll fenn;

(b) más tagállamok kritikus fontosságú szervezeteivel kapcsolatban álló vagy azokhoz kapcsolódó vállalati struktúrák részét képezik;

(c) az egyik tagállamban kritikus fontosságú szervezetként azonosított, és legalább hat tagállamban vagy több tagállamban alapvető szolgáltatásokat nyújtó szervezetként kiemelt európai jelentőségű, kritikus fontosságú szervezetnek minősülnek, és ennek megfelelően tájékoztatják a Bizottságot;

(d) egymás közti együttműködés, különösen a kritikus fontosságú szervezetek és az alapvető szolgáltatások, valamint a határokon átnyúló jelentőséggel bíró kritikus infrastruktúrák tekintetében, különösen azáltal, hogy tájékoztatják egymást az (5) pont d) alpontjának alkalmazása keretében, valamint a jelentős vagy potenciálisan jelentős, határokon átnyúló zavart okozó biztonsági eseményekről, miközben szükség szerint folyamatosan tájékoztatják a Bizottságot;

(e) a kijelölt kritikus fontosságú szervezetek rezilienciájának javítása érdekében az ilyen szervezeteknek nyújtott támogatás fokozása, amely magában foglalhatja útmutató anyagok és módszertan biztosítását, a szervezetek rezilienciájának tesztelését szolgáló gyakorlatok szervezését, tanácsadás és képzés nyújtását személyzetük számára, valamint az érzékeny szerepet betöltő személyek biztonsági ellenőrzésének lehetővé tételét az uniós és a nemzeti jogszabályokkal összhangban, a kritikus fontosságú szervezetek munkavállalókra vonatkozó biztonsági intézkedéseinek részeként;

(f) az illetékes hatóságon belüli egyedüli kapcsolattartó pont kijelölésének vagy létrehozásának felgyorsítása azzal a céllal, hogy a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájával kapcsolatos kérdésekben biztosítsák a határokon átnyúló együttműködést más tagállamok egyedüli kapcsolattartó pontjaival.

(6) A Tanács arra biztatja a tagállamokat, hogy a kritikus infrastruktúrát üzemeltető szervezeteket vessék alá stressztesztek. A Tanács felkéri a tagállamokat különösen arra, hogy az energiaágazatban fokozzák saját és az érintett szervezetek felkészültségét, és végezzenek az említett ágazatra kiterjedő stressztesztet, lehetőség szerint az uniós szinten közösen elfogadott elvek szerint, és emellett biztosítsák az érintett szervezetekkel való hatékony kommunikációt. Ezt követően szükség esetén stressztesztek elvégzését más kiemelt ágazatokban – nevezetesen a

digitális infrastruktúra, a közlekedés és az űrkutatás területén – is fontolóra lehetne venni, kellően figyelembe véve a légi és tengeri alágazatokban az uniós jog alapján végzett ellenőrzéseket, valamint az ágazati jogszabályok vonatkozó rendelkezéseit.

(7) A Tanács felkéri a tagállamokat, hogy – adott esetben és az uniós joggal összhangban – működjenek együtt az érintett harmadik országokkal a határokon átnyúló jelentőséggel bíró kritikus infrastruktúrát üzemeltető szervezetek rezilienciáját érintő kérdésekben.

(8) A Tanács felkéri a tagállamokat, hogy annak érdekében, hogy az Unióban – többek között például a transzeurópai hálózatok mentén – a kritikus infrastruktúrát üzemeltető szervezetek nagyobb rezilienciával tudjanak szembenézni minden jelentős fenyegetéssel, az alkalmazandó követelményekkel összhangban használják ki a potenciális uniós és nemzeti szintű finanszírozási lehetőségeket, különösen – amennyiben teljesülnek a vonatkozó támogathatósági kritériumok, az éghajlatváltozási rezilienciavizsgálatra vonatkozó rendelkezéseket is ideértve – a Belső Biztonsági Alap és az Európai Regionális Fejlesztési Alap által finanszírozott programok égisze alatt, valamint az Európai Hálózatfinanszírozási Eszköz keretében rendelkezésre állókat. Az uniós polgári védelmi mechanizmus keretében nyújtott finanszírozás – az alkalmazandó követelményekkel összhangban – szintén felhasználható erre a célra, különösen a kockázatértékeléshez, a beruházási tervekhez vagy tanulmányokhoz, a kapacitásépítéshez vagy a tudásbázis fejlesztéséhez kapcsolódó projektek esetében. A REPowerEU is lehetőségeket kínálhat a rezilienciaépítés finanszírozására.

