2025/887

2025.5.13.

A TANÁCS (KKBP) 2025/887 HATÁROZATA

(2025. május 12.)

az Uniót vagy annak tagállamait fenyegető kibertámadások elleni 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) A (KKBP) 2019/797 határozat 2025. május 18-ig alkalmazandó. Az említett határozat felülvizsgálata alapján a Tanács úgy véli, hogy annak alkalmazását 2028. május 18-ig meg kell hosszabbítani.

(3) A (KKBP) 2019/797 határozat mellékletének felülvizsgálata alapján az említett határozat 4. és 5. cikkében meghatározott intézkedések alkalmazását az említett mellékletben felsorolt természetes és jogi személyek, szervezetek és szervek tekintetében 2026. május 18-ig meg kell hosszabbítani. Továbbá hat személy esetében naprakésszé kell tenni hat, a korlátozó intézkedések hatálya alá tartozó természetes és jogi személyek, szervezetek és szervek jegyzékében szereplő személy jegyzékbe való felvételének okait.

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

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A (KKBP) 2019/797 határozat a következőképpen módosul:

1. A 10. cikk helyébe a következő szöveg lép:

„*10. cikk*

Ezt a határozatot 2028. május 18-ig kell alkalmazni, és folyamatosan felül kell vizsgálni. A 4. és az 5. cikkben foglalt intézkedéseket a mellékletben felsorolt természetes és jogi személyek, szervezetek és szervek tekintetében 2026. május 18-ig kell alkalmazni.”

2. A melléklet e határozat mellékletének megfelelően módosul.

2. cikk

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

Kelt Brüsszelben, 2025. május 12-én.

a Tanács részéről

az elnök

B. NOWACKA

[1] A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről (HL L 129I., 2019.5.17., 13. o., ELI: http://data.europa.eu/eli/dec/2019/797/oj).

MELLÉKLET

A (KKBP) 2019/797 határozat mellékletének „A. Természetes személyek” címében a 3–8. bejegyzés helyébe a következők lépnek:

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Születési idő: 1972.5.27. Születési hely: Perm Oblast, Russian SFSR (jelenleg: Russian Federation) Útlevélszám: 120017582 Kibocsátó: az Oroszországi Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation) Érvényes: 2017.4.17.-től 2022.4.17.-ig Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Alexey Minin részt vett egy a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányuló, potenciálisan jelentős hatású kibertámadási kísérletben, valamint harmadik államok elleni, jelentős hatású kibertámadásokban. Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation) (GU/GRU) humán felderítési támogató tisztjeként Alexey Minin egy négy orosz katonai hírszerzési tisztekből álló csoport tagja volt, akik 2018. áprilisban Hágában (Hollandia) megpróbáltak jogosulatlanul 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) (Militaire Inlichtingen- en Veiligheidsdienst) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt. Pennsylvania (Amerikai Egyesült Államok) nyugati körzetében egy vádesküdtszék vádat emelt Alexey Minin – a GRU tisztje – ellen számítógépes kalózkodásért, elektronikus eszköz segítségével elkövetett csalásért, a személyazonosság-lopás minősített eseteiért és pénzmosásért. A GRU továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. Ezért Alexey Minin a GRU tagjaként részt vesz jelentős hatású kibertámadásokban – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.	2020.7.30.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
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 Oroszországi Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation) Érvényes: 2017.4.17.-től 2022.4.17.-ig Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Aleksei Morenets részt vett egy a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányuló, potenciálisan jelentős hatású kibertámadási kísérletben, valamint harmadik államok elleni, jelentős hatású kibertámadásokban. Az Oroszországi 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 azon négy orosz katonai hírszerzési tisztből álló csoport tagja volt, akik 2018. áprilisban Hágában (Hollandia) megpróbáltak jogosulatlanul 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) (Militaire Inlichtingen- en Veiligheidsdienst) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt. Pennsylvania (Amerikai Egyesült Államok) nyugati körzetében egy vádesküdtszék vádat emelt – a 26165-ös katonai egységhez rendelt – Aleksei Morenets ellen számítógépes kalózkodásért, elektronikus eszköz segítségével elkövetett csalásért, a személyazonosság-lopás minősített eseteiért és pénzmosásért. A GRU továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. Ezért Aleksei Morenets a GRU tagjaként részt vesz jelentős hatású kibertámadásokban – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.	2020.7.30.

