EURÓPAI
BIZOTTSÁG

AZ UNIÓ KÜLÜGYI ÉS
BIZTONSÁGPOLITIKAI
FŐKÉPVISELŐJE

Brüsszel, 2016.4.6.
JOIN(2016) 18 final

KÖZÖS KÖZLEMÉNY AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

A hibrid fenyegetésekkel szembeni fellépés közös kerete

európai uniós válasz

1. BEVEZETÉS

Az elmúlt években az Európai Unió biztonsági környezete drámai változásokon ment keresztül. Az EU keleti és déli szomszédságából jelentkező, a békét és stabilitást veszélyeztető komoly kihívások folyamatosan nyilvánvalóvá teszik annak szükségességét, hogy az Unió megerősítse biztonságfenntartó szerepét, kiemelt figyelmet fordítva a külső és belső biztonság közötti szoros kapcsolatra. A békét, a biztonságot és a jólétet veszélyeztető számos jelenlegi kihívás az Unió közvetlen szomszédságában kialakult instabilitásból, valamint a fenyegetések változó formájából ered. 2014-es politikai iránymutatásában Jean-Claude Juncker, az Európai Bizottság elnöke kiemelte, hogy „Európát erősebbé kell tennünk, ha biztonsági és védelmi ügyekről van szó", valamint, hogy az európai és a nemzeti eszközöket hatékonyabban kell ötvözni, mint tettük azt a múltban. Ezt követően, a Külügyek Tanácsa 2015. május 18-i felkérését követően, a főképviselő – a Bizottság szolgálataival és az Európai Védelmi Ügynökséggel (EDA) szoros együttműködésben, valamint az uniós tagállamokkal egyeztetve – előterjesztette ezt a közös keretet, amely a hibrid fenyegetésekkel szembeni fellépésre vonatkozó, a gyakorlatba átültethető javaslatokat tartalmaz, és amely fokozza az EU és a tagállamok, valamint partnerei ellenálló képességét[1]. Az Európai Tanács 2015 júniusában emlékeztetett arra, hogy a hibrid fenyegetések jelentette veszélyekkel szembeni fellépés érdekében mozgósítani kell az uniós eszközöket[2].

Bár a hibrid fenyegetések fogalma nem állandó, és rugalmasnak is kell maradnia annak érdekében, hogy megfeleljen a jelenség változó jellegének, a koncepció célja, hogy megragadja azoknak a kényszerítő és felforgató tevékenységeknek, valamint hagyományos és nem hagyományos módszereknek (például katonai, diplomáciai, gazdasági, technológiai) az egyvelegét, amelyeket állami vagy nem állami szereplők összehangolt módon használhatnak fel bizonyos célok elérése érdekében úgy, hogy eközben a hivatalosan deklarált hadviselés szintje alatt maradnak. A hangsúly általában a célpont sebezhető pontjainak kihasználásán, valamint egy olyan, nem egyértelmű helyzet megteremtésén van, aminek célja a döntéshozatali folyamatok hátráltatása. A hibrid fenyegetések eszközei lehetnek erőteljes félretájékoztatási kampányok is, amelyek során a szociális médiát használják fel a politikai narratíva befolyásolása, vagy közvetítő szereplők radikalizálása, toborzása és irányítása céljából.

Amennyiben a hibrid fenyegetésekkel szembeni fellépés a nemzeti biztonságot és védelmet, valamint a közrend fenntartását érinti, az elsődleges felelősség a tagállamokra hárul, mivel a tagállamok sebezhetősége országonként változó. Több tagállam néz szembe azonban olyan közös fenyegetésekkel, amelyek határokon átnyúló hálózatokat vagy infrastruktúrákat vehetnek célba. Az ilyen fenyegetésekkel szemben hatékonyabban lehet fellépni összehangolt uniós válaszlépésekkel, az uniós szakpolitikák és eszközök felhasználásával, az európai szolidaritás és kölcsönös segítségnyújtás alapján, és a Lisszaboni Szerződésben rejlő lehetőségek teljes körű kihasználásával. Az uniós

[1] A Tanács következtetései a közös biztonság- és védelempolitikáról (KBVP), 2015. május [Consilium 8971/15]

[2] Az Európai Tanács következtetései, 2015. június [EUCO 22/15].

szakpolitikák és eszközök fontos értéknövelő szerepet játszhatnak – és jelentős mértékben már most is játszanak – a figyelemfelhívás területén. Ez elősegíti a tagállamok ellenálló képességének javítását a közös fenyegetésekkel szembeni fellépés érdekében. Az Unió azon külső tevékenységét, amelyre ez a keret javaslatot tesz, az Európai Unióról szóló szerződés (EUSZ) 21. cikkében foglalt elvek alapján kell folytatni, amelyek között szerepel a demokrácia, a jogállamiság, az emberi jogok egyetemessége és oszthatatlansága, valamint az Egyesült Nemzetek Alapokmányában foglalt elvek és a nemzetközi jog tiszteletben tartása[3].

Ennek a közös közleménynek a célja, hogy elősegítse egy olyan átfogó megközelítés kialakítását, amelynek segítségével az EU a tagállamokkal együttműködve képes lesz a hibrid típusú fenyegetésekkel szembeni célzott fellépésre azáltal, hogy szinergiákat teremt a releváns eszközök között, és előmozdítja az összes érintett szereplő szoros együttműködését[4]. Az intézkedések olyan, már meglévő stratégiákon és ágazati politikákon alapulnak, amelyek a biztonság fokozását segítik elő. Konkrétan, az európai biztonsági stratégia[5], az Európai Unió kül- és biztonságpolitikára vonatkozó, majdani globális stratégiája, valamint az európai védelmi cselekvési terv[6], az EU kiberbiztonsági stratégiája[7], az energiabiztonsági stratégia[8] és az Európai Unió tengerhajózási biztonsági stratégiája[9] olyan eszközök, amelyek hozzájárulhatnak a hibrid fenyegetésekkel szembeni fellépéshez.

Mivel a NATO is dolgozik a hibrid fenyegetésekkel szembeni fellépésen, a Külügyek Tanácsa pedig az együttműködés és a koordináció fokozását javasolta e területen, egyes javaslatok az EU és a NATO közötti együttműködés fokozására irányulnak a hibrid fenyegetésekkel szembeni fellépés terén.

A javasolt fellépés az alábbi elemekre összpontosít: tudatosságnövelés, az ellenálló képesség erősítése, válságmegelőzés, válságkezelés és helyreállítás.

2. A FENYEGETÉS HIBRID JELLEGÉNEK FELISMERÉSE

A hibrid fenyegetések célja egy ország sebezhetőségének kihasználása, és gyakran az alapvető demokratikus értékeket és szabadságokat próbálják aláásni. Első lépésként a főképviselő és a Bizottság együttműködik a tagállamokkal, hogy az EU sebezhető pontjait célzó esetleges kockázatok nyomon követése és értékelése által javítsa a helyzetismeretet. A Bizottság jelenleg biztonsági kockázatértékelési módszereket dolgoz

[3] Az Európai Unió Alapjogi Chartája – az uniós jog végrehajtása során – kötelező érvényű az uniós intézményekre és a tagállamokra nézve.

[4] Az esetleges jogalkotási javaslatok összhangban lesznek a Bizottság minőségi jogalkotásra vonatkozó követelményeivel a minőségi jogalkotásra vonatkozó bizottsági iránymutatásnak megfelelően (SWD(2015) 111.

[5] COM(2015) 185 final.

[6] 2016-ban kerül előterjesztésre.

[7] Uniós kibervédelmi szakpolitikai keret [Consilium 15585/14], valamint közös közlemény „Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér” vonatkozásában, 2013. február [JOIN(2013)1].

[8] Közös közlemény: „Európai energiabiztonsági stratégia”, 2014. május [SWD(2014) 330].

[9] Közös közlemény: „A nyitott és biztonságos globális tengeri terület megteremtése: az Európai Unió tengerbiztonsági stratégiájának elemei” — JOIN(2014) 9 final — 2014/03/06.

ki, amelyek elősegítik a döntéshozók tájékoztatását és kockázatalapú szakpolitikák kidolgozását számos területen, a légi közlekedés védelmétől kezdve a terrorizmus finanszírozása elleni küzdelmen át a pénzmosás megakadályozásáig. Ezen túlmenően fontos lenne, hogy a tagállamok felmérést készítsenek, amelyben azonosítják a hibrid fenyegetések szempontjából veszélyeztetett területeket. A cél a hibrid fenyegetéseket jelző mutatók azonosítása, ezek beépítése a korai előrejelzésekbe és a meglévő kockázatértékelési mechanizmusokba, valamint szükség esetén azok megosztása.

