EURÓPAI
BIZOTTSÁG

AZ UNIÓ KÜLÜGYI ÉS
BIZTONSÁGPOLITIKAI
FŐKÉPVISELŐJE

Brüsszel, 2017.7.19.
JOIN(2017) 30 final

KÖZÖS JELENTÉS AZ EURÓPAI PARLAMENTNEK ÉS A TANÁCSNAK

„A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz” végrehajtásáról

1. BEVEZETÉS

Az EU a történelme egyik legsúlyosabb biztonsági kihívásával néz szembe. A fenyegetések egyre nagyobb része ölt a megszokottól eltérő formát; ezek között vannak fizikai fenyegetések, például a terrorizmus új formái, és akadnak olyanok is, amelyek a digitális teret használják ki összetett kibertámadásokhoz. Más, kevésbé látványos fenyegetések célja a kényszerítő nyomásgyakorlás, ilyenek például a félretájékoztatási kampányok és a média manipulációja. A fenyegetések az olyan alapvető európai értékeket próbálják aláásni, mint az emberi méltóság, a szabadság és a demokrácia. A közelmúltban a világ különböző pontjain történt, nehezen azonosítható elkövetők által végrehajtott kibertámadások megmutatták, mennyire sebezhetőek a társadalmaink és az intézményeink.

2016 áprilisában az Európai Bizottság és a főképviselő közös közleményt fogadott el a hibrid fenyegetésekkel szembeni fellépésről[1] (a továbbiakban: közös keret). A hibrid fenyegetések határokon átívelő és összetett jellegét felismerve ez a keret összkormányzati megközelítést javasol társadalmaink általános ellenálló képességének megerősítéséhez. A Tanács[2] üdvözölte a kezdeményezést és a javasolt intézkedéseket, és felkérte a Bizottságot és a főképviselőt, hogy 2017 júliusában számoljanak be az elért haladásról. Míg az EU segítséget nyújthat a tagállamoknak a hibrid fenyegetésekkel szembeni ellenálló képességük erősítésében, a tagállamokra hárul az elsődleges felelősség, amennyiben a hibrid fenyegetésekkel szembeni fellépés a nemzeti biztonságot és védelmet, valamint a közrend fenntartását érinti.

A hibrid fenyegetésekkel szembeni fellépés közös kerete fontos részét képezi a biztonság és a védelem általános, integráltabb uniós megközelítésének. Hozzájárul egy olyan Európa megteremtéséhez, amely védelmet nyújt – erre Juncker elnök szólított fel 2016 szeptemberében, az Unió helyzetét értékelő beszédében. 2016-ban az Európai Unió lefektette egy szilárdabb európai védelmi politika alapjait is, hogy megfeleljen a polgárok fokozottabb védelemre irányuló várakozásainak. Az EU kül- és biztonságpolitikára vonatkozó globális stratégiája[3] kifejtette, hogy integrált megközelítés szükséges ahhoz, hogy a belső ellenálló képességet össze lehessen kapcsolni az EU külső tevékenységeivel, és szinergiák megvalósítására hívott fel a védelmi politika, valamint a belső piacra, az iparra, a bűnüldözésre és a hírszerzési szolgálatokra vonatkozó szakpolitikák között. Az európai védelmi cselekvési terv 2016. novemberi elfogadását követően a Bizottság konkrét kezdeményezéseket terjesztett elő, amelyek a védelmi ellátási láncok ellenálló képességének javítása és az egységes védelmi piac megerősítése útján hozzá fognak járulni ahhoz, hogy az EU hatékonyabban reagálhasson a hibrid fenyegetésekre. A Bizottság 2017. június 7-én létrehozta az Európai Védelmi Alapot, melynek javasolt finanszírozása 2020-ig 600 millió EUR, 2020 után pedig évente 1,5 milliárd EUR. A biztonsági unióról szóló közlemény[4] felismerte, hogy fel kell lépni a hibrid fenyegetésekkel szemben, és hogy a biztonságpolitika terén fontos biztosítani a belső és a külső fellépések jobb összehangolását.

[1] Közös közlemény az Európai Parlamentnek és a Tanácsnak: *A hibrid fenyegetésekkel szembeni fellépés közös kerete – európai uniós válasz*, JOIN (2016) 18 final.
[2] *A Tanács következtetései a hibrid fenyegetések elleni küzdelemről*, 196/16. sz. sajtóközlemény, 2016. április 19.
[3] A főképviselő 2016. június 28-án mutatta be az Európai Tanácsnak.
[4] COM(2016) 230 final, 2016. április 20.

Az Európa jövőjéről folytatott vitájukban az uniós vezetők a biztonság és a védelem kérdését állították a középpontba[5]. Ez tükröződik a 2017. március 25-i Római Nyilatkozatban is, amely felvázolta a közös biztonság és védelem megerősítése iránt elkötelezett, biztonságos Unió jövőképét. Hogy új lendületet adjanak az EU és a NATO közötti stratégiai partnerségnek, és új tartalommal töltsék meg azt, az Európai Tanács elnöke, az Európai Bizottság elnöke és a NATO főtitkára 2016. július 8-án közös nyilatkozatot írtak alá Varsóban. Ez a közös nyilatkozat meghatározott hét konkrét területet – köztük a hibrid fenyegetésekkel szembeni fellépést is –, amelyeken javítani szükséges a két szervezet közötti együttműködést. Ezt követően mind az EU, mind a NATO Tanácsa jóváhagyott egy közös listát, amely a végrehajtásra vonatkozó 42 javaslatot tartalmaz, és 2017 júniusában kiadásra került egy első, már jelentős előrehaladásról beszámoló jelentés[6].

A Bizottságnak az európai védelem jövőjéről szóló, 2017 júniusában bemutatott vitaanyaga[7] különböző forgatókönyveket vázol fel arra vonatkozóan, miként lehetne kezelni az Európát érintő, egyre fokozódó biztonsági és védelmi fenyegetéseket, illetve növelni Európa saját védelmi képességeit 2025-ig. A biztonságot és a védelmet mindhárom forgatókönyv az európai projekt szerves részének tekinti, mert ezáltal lehet megvédeni az érdekeinket és elősegíteni azok érvényesülését az Unión belül és kívül. Európának biztonságfenntartó szerepet kell vállalnia, és egyre inkább gondoskodnia kell a saját biztonságáról. Az előttünk álló kihívásokkal – és különösen a hibrid fenyegetésekkel szembeni fellépés feladatával – egyetlen tagállam sem tud egyedül megbirkózni. A védelmi és biztonsági együttműködés ezért nem csupán egy lehetőség, hanem elengedhetetlen ahhoz, hogy valóban olyan Európát építsünk, amely védelmet nyújt.

Ennek a jelentésnek az a célja, hogy beszámoljon az előrehaladásról és az intézkedések kapcsán tett következő végrehajtási lépésekről a közös keretben felvetett következő négy terület vonatkozásában: a helyzetismeret javítása; az ellenálló képesség erősítése; a tagállamok és az Unió azon képességeinek megszilárdítása, amelyek segítségével képesek megelőzni a válságokat, reagálni azokra, illetve összehangolt módon elhárítani a következményeiket; valamint a NATO-val való együttműködés fokozása az intézkedések egymást kiegészítő jellegének biztosítása érdekében. A jelentést a hatékony és valódi biztonsági unió megvalósítására vonatkozó havi eredményjelentésekkel együtt kell értelmezni.

2. A FENYEGETÉS HIBRID JELLEGÉNEK FELISMERÉSE

A hibrid tevékenységek az európai biztonsági környezet egyre gyakoribb velejáróivá válnak. Fokozódik az ilyen tevékenységek intenzitása, és egyre több aggodalom merül fel a választások befolyásolása, a félretájékoztatási kampányok és a rosszindulatú számítógépes tevékenységek kapcsán, illetve azt illetően, hogy a hibrid tevékenységek elkövetői megpróbálják radikalizálni a társadalom kiszolgáltatott tagjait, hogy azok a nevükben lépjenek fel. A hibrid fenyegetésekkel szembeni kiszolgáltatottság nem marad a nemzeti

[5] Az Európai Tanács 2016. szeptember 16-i pozsonyi ütemterve és a 27 tagállam, az Európai Tanács, az Európai Parlament és az Európai Bizottság vezetőinek 2017. március 25-i Római Nyilatkozata.

[6] http://www.consilium.europa.eu/hu/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

[7] Vitaanyag az európai védelem jövőjéről, 2017. június 7., https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_hu.pdf

határokon belül. Az ilyen fenyegetésekre összehangolt választ kell adni az Unió és a NATO szintjén is. A 2016 áprilisa óta történt fejlemények azt mutatják, hogy bár a fenyegetéseket gyakran továbbra is egymástól elszigetelten értékelik, az Unióban egyre többen ismerik fel és értik meg egyes megfigyelt tevékenységek hibrid jellegét és azt, hogy összehangolt fellépésre van szükség. Az EU a továbbiakban is törekedni fog a helyzetismeret és az együttműködés javítására.

1. intézkedés: 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 páneurópai struktúrákat és hálózatokat.

