Ez a dokumentum kizárólag tájékoztató jellegű és nem vált ki joghatást. Az EU intézményei semmiféle felelősséget nem vállalnak a tartalmáért. A jogi aktusoknak – ideértve azok bevezető hivatkozásait és preambulumbekezdéseit is – az Európai Unió Hivatalos Lapjában közzétett és az EUR-Lex portálon megtalálható változatai tekintendők hitelesnek. Az említett hivatalos szövegváltozatok közvetlenül elérhetők az ebben a dokumentumban elhelyezett linkeken keresztül

►B

A TANÁCS (EU) 2019/796 RENDELETE

(2019. május 17.)

az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

(HL L 129I., 2019.5.17., 1. o.)

Módosította:

		Hivatalos Lap		
		Szám	Oldal	Dátum
►M1	A Tanács (EU) 2020/1125 végrehajtási rendelete (2020. július 30.)	L 246	4	2020.7.30.
►M2	A Tanács (EU) 2020/1536 végrehajtási rendelete (2020. október 22.)	L 351 I	1	2020.10.22.
►M3	A Tanács (EU) 2020/1744 végrehajtási rendelete (2020. november 20.)	L 393	1	2020.11.23.
►M4	A Bizottság (EU) 2022/595 végrehajtási rendelete (2022. április 11.)	L 114	60	2022.4.12.

Helyesbítette:

►C1 Helyesbítés, HL L 230., 2020.7.17., 37. o. (2019/796)

▼B

A TANÁCS (EU) 2019/796 RENDELETE

(2019. május 17.)

az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről

1. cikk

(1) Ezt rendeletet 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 rendszerhez való hozzáférés;

b) információs rendszereket érintő 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 az alábbi 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 ágazat terén;

▼B

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 Unió működéséről szóló szerződés 21. cikkének vonatkozó rendelkezéseiben foglalt KBVP célok eléréséhez szükségesnek ítélik, a jelentős hatású kibertámadásokra válaszul e rendelet alapján korlátozó intézkedéseket lehet alkalmazni harmadik államokkal vagy nemzetközi szervezetekkel szemben is.

(7) E rendelet 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”: információs rendszer működésének akadályozása vagy megszakítása digitális adatok bevitelével, továbbításával, károsításával, törlésével, rongálásával, megváltoztatásával, eltávolításával vagy hozzáférhetetlenné tételével;

c) „adatokat érintő beavatkozás”: információs rendszerekben található digitális adatok törlése, károsítása, rongálása, megváltoztatása, eltávolítása vagy hozzáférhetetlenné tétele. A fogalom emellett magában foglalja 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;

8. E rendelet alkalmazásában a következő kiegészítő fogalommeghatározásokat kell alkalmazni:

a) „követelés”: bármely, az e rendelet hatálybalépését megelőzően vagy azt követően szerződés vagy ügylet alapján vagy ahhoz kapcsolódóan keletkezett követelés, akár érvényesítik bírósági eljárásban, akár nem, és különösen a következők:

   i. szerződés vagy ügylet alapján vagy ezekhez kapcsolódóan felmerülő kötelezettség teljesítése iránti követelés;

   ii. bármilyen formájú kötvény, pénzügyi garancia vagy viszontgarancia meghosszabbítása vagy kifizetése iránti követelés;

   iii. a szerződéssel vagy ügylettel összefüggő kártérítési kereset;

   iv. ellenkövetelés;

▼B

v. bárhol meghozott ítélet, választott bírósági ítélet vagy ezzel egyenértékű határozat elismerése vagy végrehajtása iránti követelés, beleértve a külföldön hozott határozat belföldön történő érvényesítését is;

b) „szerződés vagy ügylet”: bármely ügylet bármilyen alakban, bármilyen alkalmazandó jog vonatkozik rá, függetlenül attól, hogy egy vagy több szerződést vagy hasonló kötelezettségeket foglal-e magában ugyanazon vagy különböző felek között; e célból a „szerződés” magában foglal minden kötvényt, garanciát vagy viszontgaranciát, különösen a pénzügyi garanciát vagy a pénzügyi viszontgaranciát, minden jogilag független és nem független hitelt, és bármely olyan kapcsolódó megállapodást, amely az ügyletből származik vagy azzal kapcsolatos;

c) „illetékes hatóságok”: a tagállamoknak a II. mellékletben felsorolt honlapokon feltüntetett illetékes hatóságai;

d) „gazdasági erőforrások”: mindenféle – tárgyi vagy immateriális, ingó vagy ingatlan – vagyoni eszköz, amely nem pénzeszköz, de felhasználható pénzeszközök, áruk vagy szolgáltatások megszerzésére;

e) „gazdasági erőforrások befagyasztása”: annak megakadályozása, hogy a gazdasági erőforrásokat bármilyen módon pénzeszközök, áruk vagy szolgáltatások megszerzésére használják fel, beleértve – de nem kizárólag – azok eladását, bérbeadását vagy jelzáloggal való megterhelését is;

f) „pénzeszközök befagyasztása”: a pénzeszközök bármilyen mozgásának, átutalásának, módosításának, felhasználásának, az azokhoz való hozzáférésnek, illetve bármiféle olyan kezelésének a megakadályozása, amely bármilyen változást eredményezne a pénzeszközök mennyisége, összege, elhelyezkedése, tulajdonlása, birtoklása, jellege, rendeltetése tekintetében, vagy más olyan változást okozna, amely lehetővé tenné a pénzeszközök felhasználását, ideértve a portfóliókezelést is;