<u>1. intézkedés</u>: A tagállamok felkérést kapnak arra, hogy – szükség esetén a Bizottság és a főképviselő támogatásával – a legfontosabb sebezhető pontok és a hibrid fenyegetésekre utaló specifikus mutatók azonosítása céljából készítsenek felmérést azokról a hibrid kockázatokról, amelyek veszélyeztethetik a nemzeti és pán-európai struktúrákat és hálózatokat.

3. AZ UNIÓS VÁLASZ KIALAKÍTÁSA: TUDATOSSÁGNÖVELÉS

3.1. A hibridfenyegetéses információkat szintetizáló uniós csoport

Alapvetően fontos, hogy az EU a tagállamokkal együttműködve, megfelelő szintű helyzetismerettel rendelkezzen annak érdekében, hogy azonosítani tudja a biztonsági környezet bármely olyan változását, amely állami vagy nem állami szereplő által okozott hibrid tevékenységgel kapcsolatos. A hibrid fenyegetések elleni hatékony fellépés érdekében fontos az információcsere javítása és a hírszerzési információk cseréjének elősegítése az egyes ágazatok, illetve az Európai Unió valamint annak tagállamai és partnerei között.

Az Európai Külügyi Szolgálat (EKSZ) az Európai Unió Helyzetelemző Központján (EU SitCen) belül létrehozott, a hibridfenyegetéses információkat szintetizáló uniós csoport kizárólag a hibrid fenyegetések elemzésére fog összpontosítani. Ez az információszintetizáló csoport az EKSZ-en belüli különböző érdekelt felektől (ideértve az uniós küldöttségeket is), a Bizottságtól (és az uniós ügynökségektől[10]), valamint a tagállamoktól eredő, kifejezetten a hibrid fenyegetésekre vonatkozó előrejelzésekkel és figyelmeztetésekkel kapcsolatos minősített adatokat és nyílt forrásból származó információkat kapna, elemezne és osztana meg. Az információszintetizáló csoport hasonló, már meglévő uniós[11] és tagállami szintű szervekkel együttműködve elemezné az EU-t és a szomszédos országokat érintő hibrid fenyegetések külső vonatkozásait a releváns váratlan események gyors értékelésének lehetővé tétele, valamint az EU stratégiai döntéshozatali folyamatainak tájékoztatása céljából, ideértve azt is, hogy szakmai hozzájárulást nyújt az uniós szinten végzett kockázatelemzésekhez. Az információszintetizáló csoport elemzési eredményeinek feldolgozása és kezelése a minősített információk és adatok védelmére vonatkozó uniós szabályokkal[12] összhangban történne. A csoport együttműködne már meglévő uniós és nemzeti szervekkel. A

[10] Megbízatásukkal összhangban.
[11] Például, az Europol Számítástechnikai Bűnözés Elleni Európai Központja és Terrorizmus Elleni Központja, a Frontex, az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (CERT) – EU).
[12] Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve

tagállamok feladata, hogy nemzeti kapcsolattartó pontokat állítsanak fel, amelyek összeköttetésben állnak a hibridfenyegetéses információkat szintetizáló uniós csoporttal. Az EU-n belüli és kívüli személyzetet (az uniós küldöttségek alkalmazottait és a műveletek és missziók tagjait is ideértve) és a tagállami személyzetet képzésben kell részesíteni a hibrid veszélyek korai jeleinek felismerésére.

2. intézkedés: Hibrid fenyegetésekre vonatkozó minősített adatok és nyílt forrásból származó információk fogadására és elemzésére képes, a hibridfenyegetéses információkat szintetizáló uniós csoport létrehozása a SitCen-en belül. A tagállamok felkérést kapnak arra, hogy a hibrid fenyegetésekkel foglalkozó nemzeti kapcsolattartó pontokat hozzanak létre, amelyek biztosítják a hibridfenyegetéses információkat szintetizáló uniós csoporttal történő együttműködést és kommunikációt.

3.2. Stratégiai kommunikáció

A hibrid fenyegetések elkövetői módszeres félretájékoztatást alkalmazhatnak többek között a szociális médián keresztül folytatott célirányos kampányok által, amivel az egyének radikalizálását, a társadalom destabilizálását, és a politikai narratíva befolyásolását kívánják elérni. Alapvető fontosságú, hogy képesek legyünk határozott **kommunikációs stratégiával** reagálni a hibrid fenyegetésekre. A társadalom ellenálló képességének erősítése szempontjából döntő tényező a gyors és tényleges válaszreakciókra való képesség és a nyilvánosság figyelmének felhívása a hibrid fenyegetésekre.

A kommunikációs stratégiának teljes mértékben ki kell aknáznia azokat a lehetőségeket, amelyek a közösségi média eszközeiben, valamint az audiovizuális és internetes médiumokban rejlenek. Az EKSZ – a keleti és arab stratégiával és kommunikációval foglalkozó uniós munkacsoportok tevékenységére építve – optimalizálja az olyan, a releváns nem uniós nyelveket folyékonyan beszélő nyelvészek és közösségimédia-szakértők alkalmazását, akik képesek az unión kívülről származó információk nyomon követésére és a félretájékoztatási kampányokra reagáló célzott kommunikáció biztosítására. A tagállamoknak továbbá összehangolt stratégiai kommunikációs mechanizmusokat kell kidolgozniuk a fenyegetés forrása feltárásának elősegítése és a félretájékoztatás megakadályozása érdekében, a hibrid fenyegetések felderítése céljából.

3. intézkedés: A főképviselő a tagállamokkal együtt megvizsgálja a kapacitások modernizálásának és összehangolásának lehetőségeit egy proaktív kommunikációs stratégia kialakítása, valamint a médiafigyelő és nyelvi szakemberek alkalmazásának optimalizálása céljából.

3.3. „A hibrid fenyegetésekkel szembeni fellépéssel” foglalkozó kiválósági központ

Egyes tagállamok és partnerszervezetek[13] tapasztalataira támaszkodva valamelyik nemzetközi intézet, vagy ilyen intézetek hálózata a hibrid fenyegetésekkel foglalkozó kiválósági központként működhetne. Egy ilyen központ fő tevékenysége a hibrid

[13] A NATO kiválósági központok.

stratégiák alkalmazási módjának kutatására irányulhatna, és a központ elősegíthetné olyan új koncepciók és technológiák kifejlesztését a magán- és az ipari szektoron belül, amelyek segítségével a tagállamok erősíteni tudnák ellenálló képességüket. A kutatás megkönnyíthetné az uniós és a nemzeti szakpolitikák, elvek és koncepciók összehangolását, valamint annak biztosítását, hogy a döntéshozatal során figyelembe vegyék a hibrid fenyegetések összetett és nem egyértelmű jellegét. Egy ilyen központ programokat dolgozna ki a hibrid fenyegetések jelentette létező kihívásokra gyakorlati megoldásokat kereső kutatási tevékenység és a gyakorlati megvalósítás elősegítésére. A központ erőssége az a szakértelem lenne, amellyel a különböző nemzetiségű, és különböző – civil és katonai, magán- és tudományos – szférákba tartozó tagjai rendelkeznek.

Ez a központ szorosan együttműködhetne a meglévő uniós[14] és NATO kiválósági központokkal[15] annak érdekében, hogy hasznosíthassa a kibervédelem, stratégiai kommunikáció, polgári-katonai együttműködés, energiagazdálkodás és válságkezelés során a hibrid fenyegetésekre vonatkozóan ott megszerzett tudást.

<u>4. intézkedés</u>: A tagállamok felkérést kapnak arra, hogy vegyék fontolóra a hibrid fenyegetésekkel szembeni fellépéssel foglalkozó kiválósági központ létrehozását.

4. AZ UNIÓS VÁLASZ KIALAKÍTÁSA: AZ ELLENÁLLÓ KÉPESSÉG ERŐSÍTÉSE

Az ellenálló képesség a stressz tűrésére, valamint az arra való képességet jelenti, hogy a kihívásokat megerősödve vészeljük át. A hibrid fenyegetések elleni hatékony fellépés érdekében foglalkozni kell a létfontosságú infrastruktúrák, szállítói láncok és a társadalom lehetséges sebezhető pontjaival. Az uniós eszközökre és szakpolitikákra támaszkodva az uniós szintű infrastruktúra ellenállóbbá tehető.

