Az Európai Unió
Tanácsa

Brüsszel, 2019. május 14.
(OR. en)

7299/19

LIMITE

CORLX 106
CFSP/PESC 191
RELEX 235
CYBER 81
JAI 264
FIN 216

JOGALKOTÁSI AKTUSOK ÉS EGYÉB ESZKÖZÖK

Tárgy:	A TANÁCS HATÁROZATA az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

A TANÁCS (KKBP) 2019/... HATÁROZATA

(...)

az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

AZ EURÓPAI UNIÓ TANÁCSA,

tekintettel az Európai Unióról szóló szerződésre és különösen annak 29. cikkére,

tekintettel az Unió külügyi és biztonságpolitikai főképviselőjének javaslatára,

mivel:

(1) A Tanács 2017. június 19-én elfogadta a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretéről („kiberdiplomáciai eszköztár”) szóló következtetéseket, amelyekben a Tanács jelezte, hogy aggodalommal tölti el az állami és nem állami szereplők részéről mutatkozó, arra való fokozott képesség és hajlandóság, hogy céljaikat rossz szándékú kibertevékenységek révén igyekezzenek elérni, továbbá megállapította, hogy egyre nagyobb szükség van arra, hogy megvédjük az Unió, az uniós tagállamok és az uniós polgárok sértetlenségét és biztonságát a kiberveszélyekkel és a rossz szándékú kibertevékenységekkel szemben.

(2) A Tanács nyomatékosította, hogy a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések várható következményeinek egyértelmű jelzése hatással van a kibertámadások potenciális elkövetőire, és ezáltal erősíti az EU-nak és tagállamainak biztonságát, továbbá megerősítette, hogy a közös kül- és biztonságpolitika (KKBP) területéhez tartozó intézkedések, beleértve szükség esetén a Szerződések vonatkozó előírásai alapján elfogadott korlátozó intézkedéseket is, alkalmas eszközök lehetnek a rossz szándékú kibertevékenységekkel szembeni közös uniós diplomáciai fellépésre azzal a céllal, hogy ösztönözzék az együttműködést, előmozdítsák az azonnali és a hosszú távú veszélyek csökkentését, valamint hogy hosszú távon hatással legyenek a potenciális támadók magatartására.

(3) A Politikai és Biztonsági Bizottság 2017. október 11-én a kiberdiplomáciai eszköztárra vonatkozóan végrehajtási iránymutatásokat hagyott jóvá. A végrehajtási iránymutatások a kiberdiplomáciai eszköztáron belül öt intézkedéskategóriát említenek, köztük a korlátozó intézkedéseket, valamint ezen intézkedések bevezetésére vonatkozó eljárást.

(4) A rossz szándékú kibertevékenységekről szóló, 2018. április 16-i tanácsi következtetésekben a Tanács határozottan elítélte az információs és kommunikációs technológia (a továbbiakban: az IKT) rossz szándékú felhasználását és hangsúlyozta, hogy az IKT-k rossz szándékú felhasználása elfogadhatatlan, mert veszélyezteti a stabilitást és a biztonságot, valamint annak következtében erodálódnak azok a kedvező hatások, amelyek az internetből és az IKT-k használatából fakadnak. A Tanács emlékeztetett arra, hogy a kiberdiplomáciai eszköztár hozzájárul a kibertérben a konfliktusmegelőzéshez, az együttműködéshez és a stabilitáshoz azzal, hogy a KKBP területén olyan intézkedések, többek között korlátozó intézkedések bevezetését teszi lehetővé, amelyekkel a rossz szándékú kibertevékenységek megelőzhetők, illetve fel lehet lépni ellenük. Kijelentette, hogy az Unió továbbra is határozottan kiáll amellett, hogy a hatályos nemzetközi jogot alkalmazni kell a kibertérre, és hangsúlyozta, hogy a nemzetközi jognak – mindenekelőtt az ENSZ Alapokmányának – a tiszteletben tartása elengedhetetlen a béke és a stabilitás fenntartásához. Emellett a Tanács azt is kiemelte, hogy az államok nem bízhatnak meg másokat nemzetközi jogot sértő cselekmények IKT-k felhasználásával történő elkövetésére, és törekedniük kell annak biztosítására, hogy nem állami szereplők ne használhassák területüket ilyen cselekmények elkövetésére, ahogyan azt a nemzetközi biztonság összefüggésében az információs és távközlési technológiák területén végbemenő fejleményekkel foglalkozó illetékes ENSZ kormányzati szakértői csoport a 2015. évi jelentésében megfogalmazta.

