DECIZIA (PESC) 2020/1127 A CONSILIULUI

din 30 iulie 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 având 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. Măsurile restrictive pot fi aplicate, de asemenea, ca răspuns la atacuri cibernetice având efecte importante asupra unor state terțe sau organizații internaționale, atunci când se consideră că acest lucru este necesar pentru realizarea obiectivelor politicii externe și de securitate comune prevăzute de dispozițiile relevante de la articolul 21 din Tratatul privind Uniunea Europeană.

(3) La 16 aprilie 2018, Consiliul a adoptat concluzii prin care condamnă cu fermitate utilizarea răuvoitoare a tehnologiilor informației și comunicațiilor, inclusiv în atacurile cibernetice cunoscute sub numele de „WannaCry" și „NotPetya", care au provocat pierderi economice și prejudicii importante în Uniune și în afara acesteia. La 4 octombrie 2018, președintele Consiliului European, președintele Comisiei Europene, precum și Înaltul Reprezentant al Uniunii pentru afaceri externe și politica de securitate (denumit în continuare „Înaltul Reprezentant") și-au exprimat, printr-o declarație comună, profunda îngrijorare cu privire la o tentativă de atac cibernetic de subminare a integrității Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos, un act agresiv care exprimă disprețul față de obiectivul solemn al OIAC. Printr-o declarație în numele Uniunii la 12 aprilie 2019, Înaltul Reprezentant a îndemnat actorii să înceteze să desfășoare activități cibernetice răuvoitoare prin care se urmărește subminarea integrității, a securității și a competitivității economice a Uniunii, inclusiv actele de furt de proprietate intelectuală facilitat prin mijloace informatice. Printre astfel de furturi facilitate prin mijloace informatice se numără cele realizate de actorul cunoscut în mod public sub numele de „APT10" („Advanced Persistent Threat 10").

(4) În acest context și pentru a preveni, descuraja și împiedica comportamentul răuvoitor continuu și tot mai intens în spațiul cibernetic, precum și pentru a răspunde la acesta, șase persoane fizice și trei entități sau organisme 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. Persoanele și entitățile sau organismele respective sunt responsabile pentru desfășurarea atacurilor cibernetice sau a tentativelor de atacuri cibernetice, inclusiv a tentativei de atac cibernetic împotriva OIAC și de atacurile cibernetice cunoscute sub numele de „WannaCry" și „NotPetya", precum și „Operation Cloud Hopper", ori au fost implicate în respectivele atacuri sau tentative de atacuri, le-au oferit sprijin sau le-au facilitat.

(5) Prin urmare, Decizia (PESC) 2019/797 ar trebui modificată în consecință,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

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

([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).

Articolul 2

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

Adoptată la Bruxelles, 30 iulie 2020.

Pentru Consiliu
Președintele
M. ROTH

ANEXĂ

Următoarele persoane și entități sau organisme se adaugă pe lista persoanelor fizice și juridice, a entităților și a organismelor prevăzute în anexa la Decizia (PESC) 2019/797:

„A. Persoane fizice

	Nume	Informații de identificare	Motive	Data includerii pe listă
1.	GAO Qiang	Locul nașterii: Shandong Province, China (Provincia Shandong, China) Adresă: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China (Camera 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China) Cetățenie: chineză Sexul: masculin	Gao Qiang este implicat în «Operation Cloud Hopper», o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe. «Operation Cloud Hopper» a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Actorul cunoscut în mod public sub numele de «APT10» («Advanced Persistent Threat 10») (*alias* «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») a efectuat «Operation Cloud Hopper». Se poate stabili o legătură între Gao Qiang și APT10, inclusiv prin asocierea acestuia cu infrastructura de comandă și control a APT10. În plus, Huaying Haitai, entitate desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Gao Qiang. Acesta are legături cu Zhang Shilong, desemnat la rândul său în legătură cu «Operation Cloud Hopper». Prin urmare, Gao Qiang este asociat atât cu Huaying Haitai, cât și cu Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Adresă: Hedong, Yuyang Road No 121, Tianjin, China Cetățenie: chineză Sexul: masculin	Zhang Shilong este implicat în «Operation Cloud Hopper», o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii și a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe. «Operation Cloud Hopper» a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Actorul cunoscut în mod public sub numele de «APT10» («Advanced Persistent Threat 10») (alias «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») a efectuat «Operation Cloud Hopper».	30.7.2020