4.1. A kritikus infrastruktúra védelme

A kritikus infrastruktúrák (például energiaellátási láncok, közlekedés) védelme azért fontos, mert a hibrid fenyegetések elkövetői által bármely „puha célpont” ellen véghezvitt nem hagyományos támadás súlyos gazdasági vagy társadalmi zavarokat okozhat. A kritikus infrastruktúra védelmének biztosítása érdekében a kritikus infrastruktúrák védelmére vonatkozó európai program[16] egy minden veszélyforrást figyelembe vevő, ágazatokon átnyúló megközelítést kínál, amely tekintettel van a kölcsönös függőségekre, és a megelőzés, a felkészültség és reagálás munkafolyamatain belüli tevékenységek kifejtésén alapul. Az európai kritikus infrastruktúrákról szóló irányelv[17] meghatározza az európai kritikus infrastruktúrák (ECI) azonosítására és

[14] Például az EU Biztonságpolitikai Kutatóintézete (EU ISS), vegyi, biológiai, radiológiai és nukleáris kérdésekkel foglalkozó tematikus uniós kiválósági központok.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.
[16] A Bizottság közleménye – A létfontosságú infrastruktúrák védelmére vonatkozó európai programról, 2006.12.12. COM(2006) 786 végleges.
[17] Az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló, 2008. december 8-i 2008/114/EK tanácsi irányelv, HL L 345., 2008.12.23.

kijelölésére irányuló eljárást, valamint a védelmük javítása szükségességének értékelésére irányuló közös megközelítést. Az irányelv alapján újra kell kezdeni a munkát különösen a közlekedési ágazathoz tartozó kritikus infrastruktúrák (például a legfontosabb uniós repülőterek vagy kereskedelmi kikötők) ellenálló képességének erősítése terén. A Bizottság meg fogja vizsgálni, hogy szükséges-e közös eszközök, többek között mutatók kifejlesztése annak érdekében, hogy az összes érintett ágazatban erősíthető legyen a kritikus infrastruktúra hibrid fenyegetésekkel szembeni ellenálló képessége.

<u>5. intézkedés</u>: A Bizottság, a tagállamokkal és az érdekelt felekkel együttműködve közös eszközöket és mutatókat fog meghatározni annak érdekében, hogy javítsa a kritikus infrastruktúrák védelmét és a hibrid fenyegetésekkel szembeni ellenálló képességét az érintett ágazatokban.

4.1.1. Energiahálózatok

A villamos energia zavartalan előállítása és elosztása alapvető fontosságú az EU számára, és a jelentős feszültség-kimaradások károsak lehetnek. A hibrid fenyegetésekkel szembeni fellépés lényeges eleme az uniós energiaforrások, szolgáltatók és útvonalak további diverzifikálása annak érdekében, hogy az energiaellátás biztonságosabb és ellenállóbb legyen. A Bizottság kockázat- és biztonságértékeléseket („stressztesztet”) végez az EU-ban működő erőművek vonatkozásában is. Az energiaellátás diverzifikálásának biztosítása érdekében intenzívebb munka folyik az energiaunióra vonatkozó stratégia alapján: például, a Déli Gázfolyosó lehetővé teszi, hogy a Kaszpi-tengeri térségből származó földgáz eljusson Európába, Észak-Európában pedig több szállítón alapuló, cseppfolyósított gáz elosztását végző központok kiépítése folyik. Ezt a példát Közép- és Kelet-Európában és a földközi-tengeri térségben is követni kell, ahol jelenleg folyamatban van egy gázelosztó központ kialakítása[18]. A cseppfolyósított földgáz piacának fejlesztése szintén elő fogja segíteni ennek a célnak az elérését.

A nukleáris anyagok és létesítmények vonatkozásában a Bizottság a legszigorúbb biztonsági normák kialakítását és elfogadását támogatja, ezáltal is erősítve az ellenálló képességet. A Bizottság szorgalmazza a nukleáris biztonságról szóló irányelv[19] következetes átültetését és végrehajtását, amely meghatározza a balesetek megelőzésére vagy a balesetek következményeinek enyhítésére vonatkozó szabályokat, valamint az alapvető biztonsági előírásokról szóló irányelv[20] veszélyhelyzetre való felkészüléssel és annak elhárításával kapcsolatos nemzetközi – különösen szomszédos tagállamok közötti

[18] Az eddig elért előrehaladásról lásd az energiaunió helyzetéről szóló közleményt, 2015 (COM(2015) 572 final.

[19] A 2014. július 8-i 2014/87/Euratom tanácsi irányelvvel módosított, a nukleáris létesítmények nukleáris biztonsági közösségi keretrendszerének létrehozásáról szóló, 2009. június 25-i 2009/71/Euratom tanácsi irányelv.

[20] Az ionizáló sugárzás miatti sugárterhelésből származó veszélyekkel szembeni védelmet szolgáló alapvető biztonsági előírások megállapításáról, valamint a 89/618/Euratom, a 90/641/Euratom, a 96/29/Euratom, a 97/43/Euratom és a 2003/122/Euratom irányelv hatályon kívül helyezéséről szóló, 2013. december 5-i 2013/59/Euratom tanácsi irányelv.

és szomszédos országokkal való – együttműködésre vonatkozó rendelkezéseinek átültetését és végrehajtását.

<u>6. intézkedés</u>: A Bizottság – a tagállamokkal együttműködésben – támogatni fogja az energiaforrások diverzifikálására irányuló erőfeszítéseket, és a nukleáris infrastruktúrák ellenálló képességének erősítése érdekében elő fogja segíteni biztonsági és védelmi követelmények bevezetését.

4.1.2. A közlekedési ágazat és az ellátási láncok biztonsága

A közlekedési ágazat alapvető fontosságú az Unió működése szempontjából. A közlekedési infrastruktúrát (például repülőtereket, közúti infrastruktúrákat, kikötőket, vasutakat) érő hibrid támadások az utazás és a szállítói láncok terén zavarokat okozó, komoly következményekkel járhatnak. A légi és tengeri közlekedés biztonságára vonatkozó jogszabályok[21] végrehajtása keretében a Bizottság rendszeres ellenőrzéseket végez[22], a közúti közlekedésbiztonság terén végzett munkája által pedig a felmerülő hibrid fenyegetések kezelésére törekszik. Ebben az összefüggésben, a felülvizsgált repülésbiztonsági rendelet[23] keretében egy uniós keretszabályozás megvitatása zajlik, amely az európai légi közlekedési stratégia[24] részét képezi. Emellett, a tengerhajózás biztonságát fenyegető veszélyek kezelése az Európai Unió tengerhajózási biztonsági stratégiája és az ahhoz kapcsolódó cselekvési terv[25] keretében történik. Ez utóbbi lehetővé teszi az EU és tagállamai számára a tengeri biztonsági kihívások átfogó kezelését – és ezzel egyidejűleg a hibrid fenyegetésekkel szembeni fellépést – a civil és a katonai szereplők közötti ágazatközi együttműködés révén, amelynek célja a kritikus tengeri infrastruktúrák, átfogó ellátási láncok, a tengeri kereskedelem, valamint a tengeri természeti erőforrások és energiaforrások védelme. A nemzetközi ellátási lánc biztonságával az uniós vámügyi kockázatkezelési stratégia és cselekvési terv[26] is foglalkozik.

---

[21] Az Európai Parlament és a Tanács 2008. március 11-i 300/2008/EK rendelete a polgári légi közlekedés védelmének közös szabályairól és a 2320/2002/EK rendelet hatályon kívül helyezéséről; a Bizottság 2015. november 5-i (EU) 2015/1998 végrehajtási rendelete a közös légiközlekedés-védelmi alapkövetelmények végrehajtásához szükséges részletes intézkedések meghatározásáról; az Európai Parlament és a Tanács 2005. október 26-i 2005/65/EK irányelve a kikötővédelem fokozásáról; az Európai Parlament és a Tanács 2004. március 31-i 725/2004/EK rendelete a hajók és kikötő-létesítmények védelmének fokozásáról.

[22] Az uniós jog értelmében a Bizottság köteles ellenőrzéseket végezni annak biztosítása érdekében, hogy a tagállamok helyesen hajtsák végre a légiközlekedés-védelmi és tengerhajózási biztonsági követelményeket. Ez magában foglalja az illetékes tagállami hatóság ellenőrzését, valamint a repülőterek, kikötők, légi fuvarozók, hajók és biztonsági intézkedéseket végrehajtó szervezetek ellenőrzését. A bizottsági ellenőrzések célja annak biztosítása, hogy az uniós standardokat a tagállamok maradéktalanul végrehajtsák.

[23] A Bizottság 2016. január 5-i (EU) 2016/4 rendelete a 216/2008/EK európai parlamenti és tanácsi rendeletnek a környezet védelmére vonatkozó alapvető követelmények tekintetében történő módosításáról; az Európai Parlament és a Tanács 2008. február 20-i 216/2008/EK rendelete a polgári repülés területén közös szabályokról és az Európai Repülésbiztonsági Ügynökség létrehozásáról.

[24] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Európai légi közlekedési stratégia, COM/2015/0598 final, 2015.12.7.

[25] A Tanács 2014 decemberében cselekvési tervet fogadott el az Európai Unió tengerhajózási biztonsági stratégiájának végrehajtására; http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

[26] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak és az Európai Gazdasági és Szociális Bizottságnak az uniós vámügyi kockázatkezelési stratégiáról és cselekvési tervről: a kockázatok kezelése, az ellátási lánc biztonságának megerősítése és a kereskedelem előmozdítása, COM (2014) 527 final.