(9) Ami az Unióban található kommunikációs és hálózati infrastruktúrát illeti, a Kiberbiztonsági Együttműködési Csoportnak az (EU) 2016/1148 irányelv 11. cikkével, majd azt követően a NIS 2 irányelv 14. cikkével összhangban eljárva fel kell gyorsítania a célzott kockázatértékelésre irányuló, folyamatban lévő munkáját, és 2023 elején elő kell terjesztenie az első ajánlásokat. Biztosítani kell, hogy ez a munka koherensen és kiegészítő jelleggel illeszkedjen ahhoz a munkához, amelyet a Kiberbiztonsági Együttműködési Csoport és más érintett csoportok – például az új CER-irányelv alapján létrehozandó, a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoport és a digitális működési rezilienciáról szóló új jogszabály[23] (DORA) értelmében létrehozandó felvigyázási fórum – az információs és kommunikációs technológiák ellátási láncának biztonságával kapcsolatban végeznek.

(10) A Kiberbiztonsági Együttműködési Csoport – amelynek az (EU) 2016/1148 irányelv 11. cikkével, majd azt követően a NIS 2 irányelv 14. cikkével összhangban kell ellátnia feladatait – felkérést kap, hogy a Bizottság és az ENISA támogatásával kezelje prioritásként a digitális infrastruktúra és az űrágazat biztonságával kapcsolatos munkáját, és ennek jegyében még a NIS 2 irányelv hatálybalépését megelőzően többek között dolgozzon ki olyan szakpolitikai iránymutatást, valamint kiberbiztonsági kockázatkezelési módszereket és intézkedéseket a tenger alatti kommunikációs kábelek tekintetében, amelyek az összes veszélyre kiterjedő megközelítésen alapulnak, továbbá dolgozzon ki iránymutatást az űrágazatban tevékenykedő üzemeltetőkre vonatkozó kiberbiztonsági kockázatkezelési intézkedések tekintetében az űralapú szolgáltatások nyújtását támogató földi infrastruktúra rezilienciájának növelése céljából.

[23] COM(2020) 595 final

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

(12) A tagállamoknak sürgősen végre kell hajtaniuk az 5G kiberbiztonsággal kapcsolatos eszköztárban[24] ajánlott intézkedéseket, Azoknak a tagállamoknak, amelyek még nem vezettek be korlátozásokat a magas kockázatú beszállítókra vonatkozóan, ezt további késedelem nélkül meg kell tenniük, tekintettel arra, hogy a késlekedés növelheti az uniós hálózatok sebezhetőségét. Meg kell erősíteniük továbbá 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, ideértve az 5G-hálózatok egységes szintű biztonságának és rezilienciájának biztosítását célzó uniós szintű, jogilag kötelező érvényű előírásokat.

(13) A tagállamoknak a lehető leghamarabb végre kell hajtaniuk a határokon átnyúló villamosenergia-áramlás kiberbiztonsági szempontjaira vonatkozó, hamarosan hatályba lépő üzemi és kereskedelmi szabályzatot, a NIS 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.

(14) A tagállamoknak fejleszteniük kell a Galileo és/vagy a Kopernikusz megfigyelési célú használatát, és a releváns információkat meg kell osztaniuk a 15. pont szerint bevont szakértőkkel. Megfelelően ki kell használni a kritikus infrastruktúra megfigyelésére és a válságreagálás támogatására szolgáló képességeket, amelyeket az Unió űrprogramja keretében létrehozott állami műholdas kommunikációs programmal (GOVSATCOM) kapcsolatban.