g) „pénzeszközök”: bármilyen pénzügyi eszköz és gazdasági előny, beleértve – de nem kizárólag – a következőket is:

i. készpénz, csekk, pénzkövetelés, váltó, fizetési megbízás és egyéb fizetési eszközök;

ii. pénzügyi intézményeknél vagy egyéb szervezeteknél elhelyezett betétek, számlaegyenlegek, követelések és adóskötelezvények;

iii. nyilvánosan vagy zárt körben forgalmazott értékpapírok és hitelviszonyt megtestesítő instrumentumok, beleértve a részvényeket, az értékpapírokat megtestesítő igazolásokat, a kötvényeket, a váltókat, az opciós utalványokat, a fedezetlen kötvényeket és a származtatott ügyleteket;

iv. kamatok, osztalékok, vagy vagyoni eszközökből származó vagy azok által képzett jövedelem vagy értéktöbblet;

v. hitelek, beszámítási jogok, garanciák, teljesítési biztosítékok vagy egyéb pénzügyi kötelezettségvállalások;

vi. hitellevelek, fuvarlevelek, adásvételi szerződések; és

vii. pénzeszközökben vagy pénzügyi forrásokban fennálló érdekeltséget bizonyító okiratok;

▼B

h) „az Unió területe”: a tagállamok területét magában foglaló terület, amelyre a Szerződés az abban meghatározott feltételekkel alkalmazandó, beleértve a légterüket is.

2. cikk

Annak megállapításához, hogy egy kibertámadás az 1. cikk (1) bekezdésének a) pontjában említett jelentős hatással bír-e, többek között a következő tényezők vehetők figyelembe:

a) az előidézett zavar hatóköre, léptéke, hatása és súlyossága, ideértve a gazdasági és társadalmi tevékenységeket, az alapvető szolgáltatásokat, a kritikus állami funkciókat, a közrendet és a közbiztonságot is;

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

c) az érintett tagállamok száma;

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

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.

3. cikk

(1) Az I. mellékletben felsorolt természetes vagy jogi személyekhez, szervezetekhez vagy szervekhez tartozó, tulajdonukban álló, birtokukban lévő vagy ellenőrzésük alatt álló minden pénzeszközt és gazdasági erőforrást be kell fagyasztani.

(2) Nem bocsátható rendelkezésre – sem közvetlenül, sem közvetve – semmilyen pénzeszköz vagy gazdasági erőforrás az I. mellékletben felsorolt természetes vagy jogi személyek, szervezetek vagy szervek részére, illetve javára.

(3) Az I. mellékletbe – a Tanács által a (KKBP) 2019/797 tanácsi határozat 5. cikkének (1) bekezdésével összhangban megállapítottaknak megfelelően – fel kell venni:

a) azokat a természetes és jogi személyeket, szervezeteket és szerveket, akik, illetve amelyek kibertámadás elkövetéséért vagy megkísérléséért felelősek;

b) azokat a természetes vagy jogi személyeket, szervezeteket és szerveket, akik, illetve amelyek kibertámadás elkövetéséhez vagy megkísérléséhez pénzügyi, technikai vagy anyagi támogatást nyújtanak vagy abban más módon közreműködnek, többek között ilyen támadások tervezésével, előkészítésével, irányításával, segítésével, bátorításával vagy az ilyen támadásokban való részvétellel vagy az ilyen támadásoknak cselekménnyel vagy mulasztással történő elősegítésével;

c) az e bekezdés a) és b) pontjának hatálya alá tartozó természetes vagy jogi személyekkel, szervezetekkel vagy szervekkel kapcsolatban álló természetes vagy jogi személyeket, szervezeteket vagy szerveket.

▼B

4. cikk

(1) A 3. cikktől eltérve, a tagállamok illetékes 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) ►C1 az I. mellékletben felsorolt természetes vagy jogi személyek, szervezetek vagy szervek, valamint az ilyen 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;

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 díjainak, valamint szolgáltatási díjainak kiegyenlítésére szolgálnak;

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

e) diplomáciai vagy konzuli képviselet vagy a nemzetközi jog szerint mentességet élvező nemzetközi szervezetek 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.

(2) Az érintett tagállam az (1) bekezdés alapján megadott valamennyi engedélyről két héten belül tájékoztatja a többi tagállamot és a Bizottságot.

5. cikk

(1) A 3. cikk (1) bekezdésétől eltérve, a tagállamok illetékes hatóságai engedélyezhetik egyes befagyasztott pénzeszközök vagy gazdasági erőforrások felszabadítását, amennyiben teljesülnek az alábbi feltételek:

(a) a pénzeszközök vagy gazdasági erőforrások a 3. cikkben felsorolt természetes vagy jogi személy, szervezet vagy szerv I. 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 végrehajtandó 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 az I. mellékletben felsorolt természetes vagy jogi személy, szervezet vagy szerv javát szolgálja; és

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

▼B

(2) Az érintett tagállam az (1) bekezdés alapján megadott valamennyi engedélyről két héten belül tájékoztatja a többi tagállamot és a Bizottságot.