<u>7. intézkedés</u>: A Bizottság figyelemmel fogja kísérni a közlekedési ágazatban felmerülő fenyegetéseket és adott esetben aktualizálni fogja a jogszabályokat. Az Európai Unió tengerhajózási biztonsági stratégiájának, valamint vámügyi kockázatkezelési stratégiájának és cselekvési tervének végrehajtása során a Bizottság és a főképviselő (saját hatáskörükön belül) – a tagállamokkal koordinálva – meg fogják vizsgálni, hogy milyen válaszlépések tehetők a hibrid fenyegetésekre, különösen azokra, amelyek a kritikus közlekedési infrastruktúrákat érintik.

4.1.3 Űrpolitika

A hibrid fenyegetések a világűrbe telepített infrastruktúrákat is célba vehetik, ami számos ágazatra nézve következményekkel járhat. Az EU az űrmegfigyelést és a Föld körüli pályán haladó objektumok nyomon követését támogató keretet[27] dolgozott ki, amelynek célja, hogy létrehozza azoknak az eszközöknek a hálózatát, amelyekkel egyes tagállamok rendelkeznek, és azonosított felhasználók (tagállamok, uniós intézmények, űrjárművek tulajdonosai és üzemeltetői valamint polgári védelmi hatóságok) számára űrmegfigyelési és nyomon követési szolgáltatásokat[28] nyújtanak. A majdani európai űrstratégia keretében a Bizottság meg fogja vizsgálni, hogyan lehet azt úgy továbbfejleszteni, hogy alkalmas legyen a világűrbe telepített infrastruktúrák elleni hibrid fenyegetések nyomon követésére.

A műholdas kommunikáció (SatCom) a válságkezelés, a katasztrófaelhárítás, a rendőrségi és határrendészeti megfigyelés és a parti őrség kulcsfontosságú eszközei. Olyan nagyszabású infrastruktúrák gerincét képezik, mint például a közlekedési- és űrinfrastruktúra, vagy a távirányítású légijármű-rendszerek. Az állami műholdas kommunikáció (GovSatCom) következő generációjának előkészítésére irányuló európai tanácsi felhívással összhangban a Bizottság, az Európai Védelmi Ügynökséggel együttműködve, megvizsgálja az igények egyesítésének lehetőségeit a majdani európai űrstratégia és európai védelmi cselekvési terv keretében.

Számos kritikus infrastruktúra esetében a hálózatok szinkronizáláshoz pontos időadatokra van szükség (például energia és a távközlés, vagy időbélyegzős tranzakciók, például a pénzügyi piacokon). Egyetlen globális navigációs műholdrendszer időszinkronizáló jelétől való függőség nem biztosítja a hibrid fenyegetésekkel szembeni fellépéshez szükséges ellenálló képességet. A Galileo, az európai globális navigációs műholdrendszer egy második megbízható időzítési forrást kínálna.

<u>8. intézkedés</u>: A majdani európai űrstratégia és európai védelmi cselekvési terv keretében a Bizottság javasolni fogja a világűrbe telepített infrastruktúra hibrid fenyegetésekkel szembeni ellenálló képességének erősítését, különösen az űrmegfigyelési és nyomon követési rendszer hatályának a hibrid fenyegetésekre történő kiterjesztésével, a GovSatCom európai szintű új generációjának létrehozásával,

[27] Lásd az Európai Parlament és a Tanács 541/2014/EU határozatát.
[28] Például keringési pályán való ütközés elkerülésére vonatkozó előrejelzés, űrobjektumok felbomlására, összeütközésére vagy a Föld légkörébe való veszélyes visszajutására vonatkozó riasztás.

valamint a Galileo használatának bevezetésével olyan kritikus infrastruktúrák esetében, amelyek működéséhez elengedhetetlen az időszinkronizálás.

4.2. Védelmi képességek

Az EU hibrid fenyegetésekkel szembeni ellenálló képességének erősítéséhez szükség van a védelmi képességek javítására. Fontos a kulcsfontosságú képességi területek – például megfigyelési és felderítési képesség – meghatározása. Az Európai Védelmi Ügynökség katalizátorként szolgálhat a hibrid fenyegetésekkel kapcsolatos katonai képességfejlesztés terén (például a védelmi képességek fejlesztési ciklusainak lerövidítése, technológiákba, rendszerekbe és prototípusokba való befektetés révén, vagy a védelmi üzletág megnyitása által az innovatív kereskedelmi technológiák felé). A lehetséges intézkedéseket a majdani európai védelmi cselekvési terv keretében lehetne vizsgálni.

9. intézkedés: A főképviselő, adott esetben a tagállamok támogatásával és a Bizottsággal együttműködve projekteket fog javasolni arra vonatkozóan, hogy az uniós relevanciájú védelmi képességek és az azokat érintő fejlesztések milyen módon tehetők alkalmassá kifejezetten a valamely tagállammal vagy tagállamokkal szembeni hibrid fenyegetések leküzdésére.

4.3. A közegészségügy és az élelmezésbiztonság védelme

A lakosság egészsége veszélybe kerülhetne fertőző betegségek manipulációja vagy az élelmiszerek, a talaj, a levegő vagy az ivóvíz vegyi, biológiai, radiológiai és nukleáris anyagokkal (CBRN) való szennyezése folytán. Ezen kívül, az állat- vagy növénybetegségek szándékos terjesztése súlyosan érintheti az Unió élelmezésbiztonságát, és jelentős gazdasági és társadalmi hatássokkal járhat az uniós élelmiszerlánc alapvető fontosságú területein. A közegészség-védelem, környezetvédelem és élelmiszer-biztonság területén meglévő uniós struktúrák felhasználhatók az ilyen módszereket használó hibrid fenyegetésekkel szembeni védekezés céljából.

A határokon átterjedő súlyos egészségügyi veszélyekre vonatkozó uniós jog[29] létrehozott olyan mechanizmusokat, amelyek a határokon átterjedő súlyos egészségügyi veszélyekre való felkészültséget koordinálják, a fertőzőbetegség-figyelői és gyorsreagáló rendszer által összeköttetést teremtve a tagállamok, az uniós ügynökségek és a tudományos bizottságok között[30]. A fenyegetésekre adandó tagállami válaszokat koordináló Egészségbiztonsági Bizottság a közegészségügyet fenyegető veszélyek vonatkozásában kapcsolattartási pontként működhetne[31] annak érdekében, hogy a hibrid fenyegetések

[29] Az Európai Parlament és a Tanács 2013. október 22-i 1082/2013/EU határozata a határokon átterjedő súlyos egészségügyi veszélyekről és a 2119/98/EK határozat hatályon kívül helyezéséről (HL L 293/1., 2013.11.5.).

[30] A Bizottság 2015. augusztus 7-i C(2015) 5383 határozata a közegészségügy, a fogyasztók biztonsága és a környezetvédelem területén tudományos bizottságok létrehozásáról.

[31] A határokon átterjedő súlyos egészségügyi veszélyekről és a 2119/98/EK határozat hatályon kívül helyezéséről szóló, 2013. október 22-i 1082/2013/EU európai parlamenti és tanácsi határozattal (HL L 293/1.) összhangban.

(különösen a biológiai terrorizmus) a válságkommunikációs iránymutatások és a tagállamokkal végzett (válságszimulációs) kapacitásépítési gyakorlatok fókuszába kerüljenek. Az élelmiszerbiztonság területén az illetékes hatóságok az élelmiszerekre és takarmányokra vonatkozó sürgősségi riasztórendszeren (RASFF), és a közös vámügyi kockázatkezelési rendszeren (CRMS) keresztül a kockázatelemzésre vonatkozó információcserét folytatnak annak érdekében, hogy nyomon követhessék a szennyezett élelmiszerek által okozott egészségügyi kockázatokat. Az állat- és növény-egészségügy terén az uniós jogi keret felülvizsgálata[32] új elemekkel fogja bővíteni a jelenlegi eszköztárat[33] annak érdekében, hogy a felkészültség a hibrid fenyegetések vonatkozásában is javuljon.

10. intézkedés: A Bizottság – a tagállamokkal együttműködésben – a meglévő készültségi és koordinációs mechanizmusokon, különösen az Egészségügyi Biztonsági Bizottságon belül növelni fogja a hibrid fenyegetésekkel kapcsolatos tudatosságot, és a velük szembeni ellenálló képességet.