(5) Az Európai Tanács 2018. június 28-án következtetéseket fogadott el, amelyekben hangsúlyozta, hogy meg kell erősíteni az Unión kívülről kiinduló kiberbiztonsági fenyegetések elhárítására szolgáló képességeket. Arra kérte az intézményeket és a tagállamokat, hogy hajtsák végre a Bizottság és az Unió külügyi és biztonságpolitikai főképviselője „Ellenálló képesség, elrettentés és védelem – erős kiberbiztonság kialakítása az EU-ban” című, 2017. szeptember 13-i közös közleményben említett intézkedéseket, ideértve a kiberdiplomáciai eszköztár gyakorlati használatát is.

(6) Az Európai Tanács 2018. október 18-án következtetéseket fogadott el, amelyekben arra szólított fel, hogy a Tanács 2017. június 19-i következtetéseivel összhangban tovább kell vinni azt a munkát, amelynek célja, hogy a kibertámadásokkal szemben képesek legyünk uniós korlátozó intézkedések alkalmazásával az elrettentésre, illetve a reagálásra. Felszólított továbbá arra, hogy az Unió kibertámadásokkal szembeni ellenálló képességének megerősítése érdekében minden, kiberbiztonsággal kapcsolatos javaslat tárgyalását le kell zárni még a jelenlegi jogalkotási ciklus vége előtt.

(7) Ezzel összefüggésben ez a határozat keretet hoz létre a jelentős hatású, az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentő kibertámadások elkövetésének megakadályozását és az elhárításukat célzó célzott korlátozó intézkedésekhez. Ha azt az Európai Unióról szóló szerződés 21. cikkének vonatkozó rendelkezéseiben foglalt közös kül- és biztonságpolitikai célok eléréséhez szükségesnek ítélik, ez a határozat lehetővé teszi továbbá azt, hogy a jelentős hatású kibertámadásokra válaszul korlátozó intézkedéseket lehessen alkalmazni harmadik államokkal vagy nemzetközi szervezetekkel szemben.

(8) Az elrettentő és visszatartó hatás érdekében a célzott korlátozó intézkedéseknek az e határozat hatálya alá tartozó azon kibertámadásokra kell összpontosulniuk, amelyeket szándékosan követnek el.

(9) A célzott korlátozó intézkedéseket meg kell különböztetni valamely harmadik államnak a kibertámadásokért való felelőssé tételétől. Célzott korlátozó intézkedések alkalmazása nem jelent ilyen felelőssé tételt, ami egy eseti alapon hozott, szuverén politikai döntés. Minden tagállam szabadon dönt arról, hogy bizonyos kibertámadásokat valamely harmadik államnak tulajdonít.

(10) Egyes intézkedések végrehajtásához az Unió további fellépése szükséges,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

(1) Ezt a határozatot azokra a jelentős hatású kibertámadásokra kell alkalmazni – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.

(2) A külső fenyegetésnek minősülő kibertámadások közé tartoznak azok a kibertámadások,

a) amelyek az Unión kívülről erednek, vagy amelyeket az Unión kívül követnek el;

b) amelyek Unión kívüli infrastruktúrát alkalmaznak;

c) amelyeket az Unión kívül letelepedett vagy tevékenységét az Unión kívül végző természetes vagy jogi személy, szervezet vagy szerv követ el; vagy

d) amelyeket a tevékenységét az Unión kívül végző természetes vagy jogi személy, szervezet vagy szerv támogatásával, irányításával vagy ellenőrzése alatt követnek el.

(3) E tekintetben kibertámadásnak minősülnek az alábbiak bármelyikét magukban foglaló tevékenységek:

a) információs rendszerekhez való hozzáférés;

b) információs rendszerekbe történő beavatkozás;

c) adatokat érintő beavatkozás; vagy

d) adatkifürkészés,

amennyiben ezeket a tevékenységeket a rendszernek vagy az adatoknak vagy azok valamely részének a tulajdonosa vagy más jogosultja nem engedélyezte megfelelően, vagy ha ezeket a tevékenységeket az Unió vagy az érintett tagállam joga nem teszi lehetővé.