6. cikk

(1) A 3. cikk (1) bekezdésétől eltérve, és feltéve, hogy egy, az I. mellékletben felsorolt valamely természetes vagy jogi személy, szervezet vagy szerv általi kifizetés az adott természetes vagy jogi személy, szervezet vagy szerv által kötött olyan szerződés vagy megállapodás, illetve az adott természetes vagy jogi személy, szervezet vagy szerv tekintetében létrejött olyan kötelezettség alapján esedékes, amelyet az adott természetes vagy jogi személy, szervezet vagy szerv I. mellékletbe történő felvétele előtt kötöttek meg, illetve amely ezen időpont előtt keletkezett, a tagállamok illetékes hatóságai az általuk megfelelőnek tartott feltételekkel engedélyezhetik egyes befagyasztott pénzeszközök vagy gazdasági erőforrások felszabadítását, feltéve, hogy az érintett illetékes hatóság megállapította az alábbiakat:

a) a pénzeszközöket vagy gazdasági erőforrásokat az I. mellékletben felsorolt valamely természetes vagy jogi személy, szervezet vagy szerv általi kifizetésre használják fel; és

b) a kifizetés nem sérti a 3. cikk (2) bekezdését.

(2) Az érintett tagállam az (1) bekezdés alapján megadott valamennyi engedélyről két héten belül tájékoztatja a többi tagállamot és a Bizottságot.

7. cikk

(1) A 3. cikk (2) bekezdése nem zárja ki, hogy a pénzügyi intézmények vagy hitelintézetek a harmadik felek által a jegyzékben szereplő természetes vagy jogi személy, szervezet vagy szerv számlájára átutalt pénzeszközöket a befagyasztott számlán jóváírják, feltéve, hogy az ilyen számlákon jelentkező növekmények befagyasztására is sor kerül. Ezekről az ügyletekről a pénzügyi intézmény vagy hitelintézet köteles haladéktalanul tájékoztatni az illetékes hatóságot.

(2) A 3. cikk (2) bekezdése nem alkalmazandó a befagyasztott számlák alábbi növekményeire:

a) kamatok vagy e számlákkal kapcsolatos egyéb hozamok;

b) olyan szerződések, megállapodások vagy kötelezettségek alapján esedékes kifizetések, amelyeket azt megelőzően kötöttek, vagy amelyek azt megelőzően keletkeztek, hogy a 3. cikk (1) bekezdésében említett természetes vagy jogi személyt, szervezetet vagy szervet felvették az I. mellékletbe; vagy

c) valamely tagállamban hozott, illetve az érintett tagállamban végrehajtható bírósági, közigazgatási vagy választott bírósági határozat alapján teljesítendő kifizetések;

feltéve, hogy az ilyen kamat, egyéb hozam és kifizetés továbbra is a 3. cikk (1) bekezdésében előírt intézkedések hatálya alá tartozik.

8. cikk

(1) A tájékoztatásra, a titoktartásra és a szakmai titoktartásra vonatkozó alkalmazandó szabályok sérelme nélkül a természetes és jogi személyek, szervezetek és szervek:

▼B

a) haladéktalanul az állandó lakóhelyük vagy székhelyük szerinti tagállam illetékes hatóságának rendelkezésére bocsátják azokat az információkat – például a 3. cikk (1) bekezdésével összhangban befagyasztott számlákkal és összegekkel kapcsolatos információkat – amelyek elősegíthetik az e rendeletnek való megfelelést, és az ilyen információkat közvetlenül vagy a tagállam útján továbbítják a Bizottsághoz; és

b) együttműködnek az illetékes hatósággal az a) pontban említett információk ellenőrzése során.

(2) A Bizottság minden, hozzá közvetlenül beérkezett további információt a tagállamok rendelkezésére bocsát.

(3) Az e cikkel összhangban nyújtott vagy kapott bármely információ kizárólag arra a célra használható fel, amelyre azt adták vagy kapták.

9. cikk

Tilos tudatosan és szándékosan részt venni olyan tevékenységben, amelynek célja vagy hatása a 3. cikkben említett intézkedések kijátszása.

10. cikk

(1) A pénzeszközök vagy gazdasági erőforrások befagyasztása, illetve a pénzeszközök vagy gazdasági erőforrások rendelkezésre bocsátásának megtagadása – amennyiben e döntést jóhiszeműen hozták, abban a meggyőződésben, hogy az intézkedés e rendelettel összhangban áll – nem vonja maga után az azt végrehajtó természetes vagy jogi személy, szervezet vagy szerv, illetve ezek igazgatói vagy alkalmazottai felelősségét, kivéve, ha bizonyítást nyer, hogy a pénzeszközök vagy gazdasági erőforrások befagyasztása vagy visszatartása gondatlanság eredménye.

(2) A természetes vagy jogi személyek, szervezetek vagy szervek által végrehajtott intézkedések semmilyen formában nem vonják maguk után e természetes vagy jogi személyek, szervezetek vagy szervek felelősségét, amennyiben azok nem tudták vagy nem volt észszerű okuk feltételezni, hogy intézkedésükkel megsértik az e rendeletben foglalt intézkedéseket.