4.4. Kiberbiztonság

Az EU tagállamai az összekapcsolt digitalizált társadalom számos előnyét élvezik. A kibertámadások megzavarhatják az EU egészére kiterjedő digitális szolgáltatásokat, és a hibrid fenyegetések elkövetői alkalmazhatnak ilyen támadásokat. A kommunikációs és információs rendszerek ellenálló képességének erősítése fontos az európai digitális egységes piac támogatása érdekében. Az EU kiberbiztonsági stratégiája és az európai biztonsági stratégia átfogó stratégiai keretet biztosít a kiberbiztonsággal és a számítástechnikai bűnözés kérdésével foglalkozó uniós kezdeményezések számára. A kiberbiztonsági stratégia keretében elérendő eredmények körében az EU aktív szerepet játszik a tudatosság, az együttműködési mechanizmusok és válaszlépések kialakításában. Konkrétan, a hálózat- és információbiztonságról szóló irányelvjavaslat[34] az energiaszolgáltatási, közlekedési, pénzügyi és egészségügyi ágazatban kritikus szolgáltatások nyújtóinak széles körét érintő kiberbiztonsági kockázatokkal foglalkozik. Ezeknek a szolgáltatóknak, csakúgy, mint az alapvető digitális szolgáltatások (például felhőalapú számítástechnika) nyújtóinak megfelelő biztonsági intézkedéseket kell tenniük és a súlyos váratlan eseményeket jelenteniük kell a nemzeti hatóságoknak, melynek során fel kell hívniuk a figyelmet bármely hibrid jellemzőre. Ha a társjogalkotók elfogadták, az irányelv hatékony átültetése és végrehajtása javíthatja a tagállamok kiberbiztonsági képességeit, a hibrid fenyegetések elleni küzdelemre vonatkozó információcsere és a

[32] Az Európai Parlament és a Tanács (EU) 2016/429 rendelete a fertőző állatbetegségekről és egyes állategészségügyi jogi aktusok módosításáról és hatályon kívül helyezéséről („Állat-egészségügyi rendelet") (HL L 84., 2016.3.31.). A károsítókkal szembeni védelmi intézkedésekről szóló európai parlamenti és tanácsi rendelet („növény-egészségügyi rendelet") szövege tekintetében az Európai Parlament és a Tanács 2015. december 16-án politikai megállapodásra jutott.

[33] Így például uniós vakcinabankok, az állatbetegségek fejlett elektronikus információs rendszere, kórokozókkal foglalkozó laboratóriumok és más szervezetek által hozott intézkedésekkel szembeni szigorúbb követelmények.

[34] A hálózat- és információbiztonságnak az egész Unióban egységesen magas szintjére vonatkozó intézkedésekről szóló európai parlamenti és tanácsi irányelvre vonatkozó bizottsági javaslat COM(2013) 48 final – 2013/2/7. Az említett irányelvjavaslatra vonatkozóan politikai megállapodás jött létre az EU Tanácsa és az Európai Parlament között, és hamarosan megtörténik az irányelv hivatalos elfogadása.

legjobb gyakorlatok cseréje által megerősítve együttműködésüket a kiberbiztonság terén. Az irányelv 28 nemzeti hálózatbiztonsági incidenselhárító csoport (CSIRT) és hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT-EU) létrehozásáról rendelkezik[35], az önkéntes alapon történő operatív együttműködés biztosítása céljából.

Az állami és a magánszektor közötti együttműködés, valamint egy uniós szintű kiberbiztonsági koncepció kialakításának ösztönzése céljából a Bizottság hálózat- és információbiztonsági (NIS) platformot hozott létre, amely kidolgozza a kockázatkezelés terén alkalmazott legjobb gyakorlatokra vonatkozó iránymutatásokat. Míg a biztonsági követelményeket és a váratlan események bejelentésének gyakorlati szabályait a tagállamok határozzák meg, a Bizottság a kockázatkezelési mechanizmusok nagymértékű – különösen az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) keretében történő – közelítésére ösztönöz.

<u>11. intézkedés</u>: A Bizottság arra ösztönzi a tagállamokat, hogy haladéktalanul hozzák létre és teljes mértékben használják ki a 28 CSIRT és CERT-EU hálózatát, valamint a stratégiai együttműködés keretét. A Bizottságnak a tagállamokkal együttműködve biztosítania kell, hogy a számítógépes fenyegetésekre irányuló ágazati (például légi közlekedési, energiaügyi, tengerhajózási) kezdeményezések összhangban legyenek a kiberbiztonsági irányelv hatálya alá tartozó, az információ, a szakértelem és a gyors válaszok egyesítésére vonatkozó ágazatközi képességekkel.

4.4.1. Ipar

A felhőalapú számítástechnikára és az óriási méretű adathalmazokra való fokozott támaszkodás következtében nagyobb a hibrid fenyegetésekkel szembeni sebezhetőség. A digitális egységes piaci stratégia létrehozta a szerződéses kiberbiztonsági köz-magán társulás intézményét[36], amelynek középpontjában a kutatás és az innováció fog állni, és amelynek segítségével az Unió továbbra is magas szintű technológiai kapacitással rendelkezhet ezen a területen. A szerződéses köz- és magántársulások hozzájárulnak majd a különböző piaci szereplők közötti bizalom és a keresleti és kínálati oldal közti szinergiák kialakításához. Bár a szerződéses köz-magán társulások és a kísérő intézkedések elsősorban a polgári kiberbiztonsági termékekre és szolgáltatásokra fognak összpontosítani, az ilyen kezdeményezéseknek végső soron ahhoz is hozzá kell járulniuk, hogy a technológiát használók a hibrid fenyegetésekkel szemben is védettebbé válnak.

<u>12. intézkedés</u>: A Bizottság – a tagállamokkal koordinálva – szerződéses kiberbiztonsági köz-magán társulás keretében együtt fog működni az iparággal olyan technológiák kifejlesztése és tesztelése céljából, amelyek a felhasználók és az infrastruktúrák számára hatékonyabb védelmet nyújtanak a hibrid fenyegetések számítástechnikai aspektusaival szemben.

[35] Az uniós intézményeknél működő, hálózatbiztonsági vészhelyzeteket elhárító csoport (CERT-EU).
[36] Bevezetése a tervek szerint 2016 közepétől kezdődik.

4.4.2. Energia

Az intelligens otthonok és készülékek elterjedésével, és az intelligens hálózat kifejlesztésével az energetikai rendszer fokozódó digitalizációja szintén növeli a kibertámadásokkal szembeni sebezhetőséget. Az európai energiabiztonsági stratégia[37] és az energiaunióra vonatkozó stratégia[38] olyan, minden veszélyforrást figyelembe vevő megközelítést támogat, amely magában foglalja a hibrid fenyegetésekkel szembeni ellenálló képességet. A kritikus energetikai infrastruktúrák védelmével foglalkozó tematikus hálózat elősegíti az energiaágazaton (olaj, gáz, villamos energia) belüli szereplők közötti együttműködést. A Bizottság a fenyegetésekre és váratlan eseményekre vonatkozó információk elemzése és megosztása érdekében internetes platformot hozott létre[39]. Ezen kívül az érdekelt felekkel együttműködve[40] az energiaágazaton belüli intelligens energiahálózatok működésére vonatkozó átfogó kiberbiztonsági stratégia kialakításán is dolgozik, amelynek célja a sebezhetőség csökkentése. Míg a villamosenergia-piacok egyre inkább összekapcsolódnak, a válsághelyzetek kezelésére vonatkozó szabályok és eljárások változatlanul tagállami keretek közt maradnak. Biztosítanunk kell, hogy a kormányok együttműködjenek egymással a kockázatokra való felkészülés, azok megelőzése és hatásainak csökkentése terén, valamint, hogy minden érintett szereplő közös szabályok alapján járjon el.

13. intézkedés: A Bizottság a berendezések kiberbiztonságának növelésére vonatkozó iránymutatást fog kiadni az intelligens energiahálózattal működő eszközök tulajdonosai részére. A villamosenergia-piac szerkezetének átalakítására vonatkozó kezdeményezés keretében a Bizottság megfontolja annak lehetőségét, hogy „kockázati készültségi tervek", valamint olyan eljárási szabályok megalkotására tegyen javaslatot, amelyek válság idején biztosítják a tagállamok közti információmegosztást és szolidaritást, ideértve a kibertámadások megelőzésére és hatásainak enyhítésére vonatkozó szabályokat is.