(4) A tagállamok számára veszélyt jelentő kibertámadások közé tartoznak azok, amelyek többek között az alábbiakhoz kapcsolódó információs rendszereket érintik:

a) olyan kritikus infrastruktúra – így a tenger alatti kábelek és a világűrbe felbocsátott objektumok is –, amely elengedhetetlen a társadalom létfontosságú funkcióinak vagy az emberek egészségének, biztonságának, védelmének, illetve gazdasági vagy szociális jólétének fenntartásához;

b) alapvető társadalmi és/vagy gazdasági tevékenységek fenntartásához elengedhetetlen szolgáltatások, különösen következő ágazatok vonatkozásában: az energiaágazat (villamos energia, kőolaj és földgáz); a közlekedési ágazat (légi, vasúti, vízi és közúti közlekedés); a bankszektor; a pénzügyi piaci infrastruktúrák; az egészségügy (egészségügyi szolgáltatók, kórházak és magánklinikák); az ivóvízellátás és ivóvízelosztás; a digitális infrastruktúra; és az érintett tagállam számára alapvető fontosságú bármely egyéb ágazat terén;

c) kritikus állami funkciók, különösen a következő területeken: védelem; intézmények irányítása és működése; a nyilvános választásokat és a szavazási folyamatot is ideértve; gazdasági és polgári infrastruktúra működése; belső biztonság; valamint külkapcsolatok, többek között diplomáciai képviseletek révén;

d) minősített adatok tárolása és kezelése; vagy

e) kormányzati veszélyhelyzet-elhárító csoportok.

(5) Az Unió számára veszélyt jelentő kibertámadások közé tartoznak azok, amelyeket az intézményei, szervei és hivatalai, a harmadik országokban található küldöttségei, illetve a nemzetközi szervezeteknél működő képviseletei, a közös biztonság- és védelempolitika (KBVP) műveletei és missziói, valamint a különleges képviselői ellen intéznek.

(6) Ha azt az Európai Unióról szóló szerződés 21. cikkének vonatkozó rendelkezéseiben foglalt KBVP célok eléréséhez szükségesnek ítélik, a jelentős hatású kibertámadásokra válaszul e határozat alapján korlátozó intézkedéseket lehet alkalmazni harmadik országokkal vagy nemzetközi szervezetekkel szemben is.

2. cikk

E határozat alkalmazásában:

a) „információs rendszerek”: olyan eszköz vagy összekapcsolt, illetve egymáshoz kapcsolódó eszközök olyan csoportja, amelyek közül egy vagy több – egy program alapján – digitális adatok automatikus kezelését végzi, valamint az ezen eszköz, illetve ezen eszközök csoportja által saját működése, használata, védelme és karbantartása céljából tárolt, kezelt, beolvasott vagy továbbított digitális adatok;

b) „információs rendszerekbe történő beavatkozás”: az információs rendszer működésének akadályozása vagy megszakítása digitális adatok bevitelével, továbbításával, károsításával, törlésével, rongálásával, megváltoztatásával, eltávolításával vagy hozzáférhetetlenné tételével;

c) „adatokat érintő beavatkozás”: az információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele; e fogalom magában foglalja továbbá az adatlopást, valamint a pénzeszközök, a gazdasági erőforrások, illetve a szellemi tulajdon eltulajdonítását is;

d) „adatkifürkészés”: digitális adatok információs rendszeren belüli, oda irányuló vagy onnan kiinduló nem nyilvános továbbításának – így például az információs rendszerből kibocsátott, ilyen digitális adatokat hordozó elektromágneses jeleknek – a kifürkészése műszaki eszközökkel;

3. cikk

Annak megállapításához, hogy egy kibertámadás az 1. cikk (1) bekezdésében említett jelentős hatással bír-e, bármelyik következő tényező figyelembe vehető:

a) a – többek között a gazdasági és társadalmi tevékenységek, az alapvető szolgáltatások, a kritikus állami funkciók, a közrend és a közbiztonság tekintetében – előidézett zavar hatóköre, léptéke, hatása és súlyossága;

b) az érintett természetes vagy jogi személyek, szervezetek és szervek száma;

c) az érintett tagállamok száma;

d) a – például pénzeszközök, gazdasági erőforrások vagy szellemi tulajdon nagyszabású eltulajdonítása révén – okozott gazdasági veszteség mértéke;

e) az elkövető által saját maga vagy mások számára szerzett gazdasági előny;

f) az ellopott adatok mennyisége és jellege, vagy az adatvédelmi incidensek léptéke; vagy

g) azon kereskedelmi szempontból érzékeny adatok jellege, amelyekhez az illetéktelenek hozzáfértek.