11. cikk

(1) Nem teljesíthetők az olyan szerződésekkel vagy ügyletekkel kapcsolatos, bármilyen formájú követelések, amelyek teljesítését az e rendelet alapján előírt intézkedések közvetlenül vagy közvetve, egészben vagy részben érintik, ideértve a kártalanítás iránti vagy egyéb hasonló jellegű követeléseket, különösen a kártérítési keresetet vagy a garanciaérvényesítés keretében benyújtott követelést, azaz kötvény, garancia vagy viszontgarancia – különösen pénzügyi garancia vagy pénzügyi viszontgarancia – kifizetésére vagy meghosszabbítására irányuló bármilyen követelést, amennyiben azokat az alábbiak nyújtották be:

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

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

(2) Követelés érvényesítésére irányuló bármilyen eljárás során a követelést érvényesíteni kívánó természetes vagy jogi személyre, szervezetre vagy szervre hárul a bizonyítás terhe arra vonatkozóan, hogy az (1) bekezdés nem tiltja az adott követelés teljesítését.

(3) Ez a cikk nem érinti az (1) bekezdésben említett természetes vagy jogi személyeknek, szervezeteknek és szerveknek a szerződéses kötelezettségek teljesítése elmulasztásának jogszerűségével kapcsolatos bírósági felülvizsgálathoz való jogát, e rendelettel összhangban.

▼B

12. cikk

(1) A Bizottság és a tagállamok tájékoztatják egymást az e rendelet alapján hozott intézkedésekről, valamint megosztják egymással az e rendelettel kapcsolatban rendelkezésükre álló bármely egyéb lényeges információt, különösen az alábbiakkal kapcsolatban:

a) a 3. cikk alapján befagyasztott pénzeszközök, valamint a 4., az 5. és a 6. cikk értelmében megadott engedélyek;

b) a jogsértési és a végrehajtási problémák, valamint a nemzeti bíróságok által hozott ítéletek.

(2) A tagállamok haladéktalanul tájékoztatják egymást és a Bizottságot bármely egyéb olyan rendelkezésükre álló vonatkozó információról, amely érintheti e rendelet eredményes végrehajtását.

13. cikk

(1) Amennyiben a Tanács úgy határoz, hogy valamely természetes vagy jogi személyt, szervezetet vagy szervet a 3. cikkben említett intézkedések hatálya alá von, ennek megfelelően módosítja az I. mellékletet.

(2) A Tanács közli az (1) bekezdésben említett határozatát – ideértve a jegyzékbe vétel indokolását is – az adott természetes vagy jogi személyekkel, szervezetekkel vagy szervekkel, amennyiben a cím ismert közvetlenül, vagy értesítés közzététele útján, lehetővé téve, hogy az adott természetes vagy jogi személy, szervezet vagy szerv észrevételeket nyújtson be.

(3) Amennyiben észrevétel vagy új érdemi bizonyíték benyújtására kerül sor, a Tanács felülvizsgálja az (1) bekezdésben említett határozatát, és erről értesíti az adott természetes vagy jogi személyt, szervezetet vagy szervet.

(4) Az I. mellékletben foglalt jegyzéket rendszeres időközönként és legalább 12 havonta felül kell vizsgálni.

(5) A Bizottság felhatalmazást kap arra, hogy a tagállamok által szolgáltatott információk alapján módosítsa a II. mellékletet.

14. cikk

(1) Az I. melléklet tartalmazza az érintett természetes vagy jogi személyek, szervezetek vagy szervek jegyzékbe vételének okait.

(2) Az I. melléklet tartalmazza, amennyiben rendelkezésre áll, az érintett természetes vagy jogi személyek, szervezetek vagy szervek azonosításához szükséges, rendelkezésre álló információkat. Természetes személyek esetében ilyen információ 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. A Jogi személyek, szervezetek vagy szervek esetében ilyen információ lehet az elnevezés, a bejegyzés helye és ideje, a bejegyzés száma és a székhely.

15. cikk

(1) A tagállamok megállapítják az e rendelet rendelkezéseinek megsértése esetén alkalmazandó szankciókra vonatkozó szabályokat, és minden szükséges intézkedést megtesznek azok végrehajtása érdekében. Az előírt szankcióknak hatékonyaknak, arányosaknak és visszatartó erejűeknek kell lenniük.

▼B

(2) A tagállamok e rendelet hatálybalépését követően haladéktalanul értesítik a Bizottságot az (1) bekezdésben említett szabályokról, majd azok későbbi módosításairól.

16. cikk

(1) A Bizottság az e rendelet alapján ráruházott feladatainak elvégzése érdekében személyes adatokat kezel. E feladatok magukban foglalják a következőket:

a) az I. melléklet tartalmának belefoglalása az uniós pénzügyi szankciókkal sújtott személyeket, csoportokat és szervezeteket felsoroló, egységes szerkezetbe foglalt, nyilvánosan elérhető elektronikus jegyzékbe és a szintén nyilvánosan elérhető interaktív szankciótérképbe;

b) az e rendelettel összhangban bevezetett intézkedések hatásával kapcsolatos információk – például a befagyasztott pénzeszközök értéke és az illetékes hatóságok által megadott engedélyekre vonatkozó információk – kezelése.

(2) E rendelet alkalmazásában a Bizottság tekintetében az (EU) 2018/1725 rendelet 3. cikkének 8. pontja értelmében vett „adatkezelőként” a II. mellékletben felsorolt szolgálat kerül kijelölésre, annak érdekében, hogy az érintett természetes személyek számára biztosítva legyen az említett rendelet szerinti jogaik gyakorlása.