A Tanács létrehozott egy „elnökség barátai" csoportot, melynek tagállami szakértők a tagjai, és az a feladata, hogy kidolgozzon egy olyan általános felmérést, amely lehetővé tenné a hibrid fenyegetések legfontosabb mutatóinak pontosabb meghatározását, azoknak a korai előrejelző rendszerekbe és a meglévő kockázatértékelési mechanizmusokba való beépítését, illetve adott esetben megosztását. Megállapodás született a feladatokról, és megkezdődött a munka. Az általános felmérésnek 2017 végéig kell elkészülnie, a felmérések tényleges elvégzése azután kezdődik meg. A hibrid fenyegetések elleni védelemnek kölcsönösen erősítő jellegűnek kell lennie. Ezért arra ösztönözzük a tagállamokat, hogy a lehető leggyorsabban bonyolítsák le a szóban forgó felméréseket, mivel azok értékes információkkal fognak szolgálni arról, hogy milyen mértékű a sebezhetőség, illetve a felkészültség Európában.

a) TUDATOSSÁGNÖVELÉS

A hírszerzési elemzések és értékelések megosztása kulcsfontosságú eszköz, amely csökkenti a bizonytalanságot és javítja a helyzetismeretet. Az elmúlt évben jelentős előrelépés történt e téren. Létrejött, és már teljesen működőképes a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport, felállt a keleti stratégiai kommunikációval foglalkozó munkacsoport, és Finnország létrehozta A Hibrid Fenyegetések Elleni Küzdelem Európai Központját. Intenzív munka folyt a félretájékoztatás vagy propaganda terén használt eszközök és ösztönző erők elemzése kapcsán, és hatékony volt az együttműködés a keleti stratégiai kommunikációval foglalkozó uniós munkacsoport, a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport, valamint a NATO között. Ez jó alapot jelent ahhoz, hogy kialakítsuk a belső és külső biztonságunkat érintő fenyegetések hibrid szempontból történő elemzésének és értékelésének mélyen berögzült kultúráját.

A hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport

2. intézkedés: Hibrid fenyegetésekre vonatkozó minősített adatok és nyílt forrásból származó információk fogadására és elemzésére képes, a hibrid fenyegetésekkel foglalkozó uniós információs és elemző csoport létrehozása az Európai Unió Helyzetelemző Központján belül. A tagállamok felkérést kapnak arra, hogy a hibrid fenyegetésekkel foglalkozó nemzeti kapcsolattartó pontokat hozzanak létre, amelyek biztosítják a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoporttal történő együttműködést és kommunikációt.

Az Európai Unió Helyzetelemző Központján belül létrejött a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport, amely fogadja és elemzi a különböző érdekelt felektől érkező, a hibrid fenyegetésekre vonatkozó minősített adatokat és nyílt forrásból származó információkat. Az elemzést ezután megosztják az EU-n belül és a tagállamok között, és felhasználásra kerül az uniós döntéshozatali eljárásokban, többek között bemeneti

adatot jelent az uniós szinten elvégzett biztonsági kockázatértékelésekhez is. Az Európai Unió Katonai Törzsének Hírszerzési Osztálya katonai elemzésekkel járul hozzá az információs és elemzőcsoport munkájához. Már több mint 50 értékelés és jelentés készült a hibrid fenyegetésekkel kapcsolatos témákban. 2017 januárjától a csoport összeállít egy „Hybrid Bulletin" című időszaki kiadványt is, amelyben aktuális fenyegetéseket és a hibrid fenyegetésekhez kapcsolódó kérdéseket elemez. A kiadvány közvetlenül elérhető az uniós intézmények és szervek, valamint a nemzeti kapcsolattartó pontok[8] számára. A csoport a terveknek megfelelően 2017 májusában elérte teljes működési kapacitását. Végezetül: a személyzet kapcsolatban áll a NATO frissen létrejött, hibrid fenyegetéseket elemző csoportjának munkatársaival, egyrészt az információs és elemzőcsoport létrehozása során levont tanulságok megosztása, másrészt információmegosztás céljából (az utóbbira a minősített információk cseréjére vonatkozó uniós szabályok teljes mértékű tiszteletben tartásával kerül sor). A hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport jelenleg olyan további kezdeményezések kidolgozásával foglalkozik, amelyek javíthatják a jövőbeli együttműködést, és kulcsszerepet fog játszani a 2017 őszére tervezett EU–NATO párhuzamos gyakorlatokban, amelyek során vizsgálni fogják a csoport reagálóképességét, és elvégzik a levont tanulságok beépítését.

Stratégiai kommunikáció

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.

Az elmúlt hónapokban az intenzívebbé váló félretájékoztatási kampányok és az álhírek közösségi médiában való szisztematikus terjesztése is beletartoztak az ellenfelek helyzetének aláásására használt eszközök tárházába. Ahol a közösségi média közkedvelt platform, ott a megbízhatónak és legitimnek tűnő információk úgy befolyásolhatják a közvéleményt, hogy az egyes személyeknek, szervezeteknek vagy kormányoknak kedvezzen. Ezek a hibrid taktikák azt az általánosabb célt is szolgálják, hogy zavart keltsenek a társadalmainkban és hiteltelenné tegyék a demokratikus kormányokat és a társadalmunk struktúráit, az intézményeinket és a választásainkat. Az álhíreket gyakran online felületeken terjesztik (lásd a 17. intézkedést is). A Bizottság és a főképviselő örömmel fogadja a legutóbbi lépéseket, melyeket az online platformok és hírlapkiadók tettek a félretájékoztatás kezelése érdekében. A Bizottság a továbbiakban is ösztönözni fogja a hasonló önkéntes intézkedéseket.

A főképviselő létrehozta a keleti stratégiai kommunikációval foglalkozó munkacsoportot, amely előre jelzi a félretájékoztatás eseteit és a félretájékoztatási kampányokat, illetve reagál azokra. Ez jelentősen javítja az Unió szakpolitikáival kapcsolatos kommunikációt a keleti szomszédság országaiban, és a médiakörnyezetet is erősíti a szóban forgó államokban. A munkacsoport az elmúlt két évben több mint 3 000 egyedi félretájékoztatási esetre derített fényt, amelyek 18 nyelvet érintettek. A felhasználói hozzáférést nagyban javítani fogja, hogy hamarosan elindul az „*#EUvsdisinformation*" nevű új weboldal, melyen online keresést is lehet folytatni. A kutatási és elemzési adatok ugyanakkor arra utalnak, hogy jelentősen nőtt a félretájékoztatást szolgáló csatornák és a nap mint nap terjesztett álhírek száma. A keleti partnerség országaiban a Horizont 2020 programból finanszírozott EU-STRAT projekt keretében folyik a szakpolitika és a média elemzése.

[8] Eddig 21 tagállam jelölt ki nemzeti kapcsolattartó pontot. Ezek olyan személyek, akik a szakpolitikához köthető vagy az ellenálló képességgel kapcsolatos szerepkörben dolgoznak egy tagállami fővárosban.

A főképviselő felkéri a tagállamokat, hogy a hibrid fenyegetések szaporodása elleni hatékonyabb fellépés érdekében támogassák a stratégiai kommunikációval foglalkozó munkacsoportok munkáját. Ez segíteni fogja a déli munkacsoportot abban, hogy javítsa az arab világgal való kommunikációt és az oda irányuló tájékoztatást (arab nyelven is), tévhiteket döntsön meg, és hogy tisztázza az Európai Unióval és annak szakpolitikáival kapcsolatos tényeket. A helyi újságírókkal való együttműködés fog segíteni annak biztosításában, hogy a megjelenő hírek megfeleljenek a kulturális normáknak. A hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport által támogatott mindkét munkacsoport célja a tagállamok kapcsolódó erőfeszítéseinek támogatása és kiegészítése. A Bizottság mindezeken túl társfinanszírozást nyújt az európai stratégiai kommunikációs hálózat működéséhez, amely 26 tagállam együttműködési hálózata, és amelynek tagjai elemzéseket, bevált gyakorlatokat és a stratégiai kommunikációnak az erőszakos szélsőségesség és a félretájékoztatás elleni küzdelem terén való felhasználásával kapcsolatos ötleteket osztanak meg egymással.