4. cikk

(1) A tagállamok meghozzák az annak megakadályozásához szükséges intézkedéseket, hogy a területükre belépjenek vagy azon átutazzanak:

a) azon természetes személyek, akik kibertámadás elkövetéséért vagy megkísérléséért felelősek;

b) azon természetes személyek, akik kibertámadás elkövetéséhez vagy megkísérléséhez pénzügyi, technikai vagy anyagi támogatást nyújtanak vagy abban más módon közreműködnek, ideértve az ilyen támadások tervezését, előkészítését, az azokban való részvételt, azok irányítását, az azokhoz való segítségnyújtást és azok ösztönzését vagy azok cselekmény vagy mulasztás révén történő megkönnyítését;

c) az e bekezdés a) és b) pontjának hatálya alá tartozó személyekkel kapcsolatban álló természetes személyek;

a mellékletben felsoroltak szerint.

(2) Az (1) bekezdés nem kötelezi a tagállamokat arra, hogy saját állampolgáraik esetében megtagadják a területükre való belépést.

(3) Az (1) bekezdés nem érinti azokat az eseteket, amikor valamely tagállamot nemzetközi jogi kötelezettség terhel, nevezetesen:

a) egy nemzetközi kormányközi szervezetnek helyet adó országként;

b) az Egyesült Nemzetek által vagy annak védnöksége alatt összehívott nemzetközi konferenciának helyet adó országként;

c) kiváltságokat és mentességeket biztosító többoldalú megállapodás alapján; vagy

d) az Apostoli Szentszék (Vatikánvárosi Állam) és Olaszország között 1929-ben a megbékélésről létrejött szerződés (Lateráni Egyezmény) alapján.

(4) A (3) bekezdést azokra az esetekre is alkalmazandónak kell tekinteni, amikor egy tagállam az Európai Biztonsági és Együttműködési Szervezetnek (EBESZ) ad otthont.

(5) A Tanácsot megfelelően értesíteni kell minden olyan esetről, amikor egy tagállam a (3) vagy a (4) bekezdés értelmében mentességet ad.

(6) A tagállamok mentességet adhatnak az (1) bekezdés alapján előírt intézkedések alól, ha az utazás indoka sürgős humanitárius szükséghelyzet vagy olyan – kormányközi vagy az Unió által támogatott vagy a területén tartott üléseken, vagy az EBESZ soros elnökségét betöltő tagállamban tartott – üléseken való részvétel, amelyen a korlátozó intézkedések politikai célját – így többek között a kibertér biztonságát és stabilitását – közvetlenül előmozdító politikai párbeszéd zajlik.

(7) A tagállamok szintén mentességet adhatnak az (1) bekezdés alapján előírt intézkedések alól, ha a belépés vagy az átutazás bírósági eljárás lefolytatása miatt szükséges.

(8) A (6) és a (7) bekezdésben említett mentességeket megadni kívánó tagállam erről írásban értesíti a Tanácsot. A mentességet megadottnak kell tekinteni, ha az ellen a Tanács egy vagy több tagja a javasolt mentességről szóló értesítés kézhezvételétől számított két munkanapon belül nem emel írásban kifogást. Amennyiben a Tanács egy vagy több tagja kifogást emel, a Tanács minősített többséggel határozhat a javasolt mentesség megadásáról.

(9) Amennyiben a (3), a (4), a (6), a (7) vagy a (8) bekezdésnek megfelelően egy adott tagállam engedélyezi a mellékletben felsorolt személyeknek a területére való belépést vagy az azon történő átutazást, az engedélynek szigorúan a megadását indokló célra és a közvetlenül érintett személyekre kell korlátozódnia.

5. cikk

(1) Be kell fagyasztani minden olyan pénzeszközt és gazdasági erőforrást, amely az alábbiakhoz tartozik, az alábbiak tulajdonában vagy birtokában van, vagy ellenőrzése alatt áll:

a) azon természetes vagy jogi személyek, szervezetek vagy szervek, akik, illetve amelyek kibertámadás elkövetéséért vagy megkísérléséért felelősek;

b) azon természetes vagy jogi személyek, szervezetek vagy szervek, akik, illetve amelyek kibertámadások elkövetéséhez vagy megkísérléséhez pénzügyi, technikai vagy anyagi támogatást nyújtanak vagy abban más módon közreműködnek, ideértve az ilyen támadások tervezését, előkészítését, az azokban való részvételt, azok irányítását, az azokhoz való segítségnyújtást és azok ösztönzését vagy azok cselekmény vagy mulasztás révén történő megkönnyítését is;

c) az a) és b) pont hatálya alá tartozó természetes vagy jogi személyekkel, szervezetekkel vagy szervekkel kapcsolatban álló természetes vagy jogi személyek, szervezetek vagy szervek,

a mellékletben felsoroltak szerint.