17. cikk

(1) A tagállamok kijelölik az e rendeletben említett illetékes hatóságokat, és feltüntetik őket a II. mellékletben felsorolt honlapokon. A tagállamok a II. mellékletben felsorolt internetes honlapjaik címének megváltozásáról értesítik a Bizottságot.

(2) A tagállamok e rendelet hatálybalépését követően haladéktalanul értesítik a Bizottságot illetékes hatóságaikról – ideértve az említett hatóságok elérhetőségét is –, valamint értesítik a Bizottságot minden későbbi változásról.

(3) Azokban az esetekben, amikor e rendelet a Bizottság értesítésére, tájékoztatására vagy a vele történő egyéb kapcsolattartásra vonatkozó kötelezettséget ír elő, az ilyen kommunikáció során a II. mellékletben feltüntetetett címet és egyéb elérhetőségeket kell használni.

18. cikk

Ezt a rendeletet alkalmazni kell:

a) az Unió területén belül, ideértve annak légterét is;

b) a valamely tagállam joghatósága alá tartozó bármely légi vagy vízi jármű fedélzetén;

c) az Unió területén belül vagy kívül tartózkodó bármely természetes személyre, aki valamely tagállam állampolgára;

d) bármely tagállam joga szerint bejegyzett vagy létrehozott jogi személyre, szervezetre vagy szervre az Unió területén belül vagy azon kívül;

e) a teljes egészében vagy részben az Unión belül üzleti tevékenységet folytató bármely jogi személyre, szervezetre vagy szervre.

▼B

19. cikk

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

Ez a rendelet teljes egészében kötelező és közvetlenül alkalmazandó valamennyi tagállamban.

▼B

I. MELLÉKLET

A 3. cikkben meghatározott természetes és jogi személyek, szervezetek és szervek jegyzéke

▼M1

A. Természetes személyek

	Név:	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
▼M3				
1.	GAO Qiang	Születési idő: 1983. október 4. Születési hely: Shandong Province, China Cím: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Állampolgárság: kínai Nem: férfi	Gao Qiang részt vesz a „Cloud Hopper” műveletben, amely az Unión kívülről indított, olyan jelentős hatású kibertámadások sorozata, amelyek külső fenyegetést jelentenek az Unióra vagy annak tagállamaira nézve, valamint jelentős negatív hatással vannak harmadik államokra. A „Cloud Hopper” művelet elkövetői hat kontinensen intéztek támadásokat multinacionális vállalatok – köztük az Unió területén működő vállalatok – információs rendszerei ellen, továbbá engedély nélkül fértek hozzá érzékeny kereskedelmi adatokhoz, ami jelentős gazdasági veszteséget okozott. A „Cloud Hopper” műveletet az „APT10” („10. sz. magas szintű állandó fenyegetés”, „Advance Persistent Threat 10”) (más néven: „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” és „Potassium”) néven ismert csoport hajtotta végre. Gao Qiang kapcsolatba hozható az APT10 csoporttal, többek között az APT10 parancsnoki és irányítási infrastruktúrával fennálló kapcsolata miatt. Ezenfelül a Huaying Haitai, amely egy a „Cloud Hopper” művelet támogatása és működésének elősegítése miatt jegyzékbe vett szervezet, alkalmazásba vette Gao Qiangot. Gao Qiang kapcsolatban áll Zhang Shilonggal, akit szintén a „Cloud Hopper” művelettel összefüggésben vettek jegyzékbe. Gao Qiang ennélfogva kapcsolatban áll mind a Huaying Haitai nevű szervezettel, mind Zhang Shilonggal.	2020.7.30.
2.	ZHANG Shilong	Születési idő: 1981. szeptember 10. Születési hely: China Cím: Hedong, Yuyang Road No 121, Tianjin, China Állampolgárság: kínai Nem: férfi	Zhang Shilong részt vesz a „Cloud Hopper” műveletben, amely az Unión kívülről indított, olyan jelentős hatású kibertámadások sorozata, amelyek külső fenyegetést jelentenek az Unióra vagy annak tagállamaira nézve, valamint jelentős negatív hatással vannak harmadik államokra. A „Cloud Hopper” művelet elkövetői hat kontinensen intéztek támadásokat multinacionális vállalatok – köztük az Unió területén működő vállalatok – információs rendszerei ellen, továbbá engedély nélkül fértek hozzá érzékeny kereskedelmi adatokhoz, ami jelentős gazdasági veszteséget okozott.	2020.7.30.

▼M3

	Név:	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
			A „Cloud Hopper” műveletet az „APT10” („10. sz. magas szintű állandó fenyegetés”, „Advance Persistent Threat 10”) (más néven: „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” és „Potassium”) néven ismert csoport hajtotta végre. Zhang Shilong kapcsolatba hozható az APT10 csoporttal, többek között az APT10 kibertámadásaihoz általa kifejlesztett és tesztelt rosszindulatú szoftver révén. Ezenfelül a Huaying Haitai, amely egy a „Cloud Hopper” művelet támogatása és működésének elősegítése miatt jegyzékbe vett szervezet, alkalmazásba vette Zhang Shilongot. Zhang Shilong kapcsolatban áll Gao Qianggal, akit szintén a „Cloud Hopper” művelettel összefüggésben vettek jegyzékbe. Zhang Shilong ennélfogva kapcsolatban áll mind a Huaying Haitai nevű szervezettel, mind Gao Qianggal.	

