DECIZIA (PESC) 2025/887 A CONSILIULUI

din 12 mai 2025

de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 29,

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Decizia (PESC) 2019/797 [1].

(2) Decizia (PESC) 2019/797 se aplică până la 18 mai 2025. Pe baza unei reexaminări a deciziei respective, Consiliul consideră că aplicarea acesteia ar trebui să fie prelungită până la 18 mai 2028.

(3) Pe baza unei reexaminări a anexei la Decizia (PESC) 2019/797, aplicarea măsurilor prevăzute la articolele 4 și 5 din decizia respectivă în ceea ce privește persoanele fizice și juridice, entitățile și organismele care figurează pe lista din anexa respectivă ar trebui să fie prelungită până la 18 mai 2026. În plus, ar trebui să fie actualizate motivele includerii a șase persoane pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsuri restrictive.

(4) Prin urmare, Decizia (PESC) 2019/797 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Decizia (PESC) 2019/797 se modifică după cum urmează:

1. Articolul 10 se înlocuiește cu următorul text:

„*Articolul 10*

Prezenta decizie se aplică până la 18 mai 2028 și se reexaminează permanent. Măsurile prevăzute la articolele 4 și 5 se aplică persoanelor fizice și juridice, entităților și organismelor de pe lista cuprinsă în anexă până la 18 mai 2026."

2. Anexa se modifică în conformitate cu anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 12 mai 2025.

Pentru Consiliu

Președintele

B. NOWACKA

[1] Decizia (PESC) 2019/797 a Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129 I, 17.5.2019, p. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

ANEXĂ

În anexa la Decizia (PESC) 2019/797, la secțiunea „A. Persoane fizice”, rubricile 3-8 se înlocuiesc cu următorul text:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data nașterii: 27.5.1972 Locul nașterii: Regiunea Perm, RSFS Rusă (în prezent Federația Rusă) Numărul pașaportului: 120017582 Eliberat de: Ministerul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	Alexey Minin a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer de sprijin specializat în informații din surse umane al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), Alexey Minin a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Alexey Minin, ca ofițer al GRU, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Alexey Minin este implicat așadar în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data nașterii: 31.7.1977 Locul nașterii: Regiunea Murmansk, RSFS Rusă (în prezent Federația Rusă) Numărul pașaportului: 100135556 Eliberat de: Ministerul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	Alexey Morenets a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de operator informatic pentru Direcția principală a Statului-Major al forțelor armate ruse (GU/GRU), Aleksei Morenets a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Alexey Morenets ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Aleksei Morenets este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data nașterii: 26.7.1981 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Numărul pașaportului: 100135555 Eliberat de: Ministerul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	Evgenii Serebriakov a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de operator informatic pentru Direcția principală a Statului-Major al forțelor armate ruse (GU/GRU), Evgenii Serebriakov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Din primăvara anului 2022, Evgenii Serebriakov conduce «Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» și «Telebots»), un actor și un grup de piraterie informatică afiliat unității 74455 a Direcției principale de informații ruse. Sandworm a desfășurat atacuri cibernetice asupra Ucrainei, inclusiv asupra agențiilor guvernamentale ucrainene, în urma războiului de agresiune al Rusiei împotriva Ucrainei. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Evgenii Serebriakov este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data nașterii: 24.8.1972 Locul nașterii: Ulianovsk, RSFS Rusă (în prezent, Federația Rusă) Numărul pașaportului: 120018866 Eliberat de: Ministerul de Externe al Federației Ruse Valabil de la 17.4.2017 la 17.4.2022 Loc: Moscova, Federația Rusă Cetățenie: rusă Sexul: masculin	Oleg Sotnikov a luat parte la o tentativă de atac cibernetic cu efecte potențial semnificative asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer de sprijin specializat în informații din surse umane al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), Oleg Sotnikov a făcut parte dintr-o echipă formată din patru ofițeri din serviciul militar de informații rus, care a încercat să obțină accesul neautorizat la rețeaua Wi-Fi a OIAC de la Haga, Țările de Jos, în aprilie 2018. Tentativa de atac cibernetic viza accesul neautorizat la rețeaua Wi-Fi a OIAC, care, în caz de reușită, ar fi compromis securitatea rețelei și activitatea de investigare în curs a OIAC. Serviciul de securitate, de informații și de apărare din Țările de Jos (Militaire Inlichtingen- en Veiligheidsdienst) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Oleg Sotnikov ca ofițer al GRU, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Oleg Sotnikov este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data nașterii: 15.11.1990 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Cetățenie: rusă Sexul: masculin	Dmitry Badin a luat parte la un atac cibernetic cu efecte semnificative asupra parlamentului federal german (Deutscher Bundestag) și la atacuri cibernetice cu efecte semnificative asupra unor state terțe. În calitatea sa de ofițer în serviciul militar de informații al celui de al 85-lea Centru principal de servicii speciale (GTsSS) din cadrul Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU), Dmitry Badin a făcut parte dintr-o echipă de ofițeri ai serviciului militar de informații rus care a organizat un atac cibernetic împotriva parlamentului federal german în aprilie și mai 2015. Respectivul atac cibernetic a fost îndreptat împotriva sistemului informatic al parlamentului, căruia i-a afectat funcționarea timp de mai multe zile. A fost furat un volum important de date și au fost afectate conturile de e-mail ale mai multor parlamentari, precum și cel al fostei cancelare Angela Merkel. Un mare juriu din districtul Pennsylvania de Vest (Statele Unite ale Americii) l-a pus sub acuzare pe Dmitry Badin ca membru al unității militare 26165, pentru piraterie informatică, fraudă cu ajutorul mijloacelor de comunicare, furt de identitate calificat și spălarea banilor. GRU rămâne activă în desfășurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Dmitry Badin este așadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potențial semnificativ, care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	22.10.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data naşterii: 21.2.1961 Cetăţenie: rusă Sexul: masculin	Igor Kostyukov este actualul şef al Direcţiei principale a Statului-Major al forţelor armate al Federaţiei Ruse (GU/GRU), unde a ocupat anterior funcţia de prim-şef adjunct. Una dintre unităţile aflate sub comanda sa este cel de al 85-lea Centru principal de servicii speciale (GTsSS) (alias «unitatea militară 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» şi «Strontium»). În această calitate, Igor Kostyukov este responsabil de atacurile cibernetice desfăşurate de GTsSS, inclusiv de atacuri cu efecte semnificative care reprezintă o ameninţare externă la adresa Uniunii sau a statelor sale membre. În special, ofiţerii serviciului militar de informaţii al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) în aprilie şi mai 2015, precum şi la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea reţelei Wi-Fi a Organizaţiei pentru Interzicerea Armelor Chimice (OIAC) din Ţările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, căruia i-a afectat funcţionarea timp de mai multe zile. A fost furat un volum important de date şi au fost afectate conturile de e-mail ale mai multor parlamentari, precum şi cel al fostei cancelare Angela Merkel. GRU rămâne activă în desfăşurarea de atacuri cibernetice împotriva Uniunii sau a statelor sale membre. În calitatea sa de membru al GRU, Igor Kostyukov este aşadar implicat în atacuri cibernetice cu un efect semnificativ, inclusiv tentative de atacuri cibernetice care au un efect potenţial semnificativ, care constituie o ameninţare externă la adresa Uniunii sau a statelor sale membre.	22.10.2020”