Uniós szintű fellépések

(15) A Bizottság meg kívánja erősíteni a tagállami szakértők közötti együttműködést annak érdekében, hogy elősegítse a kritikus infrastruktúrát üzemeltető szervezetek fizikai, nem kiberjellegű rezilienciájának fokozását, különösen a következők révén:

(a) a tagállamokat e reziliencia fokozásában támogató közös eszközök – többek között módszertanok és kockázati forgatókönyvek – kidolgozásának és elterjesztésének előkészítése;

(b) a 6. pontban említett stressztesztek elvégzésére vonatkozó közös elvek tagállamok általi kidolgozásának támogatása, azokkal a tesztekkel kezdve, amelyek az energiaágazatot érintő ember okozta kockázatokra összpontosítanak, majd folytatva azokkal, amelyek fókuszában más kulcsfontosságú ágazatok – például a digitális infrastruktúra, a közlekedés és az űrágazat – állnak; egyéb jelentős kockázatok és veszélyek kezelése; valamint adott esetben az ilyen stressztesztek elvégzésével kapcsolatos támogatás és tanácsadás;

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

(c) biztonságos platform biztosítása a bevált gyakorlatok, a nemzeti tapasztalatokból levont tanulságok és az ilyen jellegű rezilienciával kapcsolatos egyéb információk összegyűjtéséhez, számbavételéhez és megosztásához, többek között az említett stressztesztek elvégzésével és azok eredményeinek protokollokba és vészhelyzeti tervekbe való átültetésével kapcsolatban.

A tagállami szakértők munkája során különös figyelmet kell fordítani az ágazatközi függőségekre és a határokon átnyúló jelentőséggel bíró kritikus infrastruktúrát üzemeltető szervezetekre, és létrejötte után a kritikus fontosságú szervezetek rezilienciájával foglalkozó csoportnak folytatnia kell ezt a munkát.

(16) A tagállamoknak teljes mértékben részt kell venniük a 15. pontban említett megerősített együttműködésben, és ennek keretében többek között ki kell jelölniük releváns szakértelemmel rendelkező kapcsolattartó pontokat, valamint meg kell osztaniuk a stressztesztekhez, protokollokhoz és vészhelyzeti tervekhez használt, e szakértelmen alapuló módszerekkel kapcsolatos tapasztalataikat. Az információcsere során óvni kell a rendelkezésre bocsátott információk bizalmas jellegét, valamint a kritikus fontosságú szervezetek biztonsági és üzleti érdekeit, egyszersmind tiszteletben tartva a tagállamok biztonságát. Ez nem foglalja magában olyan információk szolgáltatását, amelyek közlése ellentétes a tagállamok alapvető nemzetbiztonsági, közbiztonsági vagy védelmi érdekeivel.

(17) A Bizottság támogatást nyújt majd a tagállamoknak azáltal, hogy kézikönyveket és iránymutatásokat bocsát rendelkezésükre, például a kritikus infrastruktúrák és nyilvános terek pilóta nélküli légijármű-rendszerekkel szembeni védelméről szóló kézikönyvet, valamint kockázatértékelési eszközöket. Az EKSZ – különösen az Európai Unió Helyzetelemző Központján és annak hibrid fenyegetésekkel foglalkozó információs csoportján keresztül – felkérést kap arra, hogy a helyzetismeret javítása érdekében tartson tájékoztatókat az EU infrastruktúráit fenyegető veszélyekről.

(18) A Bizottság támogatni fogja a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájával kapcsolatos, uniós kutatási és innovációs programok keretében finanszírozott projektekben való részvételt. A Bizottság a 2021–2027-es időszakra vonatkozó többéves pénzügyi keretben a Horizont Európa számára elkülönített költségvetésen belül növelni kívánja az ilyen jellegű reziliencia finanszírozását. Ennek lehetővé kell tennie az e területen jelentkező jelenlegi és jövőbeli kihívások kezelését– például a kritikus infrastruktúrákra vonatkozó éghajlatváltozási rezilienciavizsgálat elvégzését –, anélkül, hogy negatív hatást gyakorolna a Horizont Európa keretében a polgári biztonsággal kapcsolatos egyéb kutatásokhoz és innovációhoz nyújtott finanszírozásra. A Bizottság nagyobb erőfeszítéseket fog tenni a releváns uniós finanszírozású kutatási projektek eredményeinek megismertetése érdekében is.