A hibrid fenyegetésekkel szembeni fellépéssel foglalkozó kiválósági központ

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

A kiválósági központ létrehozására irányuló felhívásra reagálva Finnország 2017 áprilisában létrehozta A Hibrid Fenyegetések Elleni Küzdelem Európai Központját. A központnak tíz uniós tagállam[9], Norvégia és az Egyesült Államok a tagja, és mind az Európai Unió, mind a NATO felkérést kapott arra, hogy támogassa az irányítóbizottságot[10]. A központ célja a stratégiai párbeszéd ösztönzése és az, hogy az érdeklődésre számot tartó közösségek körében végzett munka során kutatásokat folytasson és elemzéseket végezzen, így javítva az ellenálló képességet és a reagálásra való képességet a hibrid fenyegetésekkel szembeni fellépés támogatása érdekében. Várhatóan helyszínként szolgál majd a hibrid fenyegetésekkel kapcsolatos jövőbeli gyakorlatokhoz is. A központ máris szoros kapcsolatot alakított ki a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoporttal, és a két szervezet munkájának ki kell egészítenie egymást. Az EU jelenleg vizsgálja, milyen módon nyújthat konkrét támogatást a központ számára.

b) AZ ELLENÁLLÓ KÉPESSÉG ERŐSÍTÉSE

A közös keret az ellenálló képességet (például a közlekedés, a hírközlés, az energiaágazat, a pénzügyi ágazat vagy a regionális biztonsági infrastruktúrák ellenálló képességét) állítja az uniós fellépés középpontjába, hogy az EU ellen tudjon állni a propagandának és a tájékoztatási kampányoknak, a vállalkozások, társadalmak vagy gazdasági folyamatok aláásására irányuló kísérleteknek, valamint az információs technológiai és kibertérhez kötődő infrastruktúrák elleni támadásoknak. Az ellenálló képesség erősítését megelőző és elrettentő lépésnek tekinti, amelynek célja a társadalmak megszilárdítása és a válságok súlyosbodásának elkerülése mind az EU-n belül, mind azon kívül. E téren az EU hozzáadott értéke abban rejlik, hogy a meglévő eszközök és programok széles körére támaszkodva segíti a tagállamokat és a partnereket az ellenálló képességük megerősítésében. Jelentős előrelépés történt az ellenálló

[9] Finnország, Franciaország, Németország, Lettország, Litvánia, Lengyelország, Svédország, az Egyesült Királyság, Észtország és Spanyolország.
[10] Más uniós tagállamok és NATO-szövetségesek is csatlakozhatnak.

képesség erősítése kapcsán olyan területeken, mint a kiberbiztonság, a kritikus infrastruktúrák, a pénzügyi rendszer jogellenes használatával szembeni védelem vagy az erőszakos szélsőségek és a radikalizálódás elleni küzdelem.

A kritikus infrastruktúrák védelme

5. intézkedés: 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.

A kritikus infrastruktúrák védelmére vonatkozó európai program keretében a Bizottság folytatta a közös eszközök, köztük sebezhetőségi mutatók meghatározására irányuló munkát, hogy javítsa a kritikus infrastruktúrák hibrid fenyegetésekkel szembeni ellenálló képességét az érintett ágazatokban. 2017 májusában a Bizottság műhelytalálkozót szervezett a kritikus infrastruktúrákat érintő hibrid fenyegetésekről. A találkozón szinte valamennyi tagállam képviseltette magát, és a résztvevők között megtalálhatók voltak kritikus infrastruktúrák működtetői, a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport, valamint megfigyelőként a NATO is. A tagállamok nemzeti hatóságainak küldött kérdőív alapján megállapodás született a jövőbeli munka közös ütemtervéről és lépéseiről. A Bizottság az ősz folyamán további konzultációkat fog folytatni az érdekelt felekkel, azzal a céllal, hogy 2017 végéig megállapodjanak a mutatókról.

Az Európai Védelmi Ügynökség dolgozik a képességekhez és a kutatáshoz kapcsolódó azon közös hiányosságok azonosításán, amelyek az energetikai infrastruktúrák és a védelmi képességek közötti kapcsolatból erednek. Az Ügynökség 2017 őszén egy koncepciós dokumentumot, valamint holisztikus módszereket alkalmazó kísérleti fellépéseket fog kidolgozni.

Az energiaellátás biztonságának javítása az Unióban

6. intézkedés: 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.

2016 decemberében a Bizottság az energiaellátás biztonságára irányuló jogalkotási csomagban konkrét javaslatokat terjesztett elő, 2017 áprilisában pedig megállapodás született a Tanács és az Európai Parlament között a földgázellátás biztonságáról szóló új rendeletről, amely a földgázellátási válságokat hivatott megelőzni. Az új szabályok biztosítják, hogy a tagállamok regionális szinten koordinált és közös megközelítést alkalmazzanak az ellátás biztonságát szolgáló intézkedések kapcsán. Ennek köszönhetően egy válság vagy hibrid támadás esetén az EU jobb helyzetben lesz ahhoz, hogy felkészüljön az esetleges földgázhiányra és kezelje azt. Első ízben lesz alkalmazandó a szolidaritás elve: súlyos válság vagy támadás esetén a tagállamok segíteni tudnak majd a szomszédaiknak, hogy ne szakadjon meg az ellátás az európai háztartásokban és az európai vállalkozásoknál.

Az EU előrehaladást ért el azon a téren is, hogy az energiaunióra vonatkozó keretstratégiának és az európai energiabiztonsági stratégiának megfelelően kulcsprojekteket dolgozzon ki az energiaellátási útvonalainak és forrásainak diverzifikálása érdekében. Például a Déli Gázfolyosó esetében folynak az építési munkálatok mindegyik fő csővezetékprojekt kapcsán: a dél-kaukázusi, a transzanatóliai és a transzadriai csővezeték meghosszabbítása, az upstream

Shah Deniz II projekt, továbbá a Déli Gázfolyosó meghosszabbítása Közép-Ázsia, elsősorban Türkmenisztán irányába. A cseppfolyósított földgáz (LNG) Európába való behozatala egyre nagyobb méreteket ölt, és új forrásokból, például az Egyesült Államokból ered. A litvániai terminál példája megmutatja, hogy a diverzifikációs projektek hogyan csökkenthetik az egyetlen szállítótól való függést. Az energiával kapcsolatos erőfeszítések fokozása és a saját energiaforrások – különösen a megújuló energiaforrások – hatékonyabb használata szintén hozzájárul az energiaellátási útvonalak és az energiaforrások diverzifikálásához.

A nukleáris biztonság terén a Bizottság – elsősorban a nemzeti hatóságok és a szabályozó testületek részvételével tartott műhelytalálkozók útján – aktívan támogatja a nukleáris biztonságról és az alapvető biztonsági normákról szóló két irányelv következetes és eredményes végrehajtását. Az irányelveket a tagállamoknak 2017, illetve 2018 végéig kell átültetniük. Mindemellett az Euratom kutatási és képzési programja is hozzájárul a nukleáris biztonság javításához.

A közlekedési ágazat és az ellátási láncok biztonsága

7. intézkedés: 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 e stratégiák cselekvési terveinek 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.

A biztonsági unióról szóló közleménnyel összhangban a Bizottság – a tagállamokkal, az Európai Unió Helyzetelemző Központjával és az érintett ügynökségekkel karöltve – elősegíti a biztonsági kockázatok uniós szinten végzett értékelését, melynek célja a közlekedésbiztonságot érintő fenyegetések észlelése, valamint a hatékony és arányos enyhítő intézkedések kidolgozása. A Malaysia Airlines MH17-es járatának Kelet-Ukrajna feletti, 2014-ben történt lelövése rámutatott, milyen kockázattal jár a konfliktusövezetek feletti átrepülés. A konfliktusövezetekkel foglalkozó magas szintű európai munkacsoport ajánlásának[11] megfelelően a Bizottság – nemzeti légi közlekedési és biztonsági szakértők, valamint az EKSZ támogatásával – kidolgozta a „közös uniós kockázatértékelés” módszertanát, amely lehetővé teszi a minősített adatok cseréjét és a kockázatokról alkotott közös kép kialakítását. 2017 márciusában az Európai Repülésbiztonsági Ügynökség (EASA) kiadta a konfliktusövezetekre vonatkozó első tájékoztató hírlevelet[12] („Conflict Zones Information Bulletin”), amely ennek a közös uniós kockázatértékelésnek az eredményein alapul. A Bizottság mérlegeli a légi közlekedés védelme terén végzett kockázatértékelési tevékenységek más közlekedési módokra (például a vasúti és tengeri közlekedésre) való kiterjesztését, és 2018-ban javaslatokat fog előterjeszteni. 2017 júniusában a Bizottság, az EKSZ és a tagállamok elindítottak egy kockázatértékelési gyakorlatot a vasútbiztonság területén, hogy azonosítsák a hiányosságokat és a kockázatok csökkentését szolgáló lehetséges intézkedéseket.