(2) A mellékletben felsorolt természetes vagy jogi személyek, szervezetek és szervek részére vagy javára semmilyen pénzeszköz vagy gazdasági erőforrás sem közvetve, sem közvetlenül nem bocsátható rendelkezésre.

(3) Az (1) és a (2) bekezdéstől eltérve, az illetékes tagállamok hatóságai az általuk megfelelőnek ítélt feltételekkel engedélyezhetik egyes befagyasztott pénzeszközök vagy gazdasági erőforrások felszabadítását vagy rendelkezésre bocsátását, annak megállapítását követően, hogy az érintett pénzeszközök vagy gazdasági erőforrások:

a) a mellékletben felsorolt természetes személyek és e természetes személyek eltartott családtagjai alapvető szükségleteinek kielégítéséhez szükségesek, beleértve az élelmiszerekre, a bérleti díjra vagy jelzáloghitel-törlesztésre, a gyógyszerekre és orvosi kezelésre, az adókra, a biztosítási díjakra és a közüzemi díjakra fordított kifizetéseket is;

b) kizárólag észszerű mértékű szakmai munkadíjak vagy jogi szolgáltatások nyújtásával kapcsolatban felmerült kiadások fedezésére szolgálnak;

c) kizárólag a befagyasztott pénzeszközök vagy gazdasági erőforrások szokásos kezelési vagy fenntartási költségeinek, vagy szolgáltatási díjainak kiegyenlítésére szolgálnak;

d) rendkívüli kiadások fedezéséhez szükségesek, feltéve, hogy a releváns illetékes hatóság az engedély megadását megelőzően legalább két héttel értesítette a többi tagállam illetékes hatóságait és a Bizottságot a konkrét engedély megadásának alapjául szolgáló indokokról; vagy

e) diplomáciai vagy konzuli képviselet vagy a nemzetközi jog szerint mentességet élvező nemzetközi szervezet számlájára befizetendő vagy számlájáról kifizetendő pénzeszközök, amennyiben e be- vagy kifizetésekre az adott diplomáciai vagy konzuli képviselet vagy nemzetközi szervezet általi hivatalos felhasználás céljából kerül sor.

Az érintett tagállam tájékoztatja a többi tagállamot és a Bizottságot az e bekezdés alapján megadott engedélyekről.

(4) Az (1) bekezdéstől eltérve, a tagállamok illetékes hatóságai engedélyezhetik egyes befagyasztott pénzeszközök vagy gazdasági erőforrások felszabadítását, amennyiben teljesülnek az alábbi feltételek:

a) a pénzeszközök vagy gazdasági erőforrások az (1) bekezdésben említett természetes vagy jogi személy, szervezet vagy szerv mellékletbe történő felvételének napját megelőzően hozott választott bírósági határozat, vagy az említett időpontot megelőzően vagy azt követően az Unióban hozott bírósági vagy közigazgatási határozat, vagy az említett időpontot megelőzően vagy azt követően az érintett tagállamban végrehajtható bírósági határozat hatálya alá tartoznak;

b) a pénzeszközök vagy gazdasági erőforrások felhasználása kizárólag az ilyen határozatban foglalt, vagy az ilyen határozatban érvényesnek elismert követelések teljesítése érdekében történik, az ilyen követelésekkel rendelkező személyek jogait szabályozó törvényekben és rendeletekben meghatározott korlátokon belül;

c) a határozat nem a mellékletben felsorolt természetes vagy jogi személy, szervezet vagy szerv javát szolgálja; és

d) a határozat elismerése nem ellentétes az érintett tagállam közrendjével.

Az érintett tagállam tájékoztatja a többi tagállamot és a Bizottságot az e bekezdés alapján megadott engedélyekről.

(5) Az (1) bekezdésben foglaltak nem akadályozzák meg a mellékletben felsorolt természetes vagy jogi személyt, szervezetet vagy szervet abban, hogy az adott természetes vagy jogi személynek, szervezetnek vagy szervnek a mellékletbe való felvételét megelőzően szerződésben vállalt fizetési kötelezettségének eleget tegyen, feltéve, hogy az érintett tagállam megállapította, hogy a kifizetést – akár közvetlenül, akár közvetve – nem az (1) bekezdésben említett természetes vagy jogi személy, szervezet vagy szerv kapja.