(19) A Bizottság felkéri a Kiberbiztonsági Együttműködési Csoportot, hogy a Bizottsággal és a főképviselővel együttműködve és az uniós jog szerinti feladataival és felelősségével összhangban fokozza az érintett hálózatokkal, valamint a polgári és katonai szervekkel a kockázatértékelések elvégzése és a kiberbiztonsági kockázati forgatókönyvek kidolgozása terén folytatott munkát, kezdetben az energiára, a kommunikációra, a közlekedésre és az űrinfrastruktúrára, valamint az ágazatok és a tagállamok közötti kölcsönös függőségekre összpontosítva. Ennek során figyelembe kell venni az említett ágazatok alapját adó fizikai infrastruktúrát érintő kapcsolódó kockázatokat. Rendszeresen kockázatértékelést kell végezni és forgatókönyveket kell kidolgozni, és ügyelni kell arra hogy az így létrejövő kockázatértékelések a szóban

forgó ágazatokban már meglévő vagy tervezett kockázatértékeléseket kiegészítsék, azokra épüljenek és azokat ne kettőzzék meg, valamint információval szolgáljanak a kritikus infrastruktúrát üzemeltető szervezetek általános rezilienciájának megerősítéséről és sebezhetőségeik kezeléséről szóló egyeztetésekhez.

(20) A Bizottság fel fogja gyorsítani a tagállamok felkészültségének és a nagyszabású kiberbiztonsági eseményekre való reagálásának támogatását célzó tevékenységeit, nevezetesen a következőket:

(a) a hálózat- és információbiztonsággal kapcsolatos releváns kockázatértékelések kiegészítéseként átfogó helyzetfelmérő tanulmány készítése a tagállamokat és Európát a világ többi részével összekötő tenger alatti kábelinfrastruktúráról, beleértve a hálózat feltérképezését, a kapacitások és a redundanciák azonosítását, a sebezhetőségek feltárását, valamint a szolgáltatások rendelkezésre állásával kapcsolatos kockázatokat és a kockázatcsökkentés lehetőségeit. A megállapításokat meg kell osztani a tagállamokkal.

(b) a tagállamok, valamint az uniós intézmények, szervek és ügynökségek nagyszabású kiberbiztonsági eseményekre való felkészültségének támogatása.

(21) A Bizottság fokozni fogja az előretekintő megelőző intézkedésekkel kapcsolatos – többek között az uniós polgári védelmi mechanizmus keretében végzett – munkát az 1313/2013/EU határozat 6. és 10. cikke értelmében a tagállamokkal együttműködve, valamint az Európai Veszélyhelyzet-reagálási Központ operatív felkészültségét támogató vészhelyzeti tervezés formájában.

A Bizottság különösen a következő lépéseket fogja tenni:

(a) a Veszélyhelyzet-reagálási Koordinációs Központban az előrejelzéssel és az ágazatközi megelőzéssel, felkészültséggel és reagálással kapcsolatban folyó munka előmozdítása a kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatások zavarainak előrejelzése és az azokra való felkészülés érdekében;

(b) a megelőző jellegű megközelítésekbe és az ilyen zavarokra való lakossági felkészültségbe történő beruházások növelése, különösen a vegyi, biológiai, radioaktív anyagokra és nukleáris robbanóanyagokra vagy más, ember által okozott fenyegetésekre összpontosítva;

(c) a releváns ismeretek és a bevált gyakorlatok cseréjének megerősítése, valamint a kapacitásfejlesztési tevékenységek – például a kritikus infrastruktúrát üzemeltető szervezetekkel folytatott képzések és gyakorlatok – tervezésének és lebonyolításának javítása a meglévő struktúrák és szakértelem – például az uniós polgári védelmi tudáshálózat – révén.

(22) A Bizottság elő fogja mozdítani az EU felügyeleti eszközeinek (Kopernikusz és Galileo) használatát annak érdekében, hogy segítséget nyújtson a tagállamoknak a kritikus infrastruktúrák és adott esetben azok közvetlen környezetének megfigyeléséhez, valamint hogy támogassa az Unió űrprogramja keretében biztosított egyéb megfigyelési lehetőségeket.