A légi közlekedés védelme és a légiforgalmi szolgáltatás (ATM) kapcsán jelentős erőfeszítések történtek a 7. keretprogram és a Horizont 2020 biztonságkutatási projektjei

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

keretében is. A polgári légi közlekedés terén a Bizottság az Európai Repülésbiztonsági Ügynökséggel és érdekelt felekkel együttműködve két új kezdeményezést dolgoz ki a kiberbiztonság megszilárdítása érdekében, amelyek egyben a hibrid fenyegetéseket is kezelik: a repülésügyi számítógép- és hálózatbiztonsági vészhelyzeteket elhárító csoport létrehozása, valamint egy kiberbiztonsági munkacsoport felállítása az egységes európai égbolt légiforgalmi szolgáltatásaiért felelős, az „Egységes európai égbolt" légiforgalmi szolgáltatási kutatást (SESAR) végző közös vállalkozáson belül. Az Európai Védelmi Ügynökség katonai jellegű, a légi közlekedés kiberbiztonságára vonatkozó információkkal látja el a SESAR közös vállalkozást és az Európai Repülésbiztonsági Ügynökséget „a kiberbiztonsággal foglalkozó európai stratégiai koordinációs platform" útján, amely a tagállamok és az ágazat kérésére segíteni fogja a légi közlekedéshez kapcsolódó valamennyi tevékenység uniós szintű koordinációját. A légi közlekedésre vonatkozó kiberbiztonsági ütemtervvel összhangban az Európai Repülésbiztonsági Ügynökség 2016-ban hiányelemzéseket hajtott végre a meglévő szabályokra vonatkozóan, és különösen az Európai Légi Közlekedési Kiberbiztonsági Központ meghatározásával és létrehozásával kapcsolatban. Az utóbbi szervezet már megkezdte működését, és együttműködik az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportjával (CERT-EU) (2017 februárjában írták alá az egyetértési megállapodást), ennek keretében a légi közlekedést érintő fenyegetéselemzéseket készít, valamint együttműködést folytat az Eurocontrollal is (elfogadtak egy együttműködési ütemtervet), továbbá kifejlesztésre került a nyílt forrásból származó elemzések megosztását szolgáló weboldal is. 2017 őszéig elfogadásra kerül egy szabványosítási program, és kidolgozzák a biztonságos információcserét.

Vámügyi kockázatkezelés

Vámügyi szempontból a Bizottság arra összpontosít, hogy jelentős mértékben korszerűsítse az előzetes rakományinformációs és vámügyi kockázatkezelési rendszert. Ez a vámügyi kockázatok teljes skáláját átfogja, ideértve azokat a kockázatokat is, amelyek a nemzetközi ellátási láncok biztonságát és integritását vagy a kapcsolódó kritikus infrastruktúrákat érintő fenyegetésekből adódnak (például tengeri kikötői létesítményeket, repülőtereket vagy szárazföldi határokat érintő, a behozatalból eredő közvetlen fenyegetések). A korszerűsítés célja a következők biztosítása: az EU-ban a vámhatóságok kapjanak meg minden szükséges információt a kereskedőktől az áruk szállítására vonatkozóan; hatékonyabban tudják megosztani ezeket az információkat a tagállamok között; a kockázatok kapcsán alkalmazzanak közös szabályokat is a tagállam-specifikus szabályok mellett; valamint a más hatóságokkal, különösen az egyéb bűnüldözési és biztonsági ügynökségekkel való szorosabb együttműködés útján legyenek képesek hatékonyabban megcélozni a kockázatos szállítmányokat. A Bizottság által végzett korszerűsítés megvalósításához szükséges informatikai fejlesztés jelenleg a kezdeti szakaszban jár, és a következő hónapokban fognak megindulni a kapcsolódó központi szintű beruházások.

Űrpolitika

8. intézkedés: Az 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 nyomonkövetési rendszer hatályának a hibrid fenyegetésekre történő kiterjesztésével, a GovSatCom európai szintű új generációjának létrehozásával, valamint a Galileo használatának bevezetésével olyan kritikus infrastruktúrák esetében, amelyek működéséhez elengedhetetlen az időszinkronizálás.

Az állami műholdas kommunikációra (GovSatCom), valamint az űrmegfigyelésre és a Föld körüli pályán haladó objektumok nyomon követésére vonatkozó keretszabályok 2018-ban esedékes kidolgozása során a Bizottság figyelembe fogja venni a hibrid fenyegetésekkel szembeni ellenálló képességet is az értékelésében. Az űrstratégiának megfelelően a Galileo és a Kopernikusz fejlesztésének előkészítése során a Bizottság meg fogja vizsgálni, hogy ezek a szolgáltatások mennyiben képesek hozzájárulni a kritikus infrastruktúrák sebezhetőségének csökkentéséhez. Az értékelő jelentés várhatóan 2017 őszére készül el, a Kopernikusz és a Galileo következő generációjára vonatkozó javaslat pedig 2018-ban. Az Európai Védelmi Ügynökség együttműködésen alapuló képességfejlesztési projekteken dolgozik az űrbe telepített technológián alapuló kommunikáció, a katonai helymeghatározás, a navigáció és az időmeghatározás, valamint a Föld megfigyelése terén. Valamennyi projekt középpontjában az aktuális és az újonnan megjelenő hibrid fenyegetésekre tekintettel szükséges, az ellenálló képességgel kapcsolatos követelmények állnak.

Védelmi képességek

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.

2016-ban és 2017-ben az Európai Védelmi Ügynökség a Bizottsággal, az EKSZ-szel és tagállami szakértőkkel közösen három szimulációs gyakorlatot hajtott végre hibrid fenyegetéseket tartalmazó forgatókönyvek alapján. Az e gyakorlatok nyomán tett megállapításokat figyelembe fogják venni a képességfejlesztési terv felülvizsgálata során annak érdekében, hogy a hibrid fenyegetésekkel szembeni fellépéshez szükséges, a felülvizsgálatból eredő legfontosabb képességfejlesztési lépések beépüljenek az EU új képességfejlesztési prioritásaiba. A 2005. évi követelménykatalógus felülvizsgálatával kapcsolatos munka során is figyelembe fogják venni a hibrid fenyegetések dimenzióját. 2017 áprilisában az Európai Védelmi Ügynökség véglegesítette a kritikus kikötői infrastruktúrákat megcélzó hibrid támadásokból eredő katonai következményekről szóló elemző jelentését, amely egy tengerészeti szakértők részvételével 2017 októberében tartott műhelytalálkozón kerül megvitatásra. A tervek szerint 2018-ban készülni fog egy másik, a minidrónok elleni fellépés terén játszott katonai szerepre vonatkozó egyedi elemzés is. Ezenkívül lehetséges, hogy a képességeket érintő, a tagállamok által azonosított hibrid fenyegetésekkel szembeni ellenálló képesség fejlesztését célzó prioritások 2019-től az Európai Védelmi Alapból nyújtott támogatásban is részesülhetnek. A Bizottság felkéri a társjogalkotókat arra, hogy gondoskodjanak a gyors elfogadásról, a tagállamokat pedig arra, hogy nyújtsanak be a képességekhez kapcsolódó projektekre irányuló javaslatokat az EU hibrid fenyegetésekkel szembeni ellenálló képességének javítása érdekében.

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.

A Bizottság képzések, szimulációs gyakorlatok, a tapasztalatcsere elősegítése, útmutatók, valamint együttes fellépések finanszírozása útján támogatást nyújt a tagállamoknak annak érdekében, hogy javítsa a hibrid fenyegetésekre való felkészültséget és a velük szembeni ellenálló képességet, ideértve az egészségügyi rendszereken és élelmiszerrendszereken belüli kapacitásépítést is. Erre elsősorban a határokon át terjedő súlyos egészségügyi veszélyekre vonatkozó uniós közegészség-védelmi keret, valamint a Nemzetközi Egészségügyi

Rendszabályok végrehajtását célzó közegészségügyi program keretében kerül sor. A Nemzetközi Egészségügyi Rendszabályok egy 196 országra – köztük a tagállamokra – nézve kötelező jogalkotási pillér, amelynek célja a világ bármely részén megjelenő, határokon át terjedő akut közegészségügyi kockázatok megelőzése, illetve az azokra való reagálás. Az ágazatközi felkészültségnek és reagálásnak az egészségügyi ágazat szempontjából történő vizsgálata céljából a Bizottság szolgálatai 2017 őszén gyakorlatot fognak lefolytatni az összetett és többdimenziós hibrid fenyegetésekre vonatkozóan. Az oltóanyagok kínálatának megszilárdítása és a közegészség védelmének uniós szintű javítása érdekében a Bizottság és a tagállamok együttes fellépést dolgoznak ki a vakcinázással kapcsolatban, kitérve az oltóanyagok kínálatának és keresletének előrejelzésére és az innovatív oltóanyag-előállítási folyamatokra vonatkozó kutatásokra is (2018–2020). A fejlett tudományos vizsgálati módszerekhez való alkalmazkodás érdekében a Bizottság együttműködést folytat az Európai Élelmiszerbiztonsági Hatósággal és az Európai Betegségmegelőzési és Járványvédelmi Központtal is, hogy pontosabban lehessen azonosítani az egészségügyi fenyegetéseket és meghatározni azok forrását, és ennek köszönhetően gyorsan lehessen kezelni az élelmiszer-biztonságot érintő kitöréseket. A Bizottság kiépítette a kutatást finanszírozó szervezetek hálózatát (Global Research Collaboration for Infectious Disease Preparedness, azaz a fertőző betegségekre való felkészülés terén megvalósuló globális kutatási együttműködés), hogy bármilyen jelentős betegségkitörés esetén 48 órán belül összehangolt kutatási választ lehessen adni.

<u>11. intézkedés</u>: A Bizottság arra ösztönzi a tagállamokat, hogy haladéktalanul hozzák létre és teljes mértékben használják ki a 28 CSIRT és a CERT-EU (az európai intézmények, szervek és hivatalok számítógépes vészhelyzeteket elhárító csoportja) 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.