▼M1

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Születési idő: 1972.5.27. Születési hely: Perm Oblast, Russian SFSR (now Russian Federation) Útlevélszám: 120017582, kibocsátó: az Orosz Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation), érvényes: 2017.4.17. – 2022.4.17. Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Alexey Minin részt vett egy potenciálisan jelentős hatású kibertámadási kísérletben, amely a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányult. Az Orosz Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GU/GRU) humán felderítési támogató tisztviselőjeként Alexey Minin egy négy orosz katonai hírszerzési tisztviselőből álló csoport tagja volt, akik 2018 áprilisában Hágában (Hollandia) megpróbáltak engedély nélkül hozzáférni az OPCW Wi-Fi-hálózatához. A kibertámadási kísérlet célja az volt, hogy feltörje az OPCW Wi-Fi-hálózatát, ami – sikere esetén – veszélybe sodorta volna a hálózat biztonságát és az OPCW folyamatban lévő vizsgálati munkáját. A Holland Védelmi Hírszerzési és Biztonsági Szolgálat (Netherlands Defence Intelligence and Security Service, DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt.	2020.7.30.
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Születési idő: 1977.7.31. Születési hely: Murmanskaya Oblast, Russian SFSR (jelenleg: Russian Federation) Útlevélszám: 100135556, kibocsátó: az Orosz Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation), érvényes: 2017.4.17. – 2022.4.17. Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Aleksei Morenets részt vett egy potenciálisan jelentős hatású kibertámadási kísérletben, amely a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányult. Az Orosz Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GU/GRU) számítástechnikai operátoraként Aleksei Morenets egy négy orosz katonai hírszerzési tisztviselőből álló csoport tagja volt, akik 2018 áprilisában Hágában (Hollandia) megpróbáltak engedély nélkül hozzáférni az OPCW Wi-Fi-hálózatához. A kibertámadási kísérlet célja az volt, hogy feltörje az OPCW Wi-Fi-hálózatát, ami – sikere esetén – veszélybe sodorta volna a hálózat biztonságát és az OPCW folyamatban lévő vizsgálati munkáját. A Holland Védelmi Hírszerzési és Biztonsági Szolgálat (Netherlands Defence Intelligence and Security Service, DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt.	2020.7.30.

▼M1

	Név:	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Születési idő: 1981.7.26. Születési hely: Kursk, Russian SFSR (jelenleg: Russian Federation) Útlevélszám: 100135555, kibocsátó: az Orosz Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation), érvényes: 2017.4.17. – 2022.4.17. Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Evgenii Serebriakov részt vett egy potenciálisan jelentős hatású kibertámadási kísérletben, amely a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányult. Az Orosz Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GU/GRU) számítástechnikai operátoraként Evgenii Serebriakov egy négy orosz katonai hírszerzési tisztviselőből álló csoport tagja volt, akik 2018 áprilisában Hágában (Hollandia) megpróbáltak engedély nélkül hozzáférni az OPCW Wi-Fi-hálózatához. A kibertámadási kísérlet célja az volt, hogy feltörje az OPCW Wi-Fi-hálózatát, ami – sikere esetén – veszélybe sodorta volna a hálózat biztonságát és az OPCW folyamatban lévő vizsgálati munkáját. A Holland Védelmi Hírszerzési és Biztonsági Szolgálat (Netherlands Defence Intelligence and Security Service, DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt.	2020.7.30.
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Születési idő: 1972.8.24. Születési hely: Ulyanovsk, Russian SFSR (jelenleg: Russian Federation) Útlevélszám: 120018866, kibocsátó: az Orosz Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation), érvényes: 2017.4.17. – 2022.4.17. Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Oleg Sotnikov részt vett egy potenciálisan jelentős hatású kibertámadási kísérletben, amely a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányult. Az Orosz Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation, GU/GRU) humán felderítési támogató tisztviselőjeként Oleg Sotnikov egy négy orosz katonai hírszerzési tisztviselőből álló csoport tagja volt, akik 2018 áprilisában Hágában (Hollandia) megpróbáltak engedély nélkül hozzáférni az OPCW Wi-Fi-hálózatához. A kibertámadási kísérlet célja az volt, hogy feltörje az OPCW Wi-Fi-hálózatát, ami – sikere esetén – veszélybe sodorta volna a hálózat biztonságát és az OPCW folyamatban lévő vizsgálati munkáját. A Holland Védelmi Hírszerzési és Biztonsági Szolgálat (Netherlands Defence Intelligence and Security Service, DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt.	2020.7.30.