(23) A Tanács felkéri az uniós ügynökségeket és más érintett szerveket, hogy – adott esetben és megbízatásukkal összhangban – nyújtsanak támogatást a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájával kapcsolatos kérdésekben, különösen például:

(a) az Europol a határokon átnyúló bűnüldözési tevékenységekhez kapcsolódó információgyűjtés, bűnügyi elemzés és nyomozati támogatás terén;

(b) az EMSA az uniós tengerhasznosítási ágazat biztonságával és védelmével kapcsolatos ügyekben, beleértve a tenger biztonsággal és védelemmel kapcsolatos tengerfelügyeleti szolgáltatásokat is;

(c) az EUSPA az Unió űrprogramja keretében végzett tevékenységek tekintetében;

(d) az ENISA a kiberbiztonsággal kapcsolatos tevékenységek tekintetében.

III. FEJEZET MEGERŐSÍTETT REAGÁLÁS

Tagállami szintű fellépések

(24) A tagállamok:

(a) hangolják össze reagálásukat és a Tanács válságelhárítási mechanizmusának (IPCR) keretében továbbra is kísérjék figyelemmel a kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatásokban bekövetkező jelentős zavarokra való ágazatközi reagálást, amennyiben határokon átívelő kritikus infrastruktúrákról van szó, a nagyszabású kiberbiztonsági eseményekre vonatkozó tervet, valamint – hibrid hadjáratok esetében – a hibrid hadjáratokra való koordinált reagálásra vonatkozó keretet.

(b) fokozzák az uniós polgári védelmi mechanizmuson belül folyó információcserét a korai előrejelzés javítása, valamint az ilyen jelentős zavarokra a mechanizmus keretében való reagálásuk összehangolása érdekében, hogy ezáltal szükség esetén gyorsabban sor kerülhessen az Unió segítségével megvalósuló reagálásra;

(c) készüljenek jobban fel arra, hogy az uniós polgári védelmi mechanizmuson keresztül reagáljanak az ilyen jelentős zavarokra, különösen, ha az említett zavarok valószínűleg jelentős határokon átnyúló vagy akár páneurópai, illetve ágazatokon átívelő következményekkel járnak;

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

(e) kérjék fel a kritikus infrastruktúrát üzemeltető szervezeteket és az érintett nemzeti hatóságokat, hogy javítsák azon képességeiket, amelyek révén gyorsan helyre tudják állítani az általuk nyújtott alapvető szolgáltatások alapszintű biztosítását;

(f) gondoskodjanak arról, hogy ha szükségessé válik valamely kritikus infrastruktúra újjáépítése, akkor az újjáépített infrastruktúra a rá veszélyt jelentő valamennyi jelentős kockázattal szemben reziliens legyen, beleértve a kedvezőtlen éghajlati forgatókönyveket is.

(25) A Tanács felkéri a tagállamokat, hogy gyorsítsák fel a NIS 2 irányelv átültetésére és alkalmazására irányuló előkészítő munkát azáltal, hogy – tekintettel a CSIRT-ek új feladataira, valamint az új ágazatokban tevékenykedő szervezetek megnövekedett számára – haladéktalanul megkezdik a nemzeti számítógép-biztonsági eseményekre reagáló csoportok (CSIRT-ek) képességeinek fejlesztését kiberbiztonsági stratégiáik gyors aktualizálása, valamint a kiberbiztonsági eseményekre és válságokra vonatkozó nemzeti reagálási tervek mielőbbi elfogadása révén.

Uniós szintű fellépések

(26) A kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatásokban bekövetkező jelentős zavarokra való reagálást össze kell hangolni a tagállami szakértők között az ilyen szervezetek rezilienciája és a szóban forgó

zavarokra adható azon válaszlépések tekintetében, amelyek hozzájárulhatnak a Tanács válságelhárítási mechanizmusának (IPCR) működéséhez.

(27) A Bizottság szorosan együtt fog működni a tagállamokkal annak érdekében, hogy továbbfejlessze a bevethető veszélyhelyzet-reagálási képességeket – ezen képességek közé számítva a szakértőket és az uniós polgári védelmi mechanizmus keretében rendelkezésre álló rescEU-készleteket –, hogy ezáltal fokozott operatív felkészültséggel lehessen kezelni azokat az azonnali és közvetetett hatásokat, amelyek a kritikus infrastruktúrát üzemeltető szervezetek által nyújtott alapvető szolgáltatásokat érintő jelentős zavarok nyomán jelentkeznek.

