DECIZII

DECIZIA (PESC) 2020/1537 A CONSILIULUI

din 22 octombrie 2020

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) Măsurile restrictive specifice împotriva atacurilor cibernetice cu efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre se numără printre măsurile incluse în cadrul Uniunii privind un răspuns diplomatic comun la activitățile cibernetice răuvoitoare („Setul de instrumente pentru diplomația cibernetică"), precum și un instrument vital pentru a împiedica atacurile cibernetice și a răspunde la acestea.

(3) Pentru a preveni, descuraja și împiedica comportamentul răuvoitor continuu și tot mai intens în spațiul cibernetic, precum și pentru a răspunde la acesta, două persoane fizice și un organism ar trebui incluse pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsurile restrictive prevăzute în anexa la Decizia (PESC) 2019/797. Respectivele persoane și respectivul organism sunt responsabile de sau au fost implicate în atacuri cibernetice cu efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre, în special atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) care a avut loc în aprilie și mai 2015.

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

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Anexa la Decizia (PESC) 2019/797 se modifică în conformitate cu anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 22 octombrie 2020.

Pentru Consiliu
Președintele
M. ROTH

([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).

ANEXĂ

Următoarele rubrici se adaugă la lista persoanelor fizice și juridice, a entităților și a organismelor prevăzută în anexa la Decizia (PESC) 2019/797:

A. Persoane fizice

	Nume	Informații de identificare	Motive	Data includerii pe listă
„7.	Dmitri Sergheevici BADIN	Дмитрий Сергеевич Бадин Data nașterii: 15 noiembrie 1990 Locul nașterii: Kursk, RSFS Rusă (în prezent, Federația Rusă) Cetățenie: rusă Sexul: masculin	Dmitri Badin a luat parte la un atac cibernetic cu efecte importante împotriva parlamentului federal german (Deutscher Bundestag). 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), Dmitri 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 (Deutscher Bundestag) în aprilie și mai 2015. Acest 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 cancelarului Angela Merkel.	22.10.2020
8.	Igor Olegovici KOSTIUKOV	Игорь Олегович Костюков Data nașterii: 21 februarie 1961 Cetățenie: rusă Sexul: masculin	Igor Kostiukov este actualul șef al Direcției principale a Statului-Major al forțelor armate al Federației Ruse (GU/GRU), unde a ocupat anterior funcția de prim-șef adjunct. Una dintre unitățile aflate sub comanda sa este cel de al 85-lea Centru principal de servicii speciale (GTsSS), cunoscut și sub denumirea de «unitatea militară 26165» (pseudonime folosite în domeniu: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» și «Strontium»). În această calitate, Igor Kostiukov este responsabil de atacurile cibernetice desfășurate de GTsSS, inclusiv de atacuri cu efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre. În special, ofițerii serviciului militar de informații al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) care a avut loc în aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea rețelei Wi-fi a Organizației pentru Interzicerea Armelor Chimice (OIAC) din Țările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, 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 cancelarului Angela Merkel.	22.10.2020”

B. Persoane juridice, entități și organisme

	Denumire	Informații de identificare	Motive	Data includerii pe listă
„4.	Cel 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)	Adresa: Komsomol'ski Prospekt, 20, Moscova, 119146, Federația Rusă	Cel 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), cunoscut și sub denumirea de «unitatea militară 26165» (pseudonime folosite în domeniu: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» și «Strontium»), este responsabil de atacuri cibernetice cu efecte importante care reprezintă o amenințare externă la adresa Uniunii sau a statelor sale membre. În special, ofițerii serviciului militar de informații al GTsSS au luat parte la atacul cibernetic împotriva parlamentului federal german (Deutscher Bundestag) care a avut loc în aprilie și mai 2015, precum și la tentativa de atac cibernetic din aprilie 2018 care a avut drept scop piratarea rețelei Wi-fi a Organizației pentru Interzicerea Armelor Chimice (OIAC) din Țările de Jos. Atacul cibernetic împotriva parlamentului federal german a fost îndreptat împotriva sistemului informatic al acestuia, 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 cancelarului Angela Merkel.	22.10.2020”