A közelmúltban történt, zsarolóprogramok (ransomware) és rosszindulatú számítógépes programok használatával több ezer számítógépes rendszert megbénító kibertámadások ismét rámutattak arra, hogy az EU-ban sürgősen cselekedni kell a kibertámadásokkal szembeni ellenálló képesség javítása és a biztonsági intézkedések szigorítása érdekében. Ahogyan a digitális tartalmak egységes piacának félidős értékelésében is szerepelt, a Bizottság és a főképviselő felülvizsgálja a 2013-as uniós kiberbiztonsági stratégiát, és ennek elsődleges eszköze egy 2017 szeptemberére tervezett jogalkotási csomag elfogadása. A cél az, hogy ilyen fenyegetések esetén hatékonyabb ágazatközi válasz legyen adható, és így növekedjen a digitális társadalomba és gazdaságba vetett bizalom. A jogalkotási csomagnak részét képezi az ENISA, az Európai Uniós Hálózat- és Információbiztonsági Ügynökség megbízatásának felülvizsgálata is, hogy meghatározásra kerüljön a megváltozott kiberbiztonsági ökoszisztémában betöltött szerepe. Az Európai Tanács[13] örömmel fogadta, hogy a Bizottság a kiberbiztonsági stratégia felülvizsgálatát tervezi.

A hálózati információs szolgáltatásokról szóló irányelv[14] (kiberbiztonsági irányelv) 2016. júliusi elfogadása kulcsfontosságú lépés volt a kiberbiztonsági ellenálló képesség európai szinten történő kiépítése felé. Az irányelv első ízben határoz meg uniós szintű szabályokat a

[13] Az Európai Tanács 2017. június 22–23-i következtetései.

[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.).

kiberbiztonságra vonatkozóan, javítja a kiberbiztonsági képességeket, és megerősíti a tagállamok közötti együttműködést. Emellett a kritikus ágazatokban működő vállalkozások számára előírja, hogy hozzanak megfelelő biztonsági intézkedéseket és jelentsék be a súlyos kiberbiztonsági eseményeket az érintett nemzeti hatóságnak. Az ilyen ágazatok közé tartozik az energiaágazat, a közlekedés, a vízügyi ágazat, az egészségügy, a banki szolgáltatások és a pénzügyi piaci infrastruktúrák. Az online piactereknek, a felhőalapú számítástechnikai szolgáltatásoknak és a keresőprogramoknak is hasonló lépéseket kell tenniük. A különböző ágazatokra és a határokra tekintet nélküli egységes végrehajtást a hálózati információs szolgáltatásokkal foglalkozó együttműködési csoport biztosítja (amelyet a Bizottság 2016-ban hozott létre), ennek feladata a piac széttagoltságának megelőzése. Ebben az összefüggésben a hálózati információs szolgáltatásokról szóló irányelv tekinthető referenciakeretnek a kiberbiztonság terén születő minden ágazati kezdeményezéshez. Az irányelv létrehozza a számítógép-biztonsági eseményekre reagáló csoportok (CSIRT) hálózatát is, amely összefogja az összes érintett érdekelt felet. Ezzel párhuzamosan a Bizottság és a CERT-EU aktívan figyelemmel kíséri a kiberfenyegetésekkel kapcsolatos helyzetet, és információcserét folytat a nemzeti hatóságokkal, így biztosítva, hogy az uniós intézmények információs technológiai rendszerei biztonságosak legyenek és ellenálljanak a kibertámadásoknak. A 2017 májusi, a WannaCry zsarolóprogramhoz köthető incidens volt az első alkalom, amikor a hálózat a tanácsok terjesztése útján operatív információcserét és együttműködést folytathatott. A fenyegetés mérséklése és az áldozatoknak való segítségnyújtás érdekében az EU számítógépes vészhelyzeteket elhárító csoportja szorosan együttműködött az Europolon belül működő Számítástechnikai Bűnözés Elleni Európai Központtal (EC3), az érintett országok számítógép-biztonsági eseményekre reagáló csoportjaival (CSIRT), a kiberbiztonsági egységekkel, valamint a legfontosabb ipari partnerekkel. A nemzeti helyzetjelentések megosztásának köszönhetően a helyzetismeret egységes volt az EU egészében. Ennek a tapasztalatnak köszönhetően a hálózat jobban felkészülhetett a következő incidensekre (mint amilyen például a „NonPetya"). Fény derült számos kihívásra is, ezek kezelése folyamatban van.

<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.

2016 júliusában a Bizottság – a tagállamokkal koordinálva – szerződéses kiberbiztonsági köz-magán társulást hozott létre az iparággal közösen, és a Horizont 2020 uniós kutatási és innovációs program keretében akár 450 millió EUR-t is beruházhat olyan technológiák kifejlesztésébe és tesztelésébe, amelyek hatékonyabb védelmet nyújtanak a felhasználók és az infrastruktúrák számára a hibrid fenyegetések számítástechnikai aspektusaival szemben. A társulásnak köszönhetően jött létre az első páneurópai stratégiai kutatási menetrend, amely a kritikus infrastruktúrák és a polgárok kibertámadásokkal szembeni ellenálló képességének javítására összpontosított. A társulás fokozta az érdekelt felek közötti koordinációt, ami növelte a hatékonyságot és az eredményességet a Horizont 2020 keretében nyújtott kiberbiztonsági finanszírozás terén. A társulás ezzel párhuzamosan dolgozik az információs és kommunikációs technológiák kiberbiztonsági tanúsításához kapcsolódó problémák megoldásán és azon is, hogy hogyan lehetne kezelni a kiberbiztonság terén képzett szakemberek akut munkaerőpiaci hiányát. Mivel a védelem terén jelentős a polgári célú kutatás iránti igény és nagy fokú ellenálló képességre van szükség, az Európai Védelmi Ügynökség kiberkutatási és kibertechnológiai csoportja kutatásokat végez az Európai Kiberbiztonsági Szervezet által annak stratégiai kutatási és innovációs menetrendjében meghatározott kutatási területeken is.

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.

Az energiaágazat terén a Bizottság ágazati kiberbiztonsági stratégiát dolgoz ki, és a kiberbiztonsági irányelv végrehajtásának támogatása érdekében létrehozza az energia-szakértők kiberbiztonsági platformját. Egy 2017. februári tanulmány meghatározta az intelligens fogyasztásmérési rendszerek kiberbiztonsági szintjének javítását szolgáló elérhető legjobb technológiákat, ez is támogatja a platform munkáját. A Bizottság emellett létrehozott egy internetes felületet „*Incident and Threat Information Sharing EU Centre*" (az incidensekre és fenyegetésekre vonatkozó információk megosztásának uniós központja) néven, amely elemzi és megosztja az energiaágazatot érintő kiberfenyegetésekre és incidensekre vonatkozó információkat.

A pénzügyi szektor hibrid fenyegetésekkel szembeni ellenálló képességének javítása

14. intézkedés: A Bizottság – az ENISA[15], 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.

Felismerve, hogy a kiberfenyegetések jelentik a pénzügyi stabilitásra leselkedő egyik fő veszélyt, a Bizottság felülvizsgálta az Európai Unióban a pénzforgalmi szolgáltatásokra alkalmazandó keretszabályokat, és a felülvizsgált szabályokat most végre kell hajtani. A pénzforgalmi szolgáltatásokról szóló felülvizsgált irányelv[16] új rendelkezéseket vezetett be a készpénz-helyettesítő fizetési eszközök biztonságosságának javítása céljából, és erős ügyfél-hitelesítést írt elő, hogy visszaszorítsa a csalásokat, különösen az online fizetések terén. Az új jogszabályi keret 2018 januárjától lesz alkalmazandó. A Bizottság – az Európai Bankhatóság segítségével és egyeztetve az érdekelt felekkel – jelenleg szabályozástechnikai standardokat dolgoz ki az erős ügyfél-hitelesítésre és a kölcsönös biztonságos kommunikációra vonatkozóan, hogy érvényesüljön a biztonság a fizetési műveletek során. A standardok várhatóan még 2017-ben megjelennek. Mindezeken túl a nemzetközi színtéren a Bizottság szorosan együttműködött az érintett G7-partnerekkel „a G7-ek pénzügyi szektorra vonatkozó kiberbiztonsági alapelvei" című dokumentum kidolgozásában, amelyet 2016 októberében hagytak jóvá a G7-ek pénzügyminiszterei és jegybankelnökei. Az alapelveket pénzügyi ágazatbeli szervezetekre szabták (mind magán-, mind közjogi szervezetekre), és azok hozzájárulnak a pénzügyi ágazaton belüli összehangolt kiberbiztonsági megközelítéshez, hogy közösen lehessen leküzdeni a kiberfenyegetéseket, még ha azok egyre jelentősebb méreteket öltenek és egyre kifinomultabbak is.

[15] Európai Uniós Hálózat- és Információbiztonsági Ügynökség.
[16] Az Európai Parlament és a Tanács (EU) 2015/2366 irányelve (2015. november 25.) a belső piaci pénzforgalmi szolgáltatásokról (HL L 337., 2015.12.23., 35. o.).

Közlekedés

15. intézkedés: 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.