	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 Oroszországi Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation) Érvényes: 2017.4.17.-től 2022.4.17.-ig Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Evgenii Serebriakov részt vett egy a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányuló, potenciálisan jelentős hatású kibertámadási kísérletben, valamint harmadik államok elleni, jelentős hatású kibertámadásokban. Az Oroszországi 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 azon négy orosz katonai hírszerzési tisztből álló csoport tagja volt, akik 2018. áprilisban Hágában (Hollandia) megpróbáltak jogosulatlanul 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) (Militaire Inlichtingen- en Veiligheidsdienst) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt. 2022 tavasza óta Evgenii Serebriakov vezeti a »Sandworm«-öt (más néven: »Sandworm Team«, »BlackEnergy Group«, »Voodoo Bear«, »Quedagh«, »Olympic Destroyer« és »Telebots«), amely az orosz központi hírszerzési igazgatóság (Russian Main Intelligence Directorate) 74455-ös egységéhez kapcsolódó szereplő és hekkercsoport. Oroszország Ukrajna elleni agressziós háborúja nyomán a Sandworm kibertámadásokat hajtott végre Ukrajna, így többek között ukrán kormányzati ügynökségek ellen. A GRU továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. Ezért Evgenii Serebriakov a GRU tagjaként részt vesz jelentős hatású kibertámadásokban – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.	2020.7.30.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Születési idő: 1972.8.24. Születési hely: Ulyanovsk, Russian SFSR (jelenleg: Russian Federation) Útlevélszám: 120018866 Kibocsátó: az Oroszországi Föderáció Külügyminisztériuma (Ministry of Foreign Affairs of the Russian Federation) Érvényes: 2017.4.17.-től 2022.4.17.-ig Tartózkodási hely: Moscow, Russian Federation Állampolgárság: orosz Nem: férfi	Oleg Sotnikov részt vett egy a Hollandiában található Vegyifegyver-tilalmi Szervezet (OPCW) ellen irányuló, potenciálisan jelentős hatású kibertámadási kísérletben, valamint harmadik államok elleni, jelentős hatású kibertámadásokban. Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation) (GU/GRU) humán felderítési támogató tisztjeként Oleg Sotnikov azon négy orosz katonai hírszerzési tisztből álló csoport tagja volt, akik 2018. áprilisban Hágában (Hollandia) megpróbáltak jogosulatlanul 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) (Militaire Inlichtingen- en Veiligheidsdienst) megakadályozta a kibertámadási kísérletet, és ezáltal megelőzte az OPCW-t fenyegető súlyos kárt. Pennsylvania (Amerikai Egyesült Államok) nyugati körzetében egy vádesküdtszék vádat emelt Oleg Sotnikov – a GRU tisztje – ellen számítógépes kalózkodásért, elektronikus eszköz segítségével elkövetett csalásért, a személyazonosság-lopás minősített eseteiért és pénzmosásért. A GRU továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. Ezért Oleg Sotnikov a GRU tagjaként részt vesz jelentős hatású kibertámadásokban – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.	2020.7.30.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Születési idő: 1990.11.15. Születési hely: Kursk, Russian SFSR (jelenleg: Russian Federation) Állampolgárság: orosz Nem: férfi	Dmitry Badin részt vett egy a német szövetségi parlament (Deutscher Bundestag) elleni, jelentős hatású kibertámadásban, valamint harmadik államok elleni, jelentős hatású kibertámadásokban. Az Oroszországi Föderáció fegyveres erői vezérkara Főigazgatóságának (Main Directorate of the General Staff of the Armed Forces of the Russian Federation) (GU/GRU) 85. Különleges Szolgálati Főközpontja (85th Main Centre of Special Services, GTsSS) katonai hírszerző tisztjeként Dmitry Badin tagja volt azon orosz katonai hírszerző tisztekből álló csapatnak, akik 2015. áprilisban és májusban kibertámadást intéztek a német szövetségi parlament ellen. Az említett kibertámadás a parlament informatikai rendszere ellen irányult, és annak működését több napra megzavarta. Jelentős mennyiségű adatot tulajdonítottak el, továbbá a támadás több képviselő és Angela Merkel korábbi kancellár e-mail-fiókját is érintette. Pennsylvania (Amerikai Egyesült Államok) nyugati körzetében egy vádesküdtszék vádat emelt – a 26165-ös katonai egységhez rendelt – Dmitry Badin ellen számítógépes kalózkodásért, elektronikus eszköz segítségével elkövetett csalásért, a személyazonosság-lopás minősített eseteiért és pénzmosásért. A GRU továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. Ezért Dmitry Badin a GRU tagjaként részt vesz jelentős hatású kibertámadásokban – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.	2020.10.22.

	Név	Azonosító adatok	A jegyzékbe vétel okai	A jegyzékbe vétel időpontja
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Születési idő: 1961.2.21. 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«, »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, komoly hatással jártak. Így különösen, a GTsSS katonai hírszerző tisztjei részt vettek a német szövetségi parlament (Deutscher Bundestag) ellen 2015. áprilisban és májusban intézett kibertámadásban, valamint 2018. áprilisban a Hollandiában található 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, továbbá a támadás több képviselő, valamint Angela Merkel korábbi kancellár e-mail-fiókját is érintette. A GRU továbbra is aktív az Unió, illetve annak tagállamai elleni kibertámadások végrehajtásában. Ezért Igor Kostyukov a GRU tagjaként részt vesz jelentős hatású kibertámadásokban – ideértve a potenciálisan jelentős hatással járó, megkísérelt kibertámadásokat is –, amelyek az Unióra vagy annak tagállamaira nézve külső fenyegetést jelentenek.	2020.10.22.”