РЕШЕНИЕ (ОВППС) 2020/1127 НА СЪВЕТА

от 30 юли 2020 година

за изменение на Решение (ОВППС) 2019/797 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за Европейския съюз, и по-специално член 29 от него,

като взе предвид предложението на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност,

като има предвид, че:

(1) На 17 май 2019 г. Съветът прие Решение (ОВППС) 2019/797 ([1]).

(2) Целенасочените ограничителни мерки срещу кибератаки със значително въздействие, представляващи външна заплаха за Съюза или неговите държави членки, са сред мерките, включени в рамката на Съюза за съвместен дипломатически отговор на злонамерени действия в киберпространството („инструментариум за кибердипломация“), и са жизненоважен инструмент за възпирането и реагирането на такива действия. Ограничителните мерки може да се прилагат също и в отговор на кибератаки със значително въздействие срещу трети държави или международни организации, когато това се счете за необходимо за постигане на общите цели на външната политика и политиката на сигурност, предвидени в съответните разпоредби на член 21 от Договора за Европейския съюз.

(3) На 16 април 2018 г. Съветът прие заключения, в които категорично се осъжда злонамереното използване на информационни и комуникационни технологии, включително при кибератаките, известни в публичното пространство като WannaCry и NotPetya, които причиниха значителни щети и икономически загуби в Съюза и извън него. На 4 октомври 2018 г. председателите на Европейския съвет и на Европейската комисия и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност („върховният представител“) изразиха в съвместно изявление сериозна загриженост поради опита за кибератака с цел да се накърни репутацията на Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия — агресивен акт на незачитане на важната цел, преследвана от ОЗХО. В декларация от името на Съюза от 12 април 2019 г. върховният представител призова участниците да спрат със злонамерените действия в киберпространството, които имат за цел да накърнят репутацията, сигурността и икономическата конкурентоспособност на Съюза, включително с кражби на интелектуална собственост, извършвани чрез киберметоди. Някои от тези кражби чрез кибернетични похвати са дело на извършителя, известен в публичното пространство като „APT10“ („Advanced Persistent Threat 10“).

(4) В този контекст и с цел предотвратяване, разколебаване, възпиране и реагиране на продължаващото и засилващо се злонамерено поведение в киберпространството, в списъка на подлежащите на ограничителни мерки физически и юридически лица, образувания и органи, съдържащ се в приложението към Решение (ОВППС) 2019/797 следва да бъдат включени шест физически лица и три образувания или органи. Тези лица и образувания или органи са отговорни за кибератаки или опити за кибератаки, оказвали са подкрепа, участвали са във, или са улеснявали такива кибератаки или опити за кибератаки, включително в опита за кибератака срещу ОЗХО и кибератаките, известни в публичното пространство като WannaCry и NotPetya, а така също и „Операция Cloud Hopper“.

(5) Поради това Решение (ОВППС) 2019/797 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩОТО РЕШЕНИЕ:

Член 1

Приложението към Решение (ОВППС) 2019/797 се изменя в съответствие с приложението към настоящото решение.

([1]) Решение (ОВППС) 2019/797 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 129I, 17.5.2019 г., стр. 13).

Член 2

Настоящото решение влиза в сила в деня на публикуването му в *Официален вестник на Европейския съюз*.

Съставено в Брюксел на 30 юли 2020 година.

За Съвета
Председател
M. ROTH

ПРИЛОЖЕНИЕ

В списъка на физическите и юридическите лица, образуванията и органите, съдържащ се в приложението към Решение (ОВППС) 2019/797, се добавят следните лица и образувания или органи:

A. Физически лица

	Име	Идентификационни данни	Основания	Дата на вписване
1.	GAO Qiang	Място на раждане: Провинция Shandong, Китай Адрес: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Китай Гражданство: китайско Пол: мъжки	Gao Qiang участва в „Операция Cloud Hopper“ — серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави. Мишена на „Операция Cloud Hopper“ са информационните системи на многонационални дружества от шест континента, в т.ч. дружества на територията на Съюза, при което е осъществен неразрешен достъп до чувствителни търговски данни, довел до значителни икономически загуби. „Операция Cloud Hopper“ е дело на извършител, известен в публичното пространство като „APT10“ („Advanced Persistent Threat 10“) (изв. още като „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium“). Gao Qiang може да бъде свързан с APT10, включително чрез свързаността си с командната и контролната инфраструктура на APT10. Освен това Gao Qiang работи за Huaying Haitai — образувание, посочено като оказало подкрепа и улеснение за „Операция Cloud Hopper“. Той има връзка с Zhang Shilong, който също е посочен във връзка с „Операция Cloud Hopper“. Следователно Gao Qiang се свързва както с Huaying Haitai, така и с Zhang Shilong.	30.7.2020 г.
2.	ZHANG Shilong	Адрес: Hedong, Yuyang Road № 121, Tianjin, Китай Гражданство: китайско Пол: мъжки	Zhang Shilong участва в „Операция Cloud Hopper“ — серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави. Мишена на „Операция Cloud Hopper“ са информационните системи на многонационални дружества от шест континента, в т.ч. дружества на територията на Съюза, при което е осъществен неразрешен достъп до чувствителни търговски данни, довел до значителни икономически загуби. „Операция Cloud Hopper“ е дело на извършител, известен в публичното пространство като „APT10“ („Advanced Persistent Threat 10“) (изв. още като „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium“).	30.7.2020 г.

			Zhang Shilong може да бъде свързан с APT10, включително чрез зловредния софтуер, разработен и тестван от него във връзка с извършените от APT10 кибератаки. Освен това Zhang Shilong работи за Huaying Haitai — образувание, посочено като оказало подкрепа и улеснение за „Операция Cloud Hopper“. Той има връзка с Gao Qiang, който също е посочен във връзка с „Операция Cloud Hopper“. Следователно Zhang Shilong се свързва както с Huaying Haitai, така и с Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Дата на раждане: 27 май 1972 г. Място на раждане: Пермска област, РСФСР (днес Руска федерация) Паспорт № 120017582, издаден от Министерството на външните работи на Руската федерация, валиден от 17 април 2017 г. до 17 април 2022 г. Местопребиваване: Москва, Руска федерация Гражданство: руско Пол: мъжки	Алексей Минин участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия. Като оперативен офицер от агентурното разузнаване към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Алексей Минин е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО.	30.7.2020 г.
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Дата на раждане: 31 юли 1977 г. Място на раждане: Мурманска област, РСФСР (днес Руска федерация) Паспорт № 100135556, издаден от Министерството на външните работи на Руската федерация, валиден от 17 април 2017 г. до 17 април 2022 г. Местопребиваване: Москва, Руска федерация Гражданство: руско Пол: мъжки	Алексей Моренец участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия. Като кибероператор за Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Алексей Моренец е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО.	30.7.2020 г.

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Дата на раждане: 26 юли 1981 г. Място на раждане: Курск, РСФСР (днес Руска федерация) Паспорт № 100135555, издаден от Министерството на външните работи на Руската федерация, валиден от 17 април 2017 г. до 17 април 2022 г. Местопребиваване: Москва, Руска федерация Гражданство: руско Пол: мъжки	Евгений Серебряков участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия. Като кибероператор за Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Евгений Серебряков е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО.	30.7.2020 г.
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Дата на раждане: 24 август 1972 г. Място на раждане: Уляновск, РСФСР (днес Руска федерация) Паспорт № 120018866, издаден от Министерството на външните работи на Руската федерация, валиден от 17 април 2017 г. до 17 април 2022 г. Местопребиваване: Москва, Руска федерация Гражданство: руско Пол: мъжки	Олег Сотников участва в опит за кибератака с потенциално значително въздействие срещу Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия. Като оперативен офицер от агентурното разузнаване към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Олег Сотников е част от четиричленен екип офицери на руското военно разузнаване, опитали се да осъществят през април 2018 г. неразрешен достъп до безжичната мрежа на ОЗХО в Хага, Нидерландия. Опитът за кибератака е целял включване чрез хакерска атака в безжичната мрежа на ОЗХО, което, ако беше успяло, щеше да наруши сигурността на мрежата и извършваните към момента разследвания от ОЗХО. Нидерландската Служба за военно разузнаване и сигурност (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) прекъсва опита за кибератака, с което предотвратява сериозни щети за ОЗХО.	30.7.2020 г.