Az Európai Unió tengerhajózási biztonsági stratégiájához kapcsolódó cselekvési terv[17] végrehajtása segíteni fog az információcsere, valamint a civil és katonai hatóságok közötti közös eszközhasználat terén uralkodó silómentalitás megtörésében. Az összkormányzati megközelítésnek köszönhetően javult a különféle szereplők közötti együttműködés. A tervek szerint 2017 végére elkészül a Bizottság és az EKSZ közös polgári-katonai stratégiai kutatási menetrendje, és sor kerül egy záró műhelytalálkozóra a kritikus tengeri infrastruktúrák védelme tárgyában. Ez a munka a jövőben kiterjeszthető, hogy átfogja a tenger alatt futó csővezetékekre, az energiaszállításra és a száloptikás és a hagyományos hírközlési kábelekre leselkedő, a nemzeti vizeken kívül történő beavatkozásból eredő új fenyegetések jelentette veszélyeket.

Egy nemrég megjelent tanulmány[18] értékelte a parti őrség feladatait ellátó tagállami hatóságok kockázatértékelési kapacitását. Feltárta az együttműködés legfontosabb akadályait, és gyakorlati megoldásokat javasolt a tengerészeti hatóságok közötti, ezen a speciális területen folytatott uniós és nemzeti szintű együttműködés javítására. A kockázatértékelés alapvető szerepet játszik a tengeri fenyegetések elleni küzdelemben, és kiemelten fontos a hibrid fenyegetések értékelése és megelőzése terén, mivel ezek további és még összetettebb mérlegelést igényelnek. A szóban forgó tanulmány eredményeit ismertetni fogják a parti őrséghez kapcsolódó különböző fórumokon, hogy sor kerülhessen a benne foglalt ajánlások értékelésére és megvalósítására, és ezáltal javuljon az együttműködés ezen a téren. A fő cél a hibrid fenyegetésekre való felkészülés és megfelelő reagálás.

A terrorizmus finanszírozása elleni küzdelem

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

A hibrid fenyegetések mögött álló személyeknek, illetve az ő támogatóiknak forrásokra van szükségük a terveik végrehajtásához. Az EU-nak a bűnözés és a terrorizmus finanszírozása elleni, az európai biztonsági stratégián és a terrorizmus finanszírozása elleni küzdelemről szóló cselekvési terven alapuló erőfeszítései is hozzájárulhatnak a hibrid fenyegetésekkel szembeni fellépéshez. 2016 decemberében a Bizottság három jogalkotási javaslatot terjesztett elő, többek között a pénzmosás büntetőjogi szankcióira és a jogellenes pénzeszköz-kifizetésekre, valamint az eszközök befagyasztására és elkobzására vonatkozóan[19].

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf, valamint az Európai Unió tengerhajózási biztonsági stratégiájához kapcsolódó cselekvési terv végrehajtásáról szóló második jelentés, amelyet 2017. június 21-én mutattak be a tagállamoknak.

[18] „Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions" (A parti őrség feladatait ellátó tagállami hatóságok szintjén meglévő kockázatértékelési kapacitás értékelése) című tanulmány, 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

[19] Harmadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról (COM(2016) 831 final).

2017. június 26-ig valamennyi tagállamnak át kellett ültetnie a negyedik pénzmosási irányelvet[20], és 2016 júliusában a Bizottság célzott jogalkotási javaslatot nyújtott be az irányelv kiegészítése és további intézkedésekkel való megerősítése érdekében[21].

2017. június 26-án a Bizottság kiadta a negyedik pénzmosási irányelvben előírt szupranacionális kockázatértékelést. Javaslatot tett egy rendeletre is a harmadik országokból illegálisan kivitt kulturális javak Unióba való behozatalának és ott történő tárolásának megelőzéséről[22]. A Bizottság még idén be fog számolni az arra vonatkozó, jelenleg folyó értékelésről, hogy szükség van-e további intézkedésekre a terrorizmus finanszírozásának EU-n belüli nyomon követése érdekében. A Bizottság emellett jelenleg végzi a készpénz-helyettesítő fizetési eszközökkel összefüggő csalás és hamisítás elleni küzdelemre vonatkozó jogszabályok felülvizsgálatát is[23].

A hatékony és valódi biztonsági unió megvalósításáról szóló nyolcadik eredményjelentés további részletekkel szolgál a terrorizmus finanszírozása elleni cselekvési terv végrehajtásának aktuális állásáról.

Az EU közös értékeinek érvényre juttatása és inkluzív, nyílt és ellenállóképes társadalmak megteremtése

A radikalizálódással és az erőszakos szélsőségességgel szembeni ellenálló képesség erősítése

A vallási és az ideológiai radikalizálódást, valamint az etnikai és a kisebbségekkel kapcsolatos konfliktusokat gerjeszthetik külső szereplők azáltal, hogy támogatást nyújtanak bizonyos csoportoknak vagy a csoportok közötti konfliktusok kiélezésére törekszenek. Újabb kihívások merültek fel, mint például a magányos elkövetők jelentette fenyegetés, a radikalizálódás új útjai, köztük a migrációs válság összefüggésében történő potenciális radikalizálódás, valamint a jobboldali szélsőségesség (és a migránsok elleni erőszak) terjedése, illetve a polarizálódás veszélye. Bár a radikalizálódással kapcsolatos munka a biztonsági unió összefüggésében folyik, közvetett módon jelentőséggel bírhat a hibrid fenyegetések szempontjából is, mivel a hibrid fenyegetések mögött álló személyek manipulálhatják azokat, akik fogékonyak a radikalizálódásra.

17. intézkedés: 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.

A radikalizálódás megelőzése

[20]Az Európai Parlament és a Tanács (EU) 2015/849 irányelve (2015. május 20.) a pénzügyi rendszerek pénzmosás vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről, a 648/2012/EU európai parlamenti és tanácsi rendelet módosításáról, valamint a 2005/60/EK európai parlamenti és tanácsi irányelv és a 2006/70/EK bizottsági irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg) (HL L 141., 2015.6.5., 73–117. o.).

[21] További részletekért lásd: Harmadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról (COM(2016) 831 final) és Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról (COM(2017) 354 final).

[22] COM(2017), 2017. június 26., COM(2017) 340 final, SWD(2017) 275 final.

[23] Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról (COM(2017) 354 final).

A Bizottság folytatja az erőszakos szélsőségességhez vezető radikalizálódás megelőzésének támogatásáról szóló 2016. júniusi közleményben[24] meghatározott, sokrétű válasz végrehajtását. Ennek kulcsintézkedései közé tartozik például az inkluzív oktatás támogatása és a közös értékek előtérbe helyezése, az online szélsőséges propaganda és a börtönökben zajló radikalizálódás kezelése, a harmadik országokkal folytatott együttműködés megerősítése, valamint a radikalizálódás folyamatosan változó jellegének mélyebb megértését szolgáló és a szakpolitikai válaszokat pontosabb információkkal megalapozó kutatások támogatása. A Bizottság által a tagállamok számára e téren nyújtott támogatáshoz kapcsolódó munka elsődleges keretét az uniós radikalizálódástudatossági hálózat (RAN) jelenti, amely a közösségek szintjén dolgozik együtt a helyi szakemberekkel. További részletekkel a hatékony és valódi biztonsági unió megvalósításáról szóló nyolcadik eredményjelentés[25] szolgál.

Online radikalizálódás és gyűlöletbeszéd

Az európai biztonsági stratégiának[26] megfelelően a Bizottság – elsősorban az Europol szélsőséges internetes tartalmakkal foglalkozó uniós egysége és az Európai Uniós Internetfórum[27] útján – lépéseket tett annak érdekében, hogy minél kevesebb jogellenes tartalom legyen elérhető az interneten. Jelentős előrehaladás történt a jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódex[28] nyomán is. További részletekkel a hatékony és valódi biztonsági unió megvalósításáról szóló nyolcadik eredményjelentés[29] szolgál. E fellépések intenzitása fokozódni fog, figyelemmel az Európai Tanács következtetéseire[30], a G7-ek csúcstalálkozójára[31] és a G20-ak hamburgi csúcstalálkozójára[32] is.

Az online platformok kulcsszerepet játszanak az illegális vagy potenciálisan káros tartalmak kezelésében. A Bizottság a digitális egységes piaci stratégia alapján – ahogyan a félidős értékelésben[33] is szerepel – biztosítja a platformokról folyó párbeszédek jobb összehangolását, a jogellenes tartalom eltávolítását szolgáló mechanizmusokra és technikai megoldásokra összpontosítva. Adott esetben a cél ezeknek a mechanizmusoknak olyan szempontokra vonatkozó iránymutatással történő alátámasztása, mint a jogellenes tartalom bejelentése és törlése. A Bizottság iránymutatást fog nyújtani a felelősségre vonatkozó szabályokkal kapcsolatban is.

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf
[25] COM(2017) 354 final.
[26] További részletekért lásd: Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról, COM(2017) 354 final.
[27] További részletekért lásd: Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról, COM(2017) 354 final.
[28] A jogellenes online gyűlöletbeszéd felszámolására vonatkozó magatartási kódex, 2016. május 31., http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf
[29] További részletekért lásd: Nyolcadik eredményjelentés a hatékony és valódi biztonsági unió megvalósításáról, COM(2017) 354 final.
[30] A Tanács 2017. június 22–23-i következtetései.
[31] G7 csúcstalálkozó, Taormina, Olaszország, 2017. május 26–27.
[32] G20 csúcstalálkozó, Hamburg, Németország, 2017. július 7–8.
[33] Lásd a Bizottság fent említett, COM (2017) 228 final számú közleményét.