(6) A (2) bekezdés rendelkezései nem alkalmazandók a befagyasztott számlák alábbi növekményeire:

a) kamatokra vagy e számlákkal kapcsolatos egyéb hozamokra;

b) olyan szerződések, megállapodások vagy kötelezettségek alapján esedékes kifizetésekre, amelyeket azelőtt kötöttek, vagy amelyek azt megelőzően keletkeztek, hogy az említett számlák az (1) és a (2) bekezdésben meghatározott intézkedések hatálya alá kerültek; vagy

c) az Unióban meghozott vagy az érintett tagállamban végrehajtható bírósági, közigazgatási vagy választott bírósági határozat alapján teljesítendő kifizetésekre,

feltéve, hogy az ilyen kamat, egyéb hozam és kifizetés továbbra is az (1) bekezdésben meghatározott intézkedések hatálya alá tartozik.

6. cikk

(1) A Tanács valamely tagállamnak vagy az Unió külügyi és biztonságpolitikai főképviselőjének javaslatára egyhangú határozattal létrehozza és módosítja a mellékletben foglalt jegyzéket.

(2) A Tanács közli az (1) bekezdésben említett határozatot – ideértve a jegyzékbe vétel indokolását is – az érintett természetes vagy jogi személlyel, szervezettel vagy szervvel, amennyiben a cím ismert, egyéb esetben pedig értesítés közzététele révén, lehetővé téve az adott természetes vagy jogi személy, szervezet vagy szerv számára, hogy észrevételeket tegyen.

(3) Amennyiben észrevételeket vagy új érdemi bizonyítékokat nyújtottak be, a Tanács felülvizsgálja az (1) bekezdésben említett határozatokat, és erről értesíti az érintett természetes vagy jogi személyt, szervezetet vagy szervet.

7. cikk

(1) A mellékletnek tartalmaznia kell a 4. és az 5. cikkben említett természetes és jogi személyek, szervezetek és szervek jegyzékbe vételének indokolását.

(2) A mellékletnek tartalmaznia kell az érintett természetes vagy jogi személyek, szervezetek vagy szervek azonosításához szükséges adatokat, amennyiben azok rendelkezésre állnak. Természetes személyek esetében ilyen adat lehet: a név és a névváltozatok; a születési idő és hely; az állampolgárság, az útlevél és a személyazonosító igazolvány száma; a nem; a lakcím – amennyiben ismert –; valamint a beosztás vagy a foglalkozás. Jogi személyek, szervezetek vagy szervek esetében ilyen adat lehet az elnevezés, a nyilvántartásba vétel helye és ideje, a nyilvántartásba vétel száma és a székhely.

8. cikk

Nem teljesíthetők az olyan szerződésekkel vagy ügyletekkel kapcsolatos követelések, amelyek teljesítését az e határozat alapján előírt intézkedések közvetlenül vagy közvetve, egészben vagy részben érintik, ideértve a kártalanítási vagy egyéb hasonló jellegű követeléseket, így például a kártérítési keresetet vagy a garanciaérvényesítés keretében benyújtott követelést, különösen kötvény, garancia vagy viszontgarancia – mindenekelőtt pénzügyi garancia vagy pénzügyi viszontgarancia – meghosszabbítására vagy kifizetésére irányuló bármilyen követelést, amennyiben azokat az alábbiak nyújtották be:

a) a mellékletben felsorolt, jegyzékbe vett természetes vagy jogi személyek, szervezetek vagy szervek;

b) az a) pontban említett természetes vagy jogi személyek, szervezetek vagy szervek valamelyikén keresztül, illetve nevében eljáró természetes vagy jogi személyek, szervezetek vagy szervek.

9. cikk

Az e határozatban foglalt intézkedések hatásának maximalizálása érdekében az Unió arra ösztönzi a harmadik államokat, hogy fogadjanak el az ebben a határozatban megállapítottakhoz hasonló korlátozó intézkedéseket.

10. cikk

Ezt a határozatot … [egy évvel ezen határozat hatálybalépésének napját követően]-ig kell alkalmazni, és folyamatosan felül kell vizsgálni. Ha a Tanács úgy ítéli meg, hogy e határozat céljai nem valósultak meg, a határozatot meg kell újítani vagy adott esetben módosítani kell.

11. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetését követő napon lép hatályba.

Kelt …, …

a Tanács részéről
az elnök

MELLÉKLET

A 4. és az 5. cikkben említett természetes és jogi személyek, szervezetek és szervek jegyzéke

[…]