			Se poate stabili o legătură între Zhang Shilong și APT10, inclusiv prin programele malware pe care acesta le-a dezvoltat și testat în legătură cu atacurile cibernetice desfășurate de APT10. În plus, Huaying Haitai, entitate desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Zhang Shilong. Acesta are legături cu Gao Qiang, desemnat la rândul său în legătură cu «Operation Cloud Hopper». Prin urmare, Zhang Shilong este asociat atât cu Huaying Haitai, cât și cu Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data nașterii: 27 mai 1972 Locul nașterii: Perm Oblast, Russian SFSR (now Russian Federation) [Perm Oblast, RSFS Rusă (în prezent, Federația Rusă)] Numărul pașaportului: 120017582, emis de Ministerul Afacerilor Externe al Federației Ruse, valabil de la 17 aprilie 2017 până la 17 aprilie 2022 Locul: Moscow, Russian Federation (Moscova, Federația Rusă) Cetățenie: rusă Sexul: masculin	Alexey Minin a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos. 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 acces 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data nașterii: 31 iulie 1977 Locul nașterii: Murmanskaya Oblast, Russian SFSR (now Russian Federation) [Murmanskaya Oblast, RSFS Rusă (în prezent, Federația Rusă)] Numărul pașaportului: 100135556, emis de Ministerul Afacerilor Externe al Federației Ruse, valabil de la 17 aprilie 2017 până la 17 aprilie 2022 Locul: Moscow, Russian Federation (Moscova, Federația Rusă) Cetățenie: rusă Sexul: masculin	Aleksei Morenets a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos. 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 acces 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 WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data nașterii: 26 iulie 1981 Locul nașterii: Kursk, Russian SFSR (now Russian Federation) [Kursk, RSFS Rusă (în prezent, Federația Rusă)] Numărul pașaportului: 100135555, emis de Ministerul Afacerilor Externe al Federației Ruse, valabil de la 17 aprilie 2017 până la 17 aprilie 2022 Locul: Moscow, Russian Federation (Moscova, Federația Rusă) Cetățenie: rusă Sexul: masculin	Evgenii Serebriakov a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos. 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 acces 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 WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data nașterii: 24 august 1972 Locul nașterii: Ulyanovsk, Russian SFSR (now Russian Federation) [Ulyanovsk, RSFS Rusă (în prezent, Federația Rusă)] Numărul pașaportului: 120018866, emis de Ministerul Afacerilor Externe al Federației Ruse, valabil de la 17 aprilie 2017 până la 17 aprilie 2022 Locul: Moscow, Russian Federation (Moscova, Federația Rusă) Cetățenie: rusă Sexul: masculin	Oleg Sotnikov a luat parte la o tentativă de atac cibernetic care ar fi putut avea efecte importante asupra Organizației pentru Interzicerea Armelor Chimice (OIAC) în Țările de Jos. 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 acces 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 WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) a întrerupt tentativa de atac cibernetic, preîntâmpinând astfel un prejudiciu grav pentru OIAC.	30.7.2020

B. Persoane juridice, entități și organisme

	Nume	Informații de identificare	Motive	Data includerii pe listă
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	*alias* Haitai Technology Development Co. Ltd Localizare: Tianjin, China	Huaying Haitai a oferit sprijin financiar, tehnic sau material și a facilitat «Operation Cloud Hopper», o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe.	30.7.2020

			«Operation Cloud Hopper» a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Actorul cunoscut în mod public sub numele de «APT10» («Advanced Persistent Threat 10») (alias «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») a efectuat «Operation Cloud Hopper». Poate fi stabilită o legătură între Huaying Haitai și APT10. În plus, Gao Qiang și Zhang Shilong, ambii desemnați în legătură cu «Operation Cloud Hopper» au fost angajați ai Huaying Haitai. Prin urmare, Huaying Haitai este asociat cu Gao Qiang și cu Zhang Shilong.	
2.	Chosun Expo	*alias* Chosen Expo; Korea Export Joint Venture Locație RPDC	Chosun Expo a oferit sprijin financiar, tehnic sau material și a facilitat o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care au constituit o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe, inclusiv atacurile cibernetice cunoscute sub numele de «WannaCry» și atacurile cibernetice împotriva Autorității de supraveghere financiară din Polonia și împotriva Sony Pictures Entertainment, precum și furtul cibernetic de la Bangladesh Bank și tentativa de furt cibernetic de la Vietnam Tien Phong Bank. «WannaCry» a perturbat sistemele de informații din întreaga lume prin vizarea sistemelor de informații cu programe de tip ransomware și prin blocarea accesului la date. A afectat sistemele de informații ale întreprinderilor din Uniune, inclusiv sistemele de informații referitoare la serviciile necesare pentru menținerea serviciilor esențiale și a activităților economice din statele membre. Atacul «WannaCry» a fost comis de actorul cunoscut în mod public sub numele de «APT38 («Advanced Persistent Threat 38») sau «Lazarus Group». Se poate stabili o legătură între Chosun Expo și APT38/Lazarus Group, inclusiv prin intermediul conturilor utilizate pentru atacurile cibernetice.	30.7.2020
3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) [Centrul principal pentru tehnologii speciale (GTsST) al Direcției principale a Statului-	Adresa: 22 Kirova Street, Moscow, Russian Federation (22 Kirova Street, Moscova, Federația Rusă)	Centrul principal pentru tehnologii speciale (GTsST) al Direcției principale a Statului-Major al forțelor armate ruse (GU/GRU), cunoscut și prin codul său poștal de teren 74455, este responsabil pentru o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe, inclusiv atacurile cibernetice cunoscute în mod public sub numele «NotPetya» sau «EternalPetya» din iunie 2017 și atacurile cibernetice îndreptate împotriva unui sistem electroenergetic ucrainean din iarna anilor 2015 și 2016.	30.7.2020”

	Major al forțelor armate ruse (GU/GRU)]		«NotPetya» sau «EternalPetya» a blocat accesul la date în mai multe întreprinderi din Uniune, din Europa în ansamblu și din întreaga lume, prin vizarea computerelor prin programe de tip ransomware și prin blocarea accesului la date, ceea ce a dus, printre altele, la pierderi economice importante. Atacul cibernetic asupra unui sistem electroenergetic ucrainean a condus la întreruperea unor porțiuni ale acestuia în timpul iernii. Actorul cunoscut în mod public sub numele de «Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» și «Telebots»), aflat, de asemenea, în spatele atacului asupra sistemului electroenergetic ucrainean, a comis atacul «NotPetya» sau «EternalPetya». Centrul principal pentru tehnologii speciale al Direcției principale a Statului-Major al forțelor armate ruse din Federația Rusă are un rol activ în activitățile cibernetice desfășurate de Sandworm și poate fi stabilită o legătură între centru și acesta.	