A harmadik országokkal folytatott együttműködés megerősítése

18. intézkedés: ***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.***

Az Európai Unió fokozott figyelmet fordít a partnerországok biztonsági ágazatában történő kapacitásépítésre és ellenállóképesség-javításra többek között azáltal, hogy kihasználja a biztonság és a fejlesztés közötti kapcsolatot, kialakítja a felülvizsgált európai szomszédságpolitika biztonsági dimenzióját, valamint terrorelhárítási és biztonsági tárgyú párbeszédeket kezdeményez a Földközi-tenger partján fekvő országokkal. Ennek kapcsán elindult egy kísérleti kockázatfelmérési projekt a Moldovai Köztársaság részvételével. A célja az, hogy segítsen azonosítani az ország legfontosabb sebezhető pontjait, és biztosítsa, hogy az uniós segítség kifejezetten ezeket a területeket célozza meg. A kísérleti projekt eredményei azt mutatták, hogy maga a felmérés hasznosnak bizonyult. A tapasztalatok alapján a Bizottság és az EKSZ ajánlásokat fog tenni a hatékonyságfokozás, a stratégiai kommunikáció, a kritikus infrastruktúrák védelme és a kiberbiztonság körébe tartozó intézkedések kiemelt kezelésére vonatkozóan.

A jövőben – ezekre az első tapasztalatokra építve – további szomszédos országok számára is hasznos lehet a felmérés, bár testre kell szabni, hogy tükrözze az egyes országok eltérő helyi viszonyait és az őket érő sajátos fenyegetéseket, és ne legyen átfedésben folyamatban lévő más terrorelhárítási és biztonsági párbeszédekkel. Általánosabb szinten a Bizottság és a főképviselő 2017. június 7-én elfogadott egy közös közleményt[34] „Az ellenálló képesség stratégiai megközelítése az EU külső tevékenységeiben” címmel. A cél: támogatni a partnerországokat abban, hogy ellenállóképesebbé váljanak napjaink globális kihívásaival szemben. A közleményben szerepel az a felismerés, hogy válságkezelés helyett strukturáltabb, hosszú távú megközelítésre kell átállni a sebezhető pontok kapcsán, és az előrejelzésre, a megelőzésre és a felkészültségre kell helyezni a hangsúlyt.

A kibertámadásokkal szembeni ellenálló képesség a fejlődés szolgálatában

Az EU támogatja az Európán kívüli országokat annak érdekében, hogy megerősödjön azok információs hálózatainak ellenálló képessége. Az egyre terjedő digitalizációnak elkerülhetetlenül vannak biztonsági vonatkozásai is, ami az egész világon jelentős kihívások elé állítja az információs hálózati rendszerek ellenálló képességét, mivel a kibertámadások nem ismernek határokat. Az EU támogatja a harmadik országokat abban, hogy megerősítsék a véletlen hibák és a kibertámadások hatékony megelőzéséhez, illetve az azokra való megfelelő reagáláshoz szükséges képességeiket. A Macedónia Volt Jugoszláv Köztársaságban, Koszovóban[35] és Moldovában lebonyolított, 2016-ban zárult kísérleti kiberbiztonsági

[34]Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az ellenálló képesség stratégiai megközelítése az EU külső tevékenységeiben, JOIN (2017) 21 final.

[35] Ez a megnevezés nem érinti a jogállással kapcsolatos álláspontokat, továbbá összhangban van az 1244 sz. ENSZ BT-határozattal és a Nemzetközi Bíróságnak a koszovói függetlenségi nyilatkozatról szóló véleményével.

projektet követően a Bizottság új programot fog indítani harmadik országok kibertámadásokkal szembeni ellenálló képességének fokozása céljából. A 2017–2020-as időszakban ez elsősorban Afrikát és Ázsiát fogja érinteni, de Ukrajna is részt vesz a projektben. A cél a harmadik országbeli kritikus információs infrastruktúrák és hálózatok biztonságának és felkészültségének javítása összkormányzati megközelítés alapján, garantálva az emberi jogok és a jogállamiság elvének tiszteletben tartását.

A légi közlekedés védelme

A polgári légi közlekedés továbbra is kiemelt és szimbolikus célpontot jelent a terroristák számára, de célpont lehet egy hibrid hadjárat esetén is. Az EU kidolgozott ugyan egy szilárd légiközlekedés-védelmi keretrendszert, de a harmadik országokból érkező járatok sebezhetőbbek lehetnek. Az ENSZ Biztonsági Tanácsának 2309 (2016) számú határozatával összhangban a Bizottság fokozza a harmadik országokban történő kapacitásépítést célzó erőfeszítéseit. 2017 januárjában a Bizottság új, integrált kockázatértékelést vezetett be, hogy biztosítsa az uniós és tagállami szinten, illetve nemzetközi partnereknél végrehajtott kapacitásépítési intézkedések fontossági sorrendjének megállapítását és az intézkedések összehangolását. 2016-ban a Bizottság négyéves polgári légiközlekedés-védelmi projektet indított Afrikában és az Arab-félszigeten, hogy így szálljon szembe a polgári légi közlekedést érintő terrorizmusveszéllyel. A projekt középpontjában a partnerországok, illetve az Európai Polgári Repülési Konferencia tagállamainak szakértői közötti tapasztalatcsere, valamint mentorálási, képzési és tanácsadási tevékenységek állnak. 2017 során még intenzívebbé válnak a tevékenységek.

c) A VÁLSÁG MEGELŐZÉSE, KEZELÉSE ÉS HATÁSAINAK ELHÁRÍTÁSA

Bár a következmények hosszú távú tagállami és uniós szakpolitikák révén enyhíthetők, rövid távon elengedhetetlenül szükséges marad a tagállamok és az Unió azon képességeinek erősítése, amelyek segítségével gyors és összehangolt módon képesek megelőzni a hibrid fenyegetéseket, válaszlépéseket tenni azokra, és elhárítani a következményeiket. Elengedhetetlenül fontos, hogy képesek legyünk gyorsan reagálni a hibrid fenyegetések által kiváltott eseményekre. Tavaly jelentős előrelépést sikerült elérni ezen a területen, bevezetésre került az EU-ban egy operatív protokoll, amely meghatározza a hibrid támadás esetén követendő válságkezelési eljárást. A továbbiakban rendszeres nyomon követésre és gyakorlatokra fog sor kerülni.

19. intézkedés: ***A főképviselő és a Bizottság, a tagállamokkal együttműködésben, a válságkezelési és a politikai szintű integrált válságelhárítási 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.***

A közös keret a hibrid fenyegetések által kiváltott eseményekre való gyors reagálást lehetővé tevő mechanizmusok bevezetését javasolta az uniós válaszmechanizmusok[36] és a korai előrejelző rendszerek közötti koordináció érdekében. Ebből a célból a Bizottság szolgálatai és az EKSZ kiadták a hibrid fenyegetésekkel szembeni fellépés uniós operatív protokollját („EU

[36] A Tanács uniós politikai szintű integrált válságelhárítási intézkedései, a Bizottság ARGUS rendszere és az EKSZ CRM rendszere.

Playbook)”[37], amely felvázolja azokat a gyakorlati szabályokat, melyeket hibrid fenyegetés esetén kell alkalmazni a koordinációra, a hírszerzési információk szintetizálására és elemzésére, az információk szakpolitikai döntéshozatali folyamatokban való felhasználására, a gyakorlatokra és a képzésre, valamint a partnerszervezetekkel – elsősorban a NATO-val – való együttműködésre. Hasonlóképpen a NATO is kidolgozott egy protokollt a hibrid fenyegetések megelőzésével és leküzdésével kapcsolatos, a kibervédelem, a stratégiai kommunikáció, a helyzetismeret és a válságkezelés területén folytatott fokozott NATO–EU együttműködésre vonatkozóan. Az uniós operatív protokoll próbájára 2017 őszén, az Európai Unió párhuzamos és koordinált gyakorlata keretében fog sor kerülni, amelynek a NATO-val való együttműködés is részét képezi.

<u>20. intézkedés</u>: 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.