4.4.3. A pénzügyi rendszerek szilárdságának biztosítása

Az uniós gazdaság működéséhez biztonságos pénzügyi és fizetési rendszerre van szükség. A támadó szándékaitól vagy jellegétől függetlenül elengedhetetlen a pénzügyi rendszer és az ahhoz kapcsolódó infrastruktúra védelme a kibertámadásokkal szemben. Az uniós pénzügyi szolgáltatásokat fenyegető hibrid fenyegetésekkel szembeni fellépés érdekében az ágazatnak tisztában kell lennie a fenyegetettséggel, fel kell mérnie védekezési képességeit, és rendelkezni kell az ágazat támadásokkal szembeni védelméhez szükséges technológiával. Ennek megfelelően alapvető fontosságú a fenyegetésekről szóló információk megosztása a pénzügyi piaci szereplőkkel, az illetékes hatóságokkal, a kulcsfontosságú szolgáltatások nyújtóival és a szolgáltatások igénybevevőivel, azonban az információmegosztásnak biztonságosnak is kell lennie, és meg kell felelnie az adatvédelmi követelményeknek. A G7-ek által a nemzetközi

[37] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: Európai energiabiztonsági stratégia – COM/2014/0330 final.
[38] „A stabil és alkalmazkodóképes energiaunió és az előretekintő éghajlat-politika keretstratégiája" című közlemény – COM/2015/080 final.
[39] A váratlan eseményekkel és veszélyekkel kapcsolatos uniós információcsere-központ – ITIS.
[40] Energiaügyi kiberbiztonsági szakértői platform (EECSP).

fórumokon ebben az ágazatban végzett munkával összhangban a Bizottság törekedni fog arra, hogy azonosítsa azokat a tényezőket, amelyek akadályozzák a fenyegetésekre vonatkozó információk megfelelő megosztását, és megoldásokat fog javasolni. Biztosítani kell a rendszeres tesztelést és az eljárások finomítását az üzleti tevékenység és a kapcsolódó infrastruktúrák védelme érdekében, a biztonságot növelő technológiák folyamatos fejlesztése által is.

<u>14. intézkedés</u>: A Bizottság – az ENISA[41], a tagállamok, a releváns nemzetközi, európai és nemzeti hatóságok, valamint a pénzügyi intézmények közreműködésével – elősegíti és megkönnyíti a fenyegetésekre vonatkozó információk cseréjét szolgáló platformok és hálózatok működését, és foglalkozni fog az ilyen információk cseréjét akadályozó tényezőkkel.

4.4.4. Közlekedés

A modern közlekedési rendszerek (vasúti, közúti, légi, tengeri) olyan információs rendszereken alapulnak, amelyek kibertámadások célpontjai lehetnek. Tekintettel a közlekedési ágazat uniós dimenziójára, az EU különösen fontos szerepet játszik. A Bizottság a tagállamokkal együttműködve folytatni fogja a közlekedési rendszerekbe történő jogellenes beavatkozásokkal együtt járó számítógépes fenyegetések és kockázatok elemzését. A Bizottság az Európai Repülésbiztonsági Ügynökséggel (EASA) együttműködve kiberbiztonsági ütemtervet dolgoz ki a légi közlekedésre vonatkozóan[42]. A tengerhajózás biztonságát fenyegető számítógépes veszélyforrásokkal az Európai Unió tengerhajózási biztonsági stratégiája is foglalkozik.

<u>15. intézkedés</u>: A Bizottság és a főképviselő (saját hatáskörükön belül) – a tagállamokkal koordinálva – meg fogják vizsgálni, hogy milyen válaszlépések tehetők a hibrid fenyegetésekre, különösen azokra, amelyek a közlekedési ágazat elleni kibertámadásokat érintik.

4.5. A hibrid fenyegetések finanszírozásának megakadályozása

A hibrid fenyegetések elkövetőinek anyagi forrásokra van szükségük tevékenységük fenntartásához. A finanszírozás felhasználható terrorista csoportok támogatására, vagy a destabilizáció kifinomultabb formáihoz, például érdekérvényesítő csoportok vagy marginális politikai pártok támogatására. Az EU intenzívebbé tette a bűnözés és a terrorizmus finanszírozása elleni erőfeszítéseket, amint az az európai biztonsági

[41] Európai Uniós Hálózat- és Információbiztonsági Ügynökség

[42] Az új EASA-rendeletről a Bizottság 2015. decemberi javaslata alapján jelenleg tárgyal az Európai Parlament és a Tanács. A polgári repülés területén alkalmazandó közös szabályokról és az Európai Unió Repülésbiztonsági Ügynökségének létrehozásáról, valamint a 216/2008/EK európai parlamenti és tanácsi rendelet hatályon kívül helyezéséről szóló európai parlamenti és tanácsi rendeletre irányuló javaslat – COM(2015) 613 final, 2015/0277 (COD).

stratégiában, és különösen a cselekvési tervben szerepel[43]. Ezzel kapcsolatban konkrétan, a pénzmosás elleni küzdelem felülvizsgált európai keretrendszere megerősíti a terrorizmus finanszírozása és a pénzmosás elleni küzdelmet, megkönnyíti a tagállami pénzügyi információs egységek (FIU-k) munkáját a gyanús pénzátutalások és információcserék azonosítása és nyomon követése terén, és biztosítja a pénzeszközök átutalásának nyomonkövethetőségét az Európai Unión belül. Ezáltal a hibrid fenyegetések elleni küzdelemhez is hozzájárulhat. A közös kül- és biztonságpolitika eszközeinek keretében célzott és hatékony korlátozó intézkedéseket lehetne igénybe venni a hibrid fenyegetésekkel szembeni fellépés érdekében.

16. intézkedés: A Bizottság a terrorizmus finanszírozása elleni küzdelemről szóló cselekvési terv végrehajtását a hibrid fenyegetésekkel szembeni fellépés céljaira is fel fogja használni.

4.6. A radikalizálódással és az erőszakos szélsőségességgel szembeni ellenálló képesség erősítése

Bár a terrorcselekmények és az erőszakos szélsőségesség önmagukban véve nem hibrid jellegűek, a hibrid fenyegetések elkövetői célba vehetik és beszervezhetik a társadalom kiszolgáltatott tagjait, a modern kommunikációs csatornák (többek között az internetes közösségi média és közvetítő csoportok) és a propaganda eszközeivel radikalizálva őket.

A Bizottság annak érdekében, hogy fellépjen az interneten megjelenő szélsőséges tartalmak ellen, a digitális egységes piaci stratégia keretében elemzi a lehetséges új intézkedések szükségességét, megfelelően tekintetbe véve azok hatását olyan alapvető jogokra, mint a véleménynyilvánítás és a tájékozódás szabadsága. Ez magában foglalhatja az illegális tartalmak eltávolítására irányuló szigorú eljárásokat – a jogszerű tartalom eltávolításának elkerülésével – („tudomásszerzés és cselekvés”), valamint a szolgáltatók részéről nagyobb felelősséget és gondosságot a hálózataik és rendszereik kezelésében. Ez kiegészítené a meglévő önkéntes megközelítést, amelynek során az internetes és a közösségi médiát üzemeltető vállalatok (különösen az Európai Uniós Internetfórum égisze alatt) – az Europol szélsőséges internetes tartalmakkal foglalkozó uniós egységével együttműködve – haladéktalanul eltávolítják a terrorista propagandát.

Az európai biztonsági stratégia keretében a radikalizálódás elleni fellépés a tapasztalatcserét és a legjobb gyakorlatok kidolgozását foglalja magában, ideértve a harmadik országokkal folytatott együttműködést is. A Szíriával foglalkozó stratégiai kommunikációs tanácsadó csoport célja, hogy a terrorista propaganda ellensúlyozása érdekében erősítse az alternatív üzenetek kidolgozását és terjesztését. Az uniós radikalizálódás-tudatossági hálózat olyan tagállamokat és szakembereket támogat, amelyeknek, illetve akiknek radikalizálódott egyénekkel (többek között külföldi terrorista harcosokkal), vagy a radikalizálódással szemben kiszolgáltatott egyénekkel kell kapcsolatban állniuk. Az uniós radikalizálódás-tudatossági hálózat képzési és tanácsadási

[43] A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak a terrorizmus finanszírozása elleni küzdelem megerősítésére irányuló cselekvési tervről – (COM(2016) 50 final)

tevékenységet folytat, és támogatást fog nyújtani olyan kiemelt harmadik országoknak, amelyek készen állnak az együttműködésre. A Bizottság továbbá a tagállamokban megjelenő terrorizmus és radikalizálódás leküzdése céljából előmozdítja a büntető igazságszolgáltatás szereplői – ideértve az Eurojustot is – közötti igazságügyi együttműködést, amely a külföldi terrorista harcosok és a háborús térségekből visszatérők kezelésére is kiterjed.

A fenti megközelítéseket a **külső tevékenysége** terén kiegészítve, az EU hozzájárul az erőszakos szélsőségesség elleni küzdelemhez, többek között külső szerepvállalással, tájékoztatással és megelőzéssel (a radikalizálódás és a terrorizmus finanszírozása elleni küzdelemmel), valamint olyan intézkedések révén, amelyek a háttérben húzódó, a terrorista csoportok térnyerését lehetővé tévő gazdasági, politikai és társadalmi tényezők kiküszöbölésére irányulnak.

<u>17. intézkedés:</u> A Bizottság végrehajtja az európai biztonsági stratégia radikalizálódással szembeni intézkedéseit, és jelenleg azt vizsgálja, hogy szükség van-e az illegális tartalmak eltávolítására irányuló eljárások megerősítésére, és a szolgáltatók arra való kötelezésére, hogy kellő gondossággal kezeljék a hálózatokat és rendszereket.