▼M1

	Név:	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
▼M2				
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Születési idő: 1990. november 15. Születési hely: Kursk, Russian SFSR (jelenleg: Russian Federation) Állampolgárság: orosz Nem: férfi	Dmitry Badin részt vett a német szövetségi parlament (Deutscher Bundestag) elleni, jelentős hatást gyakorló kibertámadásban. Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának 85. Különleges Szolgálati Főközpontja (85th Main Centre of Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)) katonai hírszerző tisztjeként Dmitry Badin tagja volt annak az orosz katonai hírszerző tiszti csapatnak, amely 2015 áprilisában és májusában kibertámadást intézett a német szövetségi parlament (Deutscher Bundestag) ellen. A kibertámadás a parlament informatikai rendszere ellen irányult, és annak működését több napra megzavarta. Jelentős mennyiségű adatot tulajdonítottak el, és a támadás több képviselő, valamint Angela Merkel kancellár e-mail-fiókját is érintette.	2020.10.22.
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Születési idő: 1961. február 21. Állampolgárság: orosz Nem: férfi	Igor Kostyukov az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)) jelenlegi vezetője, korábbi első helyettes vezetője. Parancsnoksága alá tartozik többek között a 85. Különleges Szolgálati Főközpont (85th Main Centre of Special Services (GTsSS)), más néven „26165-ös katonai egység” (egyéb használt elnevezések: „APT28”, „Fancy Bear”, „Sofacy Group”, „Pawn Storm” és „Strontium”). Igor Kostyukov e minőségében felelős a GTsSS által végrehajtott kibertámadásokért, köztük azokért, amelyek az Unióra vagy tagállamaira nézve külső fenyegetést jelentő, jelentős hatásúak voltak. Konkrétan, a 85. Különleges Szolgálati Főközpont katonai hírszerző tisztjei részt vettek a 2015 áprilisában és májusában a német szövetségi parlament (Deutscher Bundestag) ellen intézett kibertámadásban, valamint 2018 áprilisában Hollandiában a Vegyifegyvertilalmi Szervezet (OPCW) wifi-hálózatába való betörésre irányuló kibertámadási kísérletben. A német szövetségi parlament elleni kibertámadás a parlament informatikai rendszere ellen irányult, és annak működését több napra megzavarta. Jelentős mennyiségű adatot tulajdonítottak el, és a támadás több képviselő, valamint Angela Merkel kancellár e-mail-fiókját is érintette.	2020.10.22.

▼M1

B. Jogi személyek, szervezetek vagy szervek

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	más néven: Haitai Technology Development Co. Ltd Elhelyezkedés: Tianjin, China	A Huaying Haitai pénzügyi, technikai vagy anyagi szempontból támogatta és elősegítette a „Cloud Hopper” műveletet, amely jelentős hatású, az Unión kívülről indított és az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentő, valamint harmadik államokra jelentős negatív hatást gyakorló kibertámadások sorozata. A „Cloud Hopper” művelet keretében hat kontinensen intéztek támadásokat multinacionális vállalatok – köztük az Unió területén működő vállalatok – információs rendszerei ellen, továbbá engedély nélkül fértek hozzá érzékeny kereskedelmi adatokhoz, ami jelentős gazdasági veszteséget okozott. A „Cloud Hopper” műveletet az „APT10” („10. sz. magas szintű állandó fenyegetés”, „Advance Persistent Threat 10”) (más néven: „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass”és „Potassium”) néven ismert csoport hajtja végre. A Huaying Haitai kapcsolatba hozható az APT10 csoporttal. Ezenfelül a Huaying Haitai alkalmazásba vette Gao Qiangot és Zhang Shilongot, akiket a „Cloud Hopper” művelettel összefüggésben vettek jegyzékbe. A Huaying Haitai ennélfogva kapcsolatban áll mind Gao Qianggal, mind Zhang Shilonggal.	2020.7.30.
2.	Chosun Expo	Chosen Expo; Korea Export Joint Venture Elhelyezkedés: KNDK	A Chosun Expo pénzügyi, technikai vagy anyagi szempontból támogatta és elősegítette egy jelentős hatású, az Unión kívülről indított és az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentő, valamint harmadik államokra jelentős negatív hatást gyakorló kibertámadások sorozatát, többek között a „WannaCry” néven ismertté vált kibertámadásokat vagy a Lengyel Pénzügyi Felügyeleti Hatóság (Polish Financial Supervision Authority) és a Sony Pictures Entertainment elleni kibertámadásokat, valamint a Bangladesh Bankból történt számítógépes lopásokat és a vietnámi Tien Phong Bank elleni számítógépes lopás kísérletét. A „WannaCry” világszerte megzavarta az információs rendszereket azáltal, hogy zsarolóvírussal célozta meg ezeket a rendszereket, és blokkolta az adatokhoz való hozzáférést. Érintette az uniós vállalatok információs rendszereit, beleértve a tagállamokon belüli alapvető szolgáltatások és gazdasági tevékenységek fenntartásához szükséges szolgáltatásokkal kapcsolatos információs rendszereket is.	2020.7.30.