Az EUSZ 42. cikkének (7) bekezdése egy tagállam területe elleni fegyveres támadásról szól, az EUMSZ 222. cikke (szolidaritási klauzula) pedig arra az esetre vonatkozik, ha valamely tagállam területén terrortámadás, illetve természeti vagy ember okozta katasztrófa következik be. A bűncselekmények és felforgató tevékenységek keverékeként jellemezhető hibrid támadások esetén az utóbbi rendelkezés alkalmazása a valószínűbb. A szolidaritási klauzula alkalmazására vonatkozó kérés nyomán tanácsi szintű egyeztetés indul (politikai szintű integrált válságelhárítási intézkedések), bekapcsolódnak az érintett uniós intézmények, ügynökségek és szervek, valamint működésbe lépnek az uniós segítségnyújtási programok és mechanizmusok. A 2014/415/EU tanácsi határozat határozza meg a szolidaritási klauzula Unió által történő végrehajtására vonatkozó részletes szabályokat. Ezek a részletes alkalmazási szabályok továbbra is érvényesek, nincs szükség a tanácsi határozat felülvizsgálatára. Ha egy hibrid támadás során fegyveres agresszióra is sor kerül, a 42. cikk (7) bekezdése is alkalmazhatóvá válhat. Ilyen esetben mind a tagállamoknak, mind pedig az EU-nak segítséget és támogatást kell nyújtania. A Bizottság és a főképviselő folytatják annak értékelését, hogy milyen módszerekkel kezelhetők leghatékonyabban az ilyen támadások.

A fent említett uniós operatív protokoll elfogadása közvetlenül támogatja ezt az értékelést. A protokoll az EU 2017. októberi párhuzamos és koordinált gyakorlata (PACE) során kerül kipróbálásra. Ez a gyakorlat tesztelni fogja a különböző uniós mechanizmusokat és az EU együttműködési képességét, a célja pedig a döntéshozatal felgyorsítása olyan helyzetekben, amikor egy hibrid fenyegetés által kiváltott bizonytalanság rontja a tisztánlátást.

<u>21. intézkedés:</u> 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.

A katonai képességeknek a KKBP/KBVP támogatása érdekében történő integrációjára vonatkozó feladat kiadására reagálva, egy katonai szakértők részvételével 2016 decemberében lefolytatott szeminárium után, az Európai Unió Katonai Bizottság munkacsoportjától származó 2017. májusi iránymutatásokat követve 2017 júliusában véglegesítésre kerültek a katonai tanácsok az „uniós katonai hozzájárulás a hibrid fenyegetésekkel szembeni fellépéshez a KBVP keretében” tárgyában. Az ezzel kapcsolatos további lépésekre a koncepciókidolgozás területére vonatkozó végrehajtási terv útján kerül sor.

[37] (2016) 227. sz. bizottsági szolgálati munkadokumentum, elfogadás dátuma: 2016. július 7.

d) EU–NATO EGYÜTTMŰKÖDÉS

<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.

Az Európai Tanács és az Európai Bizottság elnöke, valamint a NATO főtitkára által 2016. július 8-án Varsóban aláírt együttes nyilatkozat alapján az EU és a NATO kidolgozott egy 42, végrehajtásra vonatkozó javaslatot tartalmazó közös listát, amelyet ezt követően külön-külön, párhuzamos eljárások keretében 2016. december 6-án jóváhagyott mind az EU, mind a NATO Tanácsa[38]. 2017 júniusában a főképviselő/alelnök és a NATO főtitkára jelentést tett közzé az együttes nyilatkozatban foglalt 42 intézkedéssel kapcsolatban elért előrehaladásról. A hibrid fenyegetésekkel szembeni fellépés egyike az együttes nyilatkozatban azonosított hét együttműködési területnek, és a 42 intézkedés közül tíz ehhez a tárgykörhöz kapcsolódik. A jelentésből az derül ki, hogy az elmúlt év során tett közös erőfeszítések jelentős eredményeket hoztak. A hibrid fenyegetésekkel szembeni fellépést célzó egyedi intézkedések közül sokat már említettünk, ezek közé tartozik a Hibrid Fenyegetések Elleni Küzdelem Európai Kiválósági Központja, a javuló helyzetismeret, a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport létrehozása és annak a NATO újonnan létrehozott, hibrid fenyegetéseket elemző csoportjával való együttműködése, valamint a stratégiai kommunikációval foglalkozó csoportok közötti együttműködés. Most első alkalommal a NATO és az EU személyzete közösen fogja gyakorolni a hibrid forgatókönyv megvalósulása esetén adandó választ. Az elképzelések szerint a gyakorlat során vizsgálni fogják a közös javaslatok több mint egyharmadának végrehajtását. Az EU idén végrehajtja a saját párhuzamos és koordinált gyakorlatát is, és arra készül, hogy 2018-ban vezető szerepet fog betölteni.

Az ellenálló képesség kapcsán mind az EU, mind a NATO munkatársai részt vettek kölcsönös tájékoztatókon, többek között az EU politikai szintű integrált válságelhárítási mechanizmusának tárgyában. A NATO és az EU személyzete közötti rendszeres kapcsolattartás, amely például műhelytalálkozók vagy az Európai Védelmi Ügynökség irányítóbizottságában való NATO-részvétel útján valósult meg, lehetővé tette a NATO nemzeti ellenálló képességre vonatkozó alapkövetelményeit érintő információcserét. A tervek szerint ősszel további eszmecserére kerül sor a Bizottság és a NATO között az ellenálló képesség megerősítése tárgyában. Az EU–NATO együttműködésről szóló következő előrehaladási jelentés tartalmazni fog a két szervezet közötti együttműködés kiterjesztésének lehetőségeire vonatkozó javaslatokat.

3. KÖVETKEZTETÉS

A közös keret olyan fellépéseket körvonalaz, amelyek kidolgozására a hibrid fenyegetésekkel szembeni küzdelem, valamint az Unió, a tagállamok és a partnerek ellenálló képessége erősítésének elősegítése céljából került sor. Míg a Bizottság és a főképviselő a tagállamokkal és a partnerekkel szoros együttműködésben minden területen eredményeket ér el, kulcsfontosságú, hogy az aktuális és folyamatosan változó hibrid fenyegetések ne törjék meg ezt a lendületet. A nemzetbiztonsághoz és a közrend fenntartásához kapcsolódó hibrid

[38] http://www.consilium.europa.eu/hu/press/press-releases/2016/12/06-eu-nato-joint-declaration/

fenyegetésekkel szembeni fellépés elsősorban a tagállamok feladata. A nemzeti ellenálló képesség és a hibrid fenyegetésekkel szembeni védelmet célzó kollektív erőfeszítések ugyanazon általános törekvés egymást kölcsönösen erősítő elemeiként értelmezendők. Ezért arra ösztönözzük a tagállamokat, hogy a lehető leggyorsabban végezzék el a hibrid fenyegetésekre vonatkozó felméréseket, mivel azok értékes információkat szolgáltatnak arról, milyen mértékű a sebezhetőség, illetve a felkészültség Európában. A tudatosságnövelés terén elért jelentős előrelépésekre építve maximalizálni kell a hibrid fenyegetésekkel foglalkozó uniós információs és elemzőcsoport potenciálját. A főképviselő felkéri a tagállamokat, hogy a hibrid fenyegetések szaporodása elleni hatékonyabb fellépés érdekében támogassák a stratégiai kommunikációval foglalkozó munkacsoportok munkáját. Az EU teljes mértékben támogatni fogja A Hibrid Fenyegetések Elleni Küzdelem Európai Központját, melyet Finnország irányít.

Az EU egyedülálló ereje abban rejlik, hogy a meglévő eszközök és programok széles körére támaszkodva segíti a tagállamokat és a partnereket az ellenálló képességük megerősítésében. Jelentős előrelépés történt az ellenálló képesség fokozása kapcsán olyan területeken, mint a közlekedés, az energiaágazat, a kiberbiztonság, a kritikus infrastruktúrák, a pénzügyi rendszer jogellenes használatával szembeni védelem vagy az erőszakos szélsőségek és a radikalizálódás elleni küzdelem. Az ellenálló képesség megerősítését célzó uniós fellépés folytatódni fog, mivel a hibrid fenyegetések jellege folyamatosan változik. Az EU mutatókat fog kidolgozni annak érdekében, hogy javítsa a kritikus infrastruktúrák védelmét és a hibrid fenyegetésekkel szembeni ellenálló képességét a fontos ágazatokban.

A hibrid fenyegetésekkel szembeni ellenálló képesség erősítése érdekében az Európai Védelmi Alap a tagállamokkal együtt társfinanszírozást nyújthat a képességeket érintő prioritásokhoz. A közelgő kiberbiztonsági jogszabálycsomag, valamint a hálózati és információs rendszerek biztonságáról szóló irányelv végrehajtását célzó ágazatközi intézkedések EU-szerte új platformokat fognak biztosítani a hibrid fenyegetésekkel szembeni fellépéshez.

A Bizottság és a főképviselő felszólítják a tagállamokat és az érdekelt feleket arra, hogy szükség esetén mielőbb jussanak megállapodásra, és biztosítsák az ellenálló képesség megerősítését célzó, ebben a közleményben említett számos intézkedés gyors és hatékony végrehajtását. Az EU támaszkodni fog a NATO-val folytatott, már jelenleg is gyümölcsöző együttműködésre, és el fogja mélyíteni azt.

Az Unió továbbra is elkötelezett amellett, hogy az összetett hibrid fenyegetésekkel szembeni fellépés érdekében minden releváns uniós eszközt mobilizálni fog. A tagállamok erőfeszítéseinek támogatása a továbbiakban is prioritást jelent az Unió számára, amely – legfontosabb partnereivel karöltve – erősebb és reakcióképesebb biztonságfenntartóként lép fel.