4.7. A harmadik országokkal folytatott együttműködés megerősítése

Az európai biztonsági stratégiában kiemelten szerepel, hogy az EU fokozott figyelmet fordít ***a partnerországok*** biztonsági ágazatában történő kapacitásépítésre többek között azáltal, hogy a biztonság és a fejlesztés közötti kapcsolatot erősíti, és kialakítja a felülvizsgált európai szomszédságpolitika biztonsági dimenzióját[44]. Ezek az intézkedések emellett erősíthetik a partnerek hibrid fenyegetésekkel szembeni ellenálló képességét is.

A Bizottság tovább kívánja fokozni az operatív és stratégiai információk cseréjét a bővítési folyamatban részt vevő országokkal, a keleti partnerségen és a déli szomszédságon belül, a szervezett bűnözés, a terrorizmus, az illegális migráció és a kézi- és könnyűfegyverek kereskedelme elleni küzdelem elősegítéséhez szükséges mértékben. A terrorizmus elleni küzdelem terén az EU a harmadik országokkal folytatott együttműködést azáltal fokozza, hogy magasabb szintű biztonsági párbeszédet és cselekvési terveket alakít ki.

Az uniós külső finanszírozási eszközök célja, hogy harmadik országokban működő és elszámoltatható intézményeket hozzon létre[45] amelyek elengedhetetlenek a biztonsági fenyegetések hatékony kezeléséhez és az ellenálló képesség fokozásához. Ebben az összefüggésben, a biztonsági ágazat reformja és a kapacitásépítés kulcsfontosságú

[44] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az európai szomszédságpolitika felülvizsgálata, 2015.11.18., JOIN(2015) 50 final.

[45] Ugyanott; A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Az EU bővítési stratégiája, 2015.11.10., COM(2015) 611 final. A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Változtatási program: az EU fejlesztéspolitikájának hathatósabbá tétele, 2011.10.13., COM(2011) 637 végleges.

eszközök a biztonság és a fejlesztés támogatása szempontjából[46]. A stabilitás és a béke elősegítését szolgáló eszköz[47] keretében a Bizottság olyan intézkedéseket dolgozott ki, amelyek erősítik a számítógépes támadásokkal szembeni ellenálló képességet és a partnerek arra való képességét, hogy észleljék a kibertámadásokat és a kiberbűnözést, és megfelelő választ adjanak azokra. Ez lehetővé teszi a hibrid fenyegetésekkel szembeni fellépést a harmadik országokban. Az EU támogatást nyújt a partnerországok kapacitásépítési tevékenységeihez a vegyi, biológiai, radiológiai és nukleáris anyagokkal (CBRN) kapcsolatos biztonsági kockázatok[48] enyhítése érdekében.

Végül, a válságkezelés átfogó megközelítésének szellemében a tagállamok az alkalmazott uniós eszközöktől függetlenül vagy azokat kiegészítve olyan közös biztonság- és védelempolitikai (KBVP) eszközöket alkalmazhatnának, amelyek segítik a partnereket kapacitásaik erősítésében. Megfontolásra érdemesek a következő intézkedések: i. stratégiai kommunikáció támogatása, ii. hibrid fenyegetéseknek kitett kulcsfontosságú minisztériumoknak nyújtott tanácsadó támogatás; iii. vészhelyzet esetében kiegészítő határigazgatási támogatás. További szinergiákat lehetne feltárni a KBVP eszközei és a biztonság, a vámügy és a jogérvényesítés területén működő szereplők között, ideértve a releváns uniós ügynökségeket[49], az Interpolt és az európai csendőrséget, hatásköreiknek megfelelően.

<u>18. intézkedés</u>: A főképviselő, a Bizottsággal együttműködve, kezdeményezni fogja a szomszédos régiókban a hibrid fenyegetések jelentette kockázatokra vonatkozó felmérés készítését.

A főképviselő, a Bizottság és a tagállamok a rendelkezésükre álló eszközöket fel fogják használni a partnerek kapacitásépítése és hibrid fenyegetésekkel szembeni ellenálló képessége erősítése érdekében. Az uniós eszközöktől függetlenül vagy azokat kiegészítve KBVP-missziókat lehetne indítani a partnerek kapacitásnövelésének elősegítése céljából.

5. A VÁLSÁG MEGELŐZÉSE, KEZELÉSE ÉS HATÁSAINAK ELHÁRÍTÁSA

Amint az a 3.1. szakaszban szerepel, a hibridfenyegetéses információkat szintetizáló, javasolt európai uniós csoport tevékenységének célja, hogy a hibrid fenyegetések megakadályozása és az azokra történő reagálás, valamint az uniós döntéshozók tájékoztatása céljából elemezze a releváns mutatókat. Bár a gyenge pontok hosszú távú, tagállami és uniós szakpolitikák révén kiküszöbölhetők, rövid távon elengedhetetlenül szükséges marad a tagállamok és az Unió azon képességeinek erősítése, amelyek

[46] Közös közlemény – „A biztonságot és a fejlesztést szolgáló kapacitásépítés – A partnerek felkészítése a válságmegelőzésre és -kezelésre” (JOIN(2015) 17final).
[47] Az Európai Parlament és a Tanács 2014. március 11-i 230/2014/EU rendelete a stabilitás és a béke elősegítését szolgáló eszköz létrehozásáról (HL L 77/1., 2014.3.15.).
[48] Ide tartozik többek között a határmegfigyelés, válságkezelés, azonnali reagálás, a kettős felhasználású termékek illegális kereskedelmének és exportjának ellenőrzése, járványfelügyelet és -ellenőrzés, nukleáris kriminalisztika, váratlan események hatásainak elhárítása, veszélyes létesítmények védelme. Az uniós CBRN cselekvési terv keretében kialakított eszközökön – például az Európai Nukleáris Védettségi Képzési Központ, vagy a határmegfigyeléssel foglalkozó nemzetközi munkacsoportban való uniós részvétel – alapuló bevált gyakorlatokat meg lehet osztani harmadik országokkal.
[49] EUROPOL, FRONTEX, CEPOL, EUROJUST

segítségével gyors és összehangolt módon képesek a hibrid fenyegetéseket megelőzni, azokra válaszlépéseket tenni, és következményeiket elhárítani.

Elengedhetetlenül fontos, hogy képesek legyünk gyors válaszlépéseket tenni a hibrid fenyegetések által kiváltott eseményekre. E tekintetben a nemzeti polgári védelmi intézkedéseknek és képességeknek az Európai Veszélyhelyzet-reagálási Koordinációs Központ[50] által történő elősegítése és erősítése hatékony válaszmechanizmus lehet a hibrid fenyegetések olyan vonatkozásai tekintetében, amelyek a polgári védelem terén teendő válaszlépéseket tesznek szükségessé. Ezt más uniós válaszmechanizmusok és korai előrejelző rendszerek – különösen az EKSZ külső biztonsági dimenziókkal foglalkozó helyzetelemző központja és a belbiztonsági stratégiai elemző és reagálási központ – koordinációja révén lehetne elérni.

A szolidaritási klauzula (az EUMSZ 222. cikke) lehetővé teszi az uniós fellépést, valamint a tagállamok fellépését, ha egy tagállamot terrortámadás ér, illetve ha természeti vagy ember okozta katasztrófa áldozatává válik. A tagállamok részére történő segítségnyújtás érdekében történő uniós fellépésnek végrehajtása a 2014/415/EU tanácsi határozat[51] alkalmazásával történik. A Tanácson belüli koordináció szabályait az uniós politikai szintű integrált válságreagálási intézkedések[52] alapján kell meghatározni. E szabályok szerint a Bizottság és a főképviselő (saját hatáskörén belül) azonosítja a releváns uniós eszközöket, és rendkívüli intézkedésekről szóló határozatokra irányuló javaslatokat nyújt be a Tanácsnak.

Az EUMSZ. 222. cikke olyan helyzetekre is vonatkozik, amikor egy vagy több tagállam közvetlen segítséget nyújt egy olyan tagállamnak, amelyet terrortámadás ért, vagy természeti vagy ember okozta katasztrófa áldozatává vált. E vonatkozásban a 2014/415/EU tanácsi határozat nem alkalmazandó. Tekintettel arra, hogy a hibrid tevékenységek homályos jellegűek, a Bizottságnak és a főképviselőnek (saját hatáskörén belül) meg kell kellene vizsgálnia, hogy végső esetben alkalmazni lehetne-e a szolidaritási záradékot akkor, amikor valamely uniós tagállamot jelentős hibrid fenyegetés éri.

Ezzel szemben, ha több komoly hibrid fenyegetés valamely tagállam elleni fegyveres támadást képez, az EUMSZ 222. cikke helyett az EUSZ 42. cikkének (7) bekezdése ad jogalapot a megfelelő és gyors reagálásra. Hibrid fenyegetések széles körű és súlyos megnyilvánulása a NATO-val is szorosabb együttműködést és koordinációt tehet szükségessé.