(28) Figyelembe véve a változó kockázati környezetet, a Bizottság a tagállamokkal együttműködve az uniós polgári védelmi mechanizmus keretében

(a) folyamatosan elemezni és tesztelni fogja a meglévő reagálási képesség megfelelőségét és operatív felkészültségét;

(b) rendszeresen felül fogja vizsgálni, hogy szükség lehet-e új uniós szintű reagálási képességek kifejlesztésére a rescEU-n keresztül;

(c) még jobban meg fogja erősíteni az ágazatközi együttműködést a megfelelő uniós szintű reagálás biztosítása érdekében, és rendszeres gyakorlatokat fog szervezni ezen együttműködés tesztelésére;

(d) tovább fogja fejleszteni az uniós szintű ágazatközi válságközpontként működő ERCC-t az érintett tagállamoknak nyújtott támogatás koordinálása érdekében.

(29) A Bizottság a főképviselővel együttműködve, a tagállamokkal szorosan egyeztetve és a releváns uniós ügynökségek támogatásával ki fogja dolgozni a kritikus infrastruktúrákat érintő biztonsági eseményekre és válságokra vonatkozó tervet, amely leírja és meghatározza a kritikus infrastruktúrákat érintő biztonsági eseményekre való reagálás terén a tagállamok, valamint az uniós intézmények, szervek, hivatalok és ügynökségek között megvalósuló együttműködés céljait és módjait, különösen a belső piacon nyújtott alapvető szolgáltatások jelentős zavara esetében. A tervnek a reagálás koordinálása érdekében a meglévő politikai szintű integrált válságelhárítási mechanizmusra (IPCR) kell támaszkodnia.

(30) A Bizottság együtt fog működni az érdekelt felekkel és a szakértőkkel a tenger alatti kábelinfrastruktúrákat érintő biztonsági események utáni lehetséges – a 20. pont a) alpontjában említett helyzetfelmérő tanulmánnyal együtt bemutatandó – helyreállítási intézkedések tekintetében, valamint a vészhelyzeti tervezés, a kockázati forgatókönyvek és az uniós katasztrófavédelmi mechanizmus keretében folyó, katasztrófavédelmi rezilienciával kapcsolatos munka továbbfejlesztése érdekében.

IV. FEJEZET: NEMZETKÖZI EGYÜTTMŰKÖDÉS

(31) A Bizottság és a főképviselő – adott esetben és az uniós jog szerinti feladataikkal és felelősségükkel összhangban – támogatni fogja a partnerországokat a területükön kritikus infrastruktúrát üzemeltető szervezetek rezilienciájának fokozásában.

(32) A Bizottság és a főképviselő – az uniós jog szerinti feladataikkal és felelősségükkel összhangban – a rezilienciáról szóló EU–NATO strukturált párbeszéd révén megerősíti a NATO-val a kritikus infrastruktúrák rezilienciája terén folytatott koordinációt, és e célból munkacsoportot hoz létre.

(33) A Tanács felkéri a tagállamokat, hogy a Bizottsággal és a főképviselővel együttműködve járuljanak hozzá az uniós hibrid eszköztár, valamint a hibrid

hadjáratokra való összehangolt uniós reagálás keretéről szóló tanácsi következtetésekben[25] említett végrehajtási iránymutatások felgyorsított kifejlesztéséhez és végrehajtásához, valamint azok későbbi alkalmazásához, hogy teljeskörűen érvényt szerezzenek a hibrid hadjáratokra való összehangolt uniós reagálási keretnek, különösen a hibrid hadjáratokra és hibrid fenyegetésekre való uniós szinten koordinált reagálás fontolóra vétele és előkészítése során, ideérve azokat a hadjáratokat vagy fenyegetéseket is, amelyek kritikus infrastruktúrát üzemeltető szervezetek ellen irányulnak.

(34) A Bizottság adott esetben mérlegelni fogja annak lehetőségét, hogy harmadik országok képviselői is részt vegyenek a kritikus infrastruktúrát üzemeltető szervezetek rezilienciájával kapcsolatos, tagállami szakértők között folyó együttműködésben és információcserében.

[…]

Kelt Strasbourgban, -án/-én.

a Tanács részéről
az elnök

[25] A Tanács következtetései a hibrid hadjáratokra való összehangolt uniós reagálás keretéről – Tanács (europa.eu)