▼M1

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
			A „WannaCry” végrehajtója az „APT38” („38. sz. magas szintű állandó fenyegetés”, „Advanced persistent Threat 38”) néven ismertté vált csoport vagy a Lazarus csoport volt. A Chosun Expo többek között a kibertámadásokhoz használt fiókok révén hozható kapcsolatba az APT38 csoporttal és a Lazarus csoporttal.	
3.	Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának Különleges Technológiai Főközpontja (Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU))	Cím: 22 Kirova Street, Moscow, Russian Federation	Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának Különleges Technológiai Főközpontja, amely a 74455 katonai azonosító FPN-számon is ismert, felelős az Unión kívülről indított és az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentő, valamint harmadik államokra jelentős negatív hatást gyakorló olyan kibertámadásokért, amelyek közé tartozik például a „NotPetya” vagy „EternalPetya” (2017. június), valamint a 2015–2016 telén az ukrán energiahálózat ellen intézett kibertámadások. A „NotPetya” vagy „EternalPetya” az Unióban, Európa egészében és világszerte számos vállalatnál tette hozzáférhetetlenné az adatokat azáltal, hogy zsarolóvírussal támadta meg a számítógépeket, és blokkolta az adatokhoz való hozzáférést, ami többek között jelentős gazdasági veszteséget okozott. Az ukrán energiahálózatot érintő kibertámadás következtében a hálózat egyes részeinek működése leállt a tél folyamán.	2020.7.30.
			A „Sandworm” (más néven „Sandworm Team”, „BlackEnergy Group”, „Voodoo Bear”, „Quedagh”, „Olympic Destroyer” és „Telebots”) csoport néven ismert szervezet, amely az ukrán energiahálózat elleni kibertámadás mögött is állt, hajtotta végre a „NotPetya” vagy „EternalPetya” támadást. Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának Különleges Technológiai Főközpontja tevékeny szerepet játszik a Sandworm kibertevékenységeiben, és kapcsolatba hozható a Sandworm csoporttal.	

▼M1

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
▼M2				
4.	Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának 85. Különleges Szolgálati Főközpontja (85th Main Centre of Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU))	Cím: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának 85. Különleges Szolgálati Főközpontja (85th Main Centre of Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)), más néven „26165-ös katonai egység" (egyéb használt elnevezések: „APT28", „Fancy Bear", „Sofacy Group", „Pawn Storm" és „Strontium") felelős olyan kibertámadásokért, amelyek az Unióra vagy tagállamaira nézve külső fenyegetést jelentő, jelentős hatásúak voltak. Konkrétan, a GTsSS katonai hírszerző tisztjei részt vettek a 2015 áprilisában és májusában a német szövetségi parlament (Deutscher Bundestag) ellen intézett kibertámadásban, valamint 2018 áprilisában Hollandiában a Vegyifegyvertilalmi Szervezet (OPCW) wifi-hálózatába való betörésre irányuló kibertámadási kísérletben. A német szövetségi parlament elleni kibertámadás a parlament informatikai rendszere ellen irányult, és annak működését több napra megzavarta. Jelentős mennyiségű adatot tulajdonítottak el, és a támadás több képviselő, valamint Angela Merkel kancellár e-mail-fiókját is érintette.	2020.10.22.

▼B

II. MELLÉKLET

Az illetékes hatóságokra vonatkozó információkat tartalmazó internetes honlapok, valamint az Európai Bizottság értesítési címe

▼M4

BELGIUM

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGÁRIA

https://www.mfa.bg/en/EU-sanctions

CSEHORSZÁG

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DÁNIA

http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/

NÉMETORSZÁG

https://www.bmwi.de/Redaktion/DE/Artikel/Aussenwirtschaft/embargos-aussenwirtschaftsrecht.html

ÉSZTORSZÁG

https://vm.ee/et/rahvusvahelised-sanktsioonid

ÍRORSZÁG

https://www.dfa.ie/our-role-policies/ireland-in-the-eu/eu-restrictive-measures/

GÖRÖGORSZÁG

http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html

SPANYOLORSZÁG

https://www.exteriores.gob.es/es/PoliticaExterior/Paginas/SancionesInternacionales.aspx

FRANCIAORSZÁG

http://www.diplomatie.gouv.fr/fr/autorites-sanctions/

HORVÁTORSZÁG

https://mvep.gov.hr/vanjska-politika/medjunarodne-mjere-ogranicavanja/22955

OLASZORSZÁG

https://www.esteri.it/it/politica-estera-e-cooperazione-allo-sviluppo/politica_europea/misure_deroghe/

CIPRUS

https://mfa.gov.cy/themes/

LETTORSZÁG

http://www.mfa.gov.lv/en/security/4539

LITVÁNIA

http://www.urm.lt/sanctions

LUXEMBURG

https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/organisations-economiques-int/mesures-restrictives.html

MAGYARORSZÁG

https://kormany.hu/kulgazdasagi-es-kulugyminiszterium/ensz-eu-szankcios-tajekoztato

▼**M4**

MÁLTA

https://foreignandeu.gov.mt/en/Government/SMB/Pages/SMB-Home.aspx

HOLLANDIA

https://www.rijksoverheid.nl/onderwerpen/internationale-sancties

AUSZTRIA

https://www.bmeia.gv.at/themen/aussenpolitik/europa/eu-sanktionen-nationale-behoerden/

LENGYELORSZÁG

https://www.gov.pl/web/dyplomacja/sankcje-miedzynarodowe

https://www.gov.pl/web/diplomacy/international-sanctions

PORTUGÁLIA

https://www.portaldiplomatico.mne.gov.pt/politica-externa/medidas-restritivas

ROMÁNIA

http://www.mae.ro/node/1548

SZLOVÉNIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

SZLOVÁKIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINNORSZÁG

https://um.fi/pakotteet

SVÉDORSZÁG

https://www.regeringen.se/sanktioner

Az Európai Bizottság értesítési címe:

European Commission

Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA)

Rue de Spa 2

B-1049 Brussels, Belgium

E-mail-cím: relex-sanctions@ec.europa.eu