Б. Юридически лица, образувания и органи

	Наименование	Идентификационни данни	Основания	Дата на вписване
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd	Известно също като: Haitai Technology Development Co. Ltd Местонахождение: Tianjin, Китай	Huaying Haitai предоставя финансова, техническа или материална подкрепа и улеснява „Операция Cloud Hopper“ — серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави.	30.7.2020 г.

			Мишена на „Операция Cloud Hopper“ са информационните системи на многонационални дружества от шест континента, в т.ч. дружества на територията на Съюза, при което е осъществен неразрешен достъп до чувствителни търговски данни, довел до значителни икономически загуби. „Операция Cloud Hopper“ е дело на извършител, известен в публичното пространство като „APT10“ („Advanced Persistent Threat 10“) (изв. още като „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ и „Potassium“). Huaying Haitai може да бъде свързан с APT10. Освен това за Huaying Haitai работят Gao Qiang и Zhang Shilong, които се свързват с „Операция Cloud Hopper“. Следователно Huaying Haitai се свързва с Gao Qiang и Zhang Shilong.	
2.	Chosun Expo	Известно също като: Chosen Expo; Korea Export Joint Venture Местонахождение: КНДР	Chosun Expo предоставя финансова, техническа или материална подкрепа и улеснява серия кибератаки със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави, в т.ч. кибератаките, известни в публичното пространство като „WannaCry“, кибератаките срещу полския орган за финансов надзор и Sony Pictures Entertainment, както и киберкражбата от Bangladesh Bank и опита за киберкражба от Vietnam Tien Phong Bank. „WannaCry“ предизвиква срив в информационни системи по света, като ги заразява със софтуер за изнудване и блокира достъпа до данните. Засегнати са информационни системи на дружества в Съюза, включително системи, свързани с услуги, необходими за поддържането на основни услуги и икономически дейности в държавите членки. „WannaCry“ е дело на извършител, известен в публичното пространство като „APT38“ („Advanced Persistent Threat 38“), или „Lazarus Group“. Chosun Expo може да бъде свързано с APT38/Lazarus Group, включително чрез профилите, използвани при кибератаките.	30.7.2020 г.
3.	Главен център за специални технологии (ГЦСТ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ)	Адрес: Ул. „Кирова“ № 22, Москва, Руска федерация	Главният център за специални технологии (ГЦСТ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ), известен още като „Подразделение 74455“, е отговорен за кибератаките със значително въздействие, задействани извън Съюза и представляващи външна заплаха за Съюза или неговите държави членки, и кибератаки със значително въздействие върху трети държави, в т.ч. кибератаките от юни 2017 г., известни в публичното пространство като „NotPetya“ или „EternalPetya“, и кибератаките срещу електроенергийната мрежа на Украйна през зимата на 2015/2016 г.	30.7.2020 г.

			„NotPetya“ или „EternalPetya“ прекъсват достъпа до данните на редица дружества в Съюза, в Европа като цяло и по света, като заразяват компютрите със софтуер за изнудване и блокират достъпа до данните, което освен всичко друго води до значителни икономически загуби. Кибератаката срещу електроенергийна мрежа на Украйна води до частичното ѝ изключване през зимата. „NotPetya“ или „EternalPetya“ е дело на извършител, известен в публичното пространство като „Sandworm“ (изв. още като „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ и „Telebots“). Той стои и зад атаката срещу електроенергийната мрежа на Украйна. Главният център за специални технологии към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация играе активна роля в действията в киберпространството, дело на Sandworm, и може да бъде свързан с него.	