A TANÁCS (KKBP) 2020/1127 HATÁROZATA

(2020. július 30.)

az Uniót vagy annak tagállamait fenyegető kibertámadásokelleni korlátozó intézkedésekről szóló (KKBP) 2019/797 határozat módosításáról

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 2019. május 17-én elfogadta a (KKBP) 2019/797 határozatot ([1]).

(2) Az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentő, jelentős hatású kibertámadások elleni célzott korlátozó intézkedések a rosszhiszemű kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretébe (kiberdiplomáciai eszköztár) tartozó intézkedések részét képezik, és az ilyen tevékenységek megakadályozásának és azok elhárításának kulcsfontosságú eszközéül szolgálnak. Korlátozó intézkedéseket a harmadik államokkal vagy nemzetközi szervezetekkel szembeni jelentős hatású kibertámadásokra válaszul is lehet alkalmazni, amennyiben ez az Európai Unióról szóló szerződés 21. cikkének vonatkozó rendelkezéseiben meghatározott közös kül- és biztonságpolitikai célkitűzések elérése érdekében szükségesnek bizonyul.

(3) A Tanács 2018. április 16-án következtetéseket fogadott el, amelyekben határozottan elítélte az információs és kommunikációs technológiák rosszhiszemű használatát, többek között a „WannaCry” és a „NotPetya” néven ismert kibertámadások kapcsán, amelyek jelentős kárt és gazdasági veszteséget okoztak az Unióban és azon kívül. Az Európai Tanács elnöke, az Európai Bizottság elnöke, valamint az Unió külügyi és biztonságpolitikai főképviselője (a továbbiakban: a főképviselő) 2018. október 4-én egy együttes nyilatkozatban komoly aggodalmának adott hangot a Vegyifegyver-tilalmi Szervezet (OPCW) integritásának aláásását célzó, Hollandiában megkísérelt kibertámadás miatt; az agresszív cselekmény az OPCW tiszteletre méltó célja iránti ellenérzést juttatta kifejezésre. Az Unió nevében tett, 2019. április 12-i nyilatkozatában a főképviselő felhívta az elkövetőket, hogy hagyjanak fel az olyan rosszhiszemű kibertevékenységekkel, ideértve a szellemi tulajdonnak az internet felhasználásával elkövetett eltulajdonítását is, amelyek célja az Unió integritásának, biztonságának és gazdasági versenyképességének aláásása. Az ilyen, az internet felhasználásával elkövetett eltulajdonítások körébe tartoznak az Advance Persistent Threat 10 („APT10”) néven ismert csoport által elkövetett eltulajdonítások is.

(4) Ezzel összefüggésben, valamint a kibertérben folyamatban lévő és egyre fokozódó, rosszhiszemű magatartások megelőzése, visszaszorítása, megakadályozása és elhárítása érdekében hat természetes személyt és három szervezetet vagy szervet fel kell venni a korlátozó intézkedések hatálya alá tartozó természetes és jogi személyeknek, szervezeteknek és szerveknek a (KKBP) 2019/797 határozat mellékletében foglalt jegyzékébe. Az említett személyek, szervezetek vagy szervek felelősek kibertámadások elkövetéséért vagy ilyen támadásra tett kísérletekért, vagy támogatást nyújtottak ezekhez, vagy közreműködtek ilyenekben, vagy elősegítették ezeket, ideértve az OPCW ellen megkísérelt kibertámadást, a „WannaCry” és „NotPetya” néven ismert kibertámadásokat, valamint a „Cloud Hopper” műveletet is.

(5) A (KKBP) 2019/797 határozatot ezért ennek megfelelően módosítani kell,

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A (KKBP) 2019/797 határozat melléklete az e határozat mellékletével összhangban módosul.

([1]) A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről (HL L 129. I., 2019.5.17., 13. o.).

2. cikk

Ez a határozat az *Európai Unió Hivatalos Lapjában* való kihirdetésének napján lép hatályba.

Kelt Brüsszelben, 2020. július 30-án.

a Tanács részéről
az elnök
M. ROTH

Melléklet

A természetes és jogi személyeknek, valamint szervezeteknek vagy szerveknek az (KKBP) 2019/797 határozat mellékletében foglalt jegyzéke a következő személyekkel, szervezetekkel és szervekkel egészül ki:

„A. Természetes személyek

	Név:	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
1.	GAO Qiang	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 hajtja 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	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 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.	2020.7.30.

			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.	
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.

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.

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.	2020.7.30.

			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.	
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. 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.	2020.7.30.
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.	2020.7.30.“

			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. 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.	