A tagállamokat ösztönözni kell arra, hogy fegyveres erőik felkészítése során a lehetséges hibrid fenyegetéseket is figyelembe vegyék. Annak érdekében, hogy egy hibrid támadás esetén a tagállamok képesek legyenek a gyors és hatékony döntéshozatalra, rendszeres gyakorlatokat kell tartaniuk munkacsoporti és politikai szinten a nemzeti és nemzetközi

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en.
[51] A Tanács 2014/415/EU határozata a szolidaritási klauzula Unió által történő végrehajtására vonatkozó részletes szabályokról (HL L 192., 2014.7.1., 53. o.).
[52] http://www.consilium.europa.eu/hu/documents-publications/publications/2014/eu-ipcr/

döntéshozatali képességek tesztelése céljából. A cél az lenne, hogy a tagállamok, a Bizottság és a főképviselő közös operatív protokollal rendelkezzenek, amely meghatározza a hibrid fenyegetések esetén követendő hatékony eljárásokat, a kezdeti, azonosítási szakasztól a támadás végső szakaszáig, és körvonalazza a folyamatban résztvevő valamennyi uniós intézmény és szereplő feladatát.

A KBVP keretében történő szerepvállalás a következőket foglalhatná magában: a) polgári és katonai képzés, b) valamely fenyegetett állam biztonsági és védelmi képességeinek javítását célzó mentori és tanácsadói feladatok, c) vészhelyzeti tervezés a hibrid fenyegetésekre utaló jelek azonosítása és a korai előrejelzésre való képesség erősítése érdekében, d) vészhelyzet esetén segítségnyújtás a határellenőrzés-igazgatás terén, e) segítségnyújtás egyes speciális területeken, például a vegyi, biológiai, radiológiai és nukleáris kockázatok enyhítése vagy a nem harci jellegű evakuálási műveletek terén.

19. intézkedés: A főképviselő és a Bizottság, a tagállamokkal együttműködésben, a válságkezelési és a politikai szintű integrált válság-elhárítási eljárásokon alapuló közös operatív protokollt fog kidolgozni, és rendszeres gyakorlatokat fog szervezni a komplex hibrid fenyegetésekre adott válaszlépések során a stratégiai döntéshozatali kapacitás javítása érdekében.

20. intézkedés: A Bizottság és a főképviselő (saját hatáskörén belül) meg fogja vizsgálni az EUMSZ 222. cikkének és 42. cikke (7) bekezdésének alkalmazhatóságát és gyakorlati vonatkozásait széles körű és súlyos hibrid támadás bekövetkezése esetén.

21. intézkedés: A főképviselő – a tagállamok közreműködésével – gondoskodni fog a hibrid fenyegetésekkel szemben a közös biztonság- és védelempolitika keretében végzett katonai akciók kapacitásainak integrálásáról, kihasználásáról és összehangolásáról.

6. A NATO-VAL FOLYTATOTT EGYÜTTMŰKÖDÉS MEGERŐSÍTÉSE

A hibrid fenyegetések nemcsak az Európai Unió számára jelentenek kihívást, hanem más fontos partnerszervezetek, többek között az Egyesült Nemzetek Szervezete (ENSZ), az Európai Biztonsági és Együttműködési Szervezet (EBESZ), és különösen a NATO számára is. A hatékony válaszadáshoz szükséges a szervezetek közötti párbeszéd és koordináció mind politikai, mind pedig operatív szinten. Az EU és a NATO közötti szorosabb együttműködés mindkét szervezet számára lehetővé tenné, hogy hatékonyabban tudjanak felkészülni és reagálni a hibrid fenyegetésekre, olyan összehangolt és egymást kölcsönösen támogató módon, amely az inkluzivitás elvén alapul, ugyanakkor tiszteletben tartja az egyes intézmények döntéshozatali autonómiáját és adatvédelmi szabályait.

A két szervezet ugyanazokat az értékeket képviseli, és hasonló kihívásokkal szembesül. Az uniós tagállamok és a NATO-szövetségesek azt várják el szervezeteiktől, hogy segítsék őket, válság esetén gyorsan, határozottan és összehangoltan cselekedjenek, illetve ideális esetben, megakadályozzák a válság bekövetkezését. Több olyan terület került kijelölésre, ahol szorosabb EU–NATO együttműködésre és koordinációra van

szükség. Ilyen többek között a helyzetismeret, a stratégiai kommunikáció, a kiberbiztonság, a válságmegelőzés és válságkezelés területe. A két szervezet e területeken folytatott tevékenységének összehangolása érdekében fokozni kell a hibrid fenyegetésekkel kapcsolatosan jelenleg zajló informális EU-NATO párbeszédet.

Annak érdekében, hogy az EU és a NATO fellépése egymást kiegészítse, fontos, hogy mindkét intézmény ugyanolyan helyzetismereti képpel rendelkezzen a válság kialakulása előtt és a válság idején is. Ez az elemzések és a levont tanulságok rendszeres cseréje révén valósulhatna meg, de azáltal is, ha a hibridfenyegetéses információkat szintetizáló uniós csoport és a NATO hibrid fenyegetésekkel foglalkozó sejtje közvetlen összeköttetésben állna egymással. A gyors és hatékony reagálás érdekében ugyanilyen fontos az egymás válságkezelési eljárásairól való kölcsönös ismeretszerzés is. Az ellenálló képesség erősíthető a saját infrastrukrúrák kritikus pontjaira vonatkozó közös viszonyítási alapok meghatározásával, valamint szoros együttműködés kialakításával a stratégiai kommunikáció és a kibervédelem terén. A másik fél maximális bevonásával végzett közös gyakorlatok – mind politikai, mind technikai szinten – javítanák a két szervezet döntéshozatali képességét. A képzési tevékenységek terén a további lehetőségek kiaknázásával elősegíthető lenne a kritikus területeken összehasonlítható szintű szakértelem kialakítása.

<u>22. intézkedés</u>: A főképviselő, a Bizottsággal együttműködésben, a hibrid fenyegetésekkel szembeni fellépés érdekében folytatni fogja az informális párbeszédet és fokozni fogja a NATO-val való együttműködést és koordinációt a helyzetismeret, a stratégiai kommunikáció, a kiberbiztonság, valamint a válságmegelőzés és válságkezelés területén, tiszteletben tartva az inkluzivitás és az egyes intézmények döntéshozatali autonómiájának elvét.

7. KÖVETKEZTETÉSEK

Ez a közös közlemény azokat a fellépéseket körvonalazza, amelyek kidolgozására a hibrid fenyegetésekkel szembeni küzdelem, és az Unió, a tagállamok, valamint a partnerek ellenálló képessége erősítésének elősegítése céljából került sor. Mivel a legfontosabb feladat **a tudatosság növelése**, a Bizottság célzott mechanizmusok kialakítását javasolja a tagállamokkal való információcsere, valamint az EU stratégiai kommunikáció biztosítására való képességének koordinálása céljából. A közös közlemény ezen kívül vázolja azokat az intézkedéseket, amelyek **az ellenálló képességet erősítik** olyan területeken, mint például a kiberbiztonság, a kritikus infrastruktúrák, a pénzügyi rendszer jogellenes használatával szembeni védelem, vagy az erőszakos szélsőségek és a radikalizálódás elleni küzdelem. E területek mindegyikén, az Európai Unió és a tagállamok által elfogadott stratégiák végrehajtása, valamint a meglévő jogszabályoknak a tagállamok általi maradéktalan végrehajtása lesz az első fontos lépés. Ezzel egyidejűleg az egyes konkrétabb intézkedésekre tett javaslatok ezeknek az erőfeszítéseknek további fokozását célozzák.

Ami **a hibrid fenyegetések megelőzését, az azokra való reagálást és következményeik elhárítását** illeti, a Bizottság javasolja annak vizsgálatát, hogy széles

körű és súlyos hibrid támadás bekövetkezése esetén hogyan lehet alkalmazni az EUMSZ 222. cikkében (a megfelelő határozatban részletezve), és az EUSZ 42. cikkének (7) bekezdésében foglalt szolidaritási klauzulát. A stratégiai döntéshozatali képesség közös operatív protokoll kidolgozásával fokozható.

Végezetül a Bizottság javasolja **az EU** és **a NATO közötti együttműködés és koordináció fokozását** a hibrid fenyegetésekkel szembeni fellépés körében tett közös erőfeszítések során.

E közös keret végrehajtása során a főképviselő és a Bizottság egyaránt elkötelezett a rendelkezésére álló releváns uniós eszközök mozgósítása iránt. Az EU és tagállamai számára is fontos, hogy dolgozzanak az állami és nem állami szereplőktől eredő potenciális hibrid fenyegetéseknek való kitettségből eredő kockázatok csökkentése érdekében.