►**B** **РЕШЕНИЕ (ОВППС) 2019/797 НА СЪВЕТА**

от 17 май 2019 година

относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

(ОВ L 129I, 17.5.2019 г., стр. 13)

Изменено със:

		Официален вестник		
		№	страница	дата
►**M1**	Решение (ОВППС) 2020/651 на Съвета от 14 май 2020 година	L 153	4	15.5.2020 г.
►**M2**	Решение (ОВППС) 2020/1127 на Съвета от 30 юли 2020 година	L 246	12	30.7.2020 г.
►**M3**	Решение (ОВППС) 2020/1537 на Съвета от 22 октомври 2020 година	L 351 I	5	22.10.2020 г.
►**M4**	Решение (ОВППС) 2020/1748 на Съвета от 20 ноември 2020 година	L 393	19	23.11.2020 г.

Поправено със:

►**C1** Поправка, ОВ L 230, 17.7.2020 г., стр. 36 (2019/797)

▼B

РЕШЕНИЕ (ОВППС) 2019/797 НА СЪВЕТА

от 17 май 2019 година

относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

Член 1

1. Настоящото решение се прилага по отношение на кибератаки със значително въздействие, включително опити за кибератаки с потенциално значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки.

2. Кибератаките, представляващи външна заплаха, включват кибератаките:

а) които водят началото си или се извършват от място извън Съюза;

б) за които се използва инфраструктура извън Съюза;

в) които се извършват от което и да било физическо или юридическо лице, образувание или орган, установено или упражняващо дейност извън Съюза; или

г) които се извършват с подкрепата, под ръководството или под контрола на физическо или юридическо лице, образувание или орган, упражняващо дейност извън Съюза.

3. За тази цел кибератаките са действия, които включват което и да било от следните:

а) достъп до информационни системи;

б) намеса в информационни системи;

в) намеса в данни; или

г) прихващане на данни,

когато тези действия не са надлежно разрешени от собственика или от друг държател на правата за системата, данните или част от тях, или когато не са разрешени съгласно правото на Съюза или на съответната държава членка.

4. Кибератаките, представляващи заплаха за държавите членки, включват кибератаки, които засягат информационните системи, свързани, наред с останалото, с:

а) критичната инфраструктура, включително подводни кабели и изстреляни в космическото пространство обекти, която е от основно значение за поддържането на жизненоважни функции на обществото или за здравето, безопасността, сигурността и икономическото или социалното благосъстояние на хората;

б) услугите, необходими за поддържането на основните обществени и/или икономически дейности, по-специално в секторите на енергетиката (електричество, петрол и газ); транспорта (въздушен, железопътен, воден и автомобилен); банковото дело; инфраструктурите на финансовия пазар; здравеопазването (доставчици на здравни услуги, болници и частни

▼B

клиники); снабдяването с питейна вода и разпределението на питейна вода; цифровата инфраструктура; и всеки друг сектор, който е от основно значение за съответната държава членка;

в) критичните функции на държавата, по-специално в сферите на отбраната, управлението и работата на институциите, включително за избори или за избирателния процес, функционирането на икономическата или гражданската инфраструктура, вътрешната сигурност и външните отношения, включително посредством дипломатическите мисии;

г) съхранението или обработката на класифицирана информация; или

д) държавните екипи за реагиране при извънредни ситуации.

5. Кибератаките представляват заплаха за Съюза, включително тези, които са насочени срещу неговите институции, органи, служби и агенции, срещу неговите делегации в трети държави или към международни организации, срещу операциите и мисиите му в рамките на общата политика за сигурност и отбрана (ОПСО) и срещу специалните му представители.

6. Когато бъде счетено за необходимо за постигане на целите на ОВППС, съдържащи се в съответните разпоредби на член 21 от Договора за Европейския съюз, ограничителните мерки съгласно настоящото решение могат да бъдат приложени и в отговор на кибератаки със значително въздействие срещу трети държави или международни организации.

Член 2

За целите на настоящото решение се използват следните определения:

а) „Информационни системи“ означава устройство или група от взаимосвързани или имащи връзка помежду си устройства, едно или повече от които, съобразно дадена програма, извършват автоматизирано обработване на цифрови данни, както и цифровите данни, съхранявани, обработвани, извличани или предавани от такова устройство или група от устройства с цел експлоатация, използване, защита и поддръжка на устройството или групата устройства;

б) „Намеса в информационна система“ означава затрудняване или прекъсване на функционирането на информационна система чрез внасяне на цифрови данни, чрез предаване, увреждане, заличаване, влошаване, изменение или скриване на такива данни или чрез премахване на достъпа до такива данни;

в) „Намеса в данни“ означава заличаване, увреждане, влошаване, изменение или скриване на цифрови данни в информационна система или премахване на достъпа до такива данни. Това включва също така кражбата на данни, финансови средства, икономически ресурси или интелектуална собственост;

г) „Прихващане на данни“ означава извършено с технически средства прихващане на непублични цифрови данни, изпращани до дадена информационна система, от нея или в нейните рамки, включително електромагнитни емисии от информационна система, пренасящи такива цифрови данни.

▼B

Член 3

Факторите, определящи дали дадена кибератака има значително въздействие съгласно посоченото в член 1, параграф 1, включват всеки един от изредените:

а) обхватът, мащабът, въздействието или сериозността на предизвиканото прекъсване, включително за икономическите и обществените дейности, основните услуги, критичните държавни функции, обществения ред или обществената безопасност;

б) броят на засегнатите физически или юридически лица, образувания или органи;

в) броят на засегнатите държави членки;

г) размерът на предизвиканата икономическа загуба, например чрез широкомащабно присвояване на средства, икономически ресурси или интелектуална собственост;

д) икономическата полза, която извършителят е извлякъл за себе си или за други;

е) размерът или естеството на откраднатите данни или мащабът на пробивите в сигурността на данните; или

ж) естеството на чувствителната търговска информация, до която е постигнат достъп.

Член 4

1. Държавите членки предприемат необходимите мерки за предотвратяване на влизането или транзитното преминаване през тяхна територия на:

а) физически лица, които са отговорни за кибератаки или опити за кибератаки;

б) физически лица, които предоставят финансова, техническа или материална подкрепа или са замесени по друг начин в кибератаки или опити за кибератаки, включително чрез планиране, подготовка, участие, ръководене, подпомагане или поощряване на такива атаки или чрез улесняването им посредством действие или бездействие;

в) физически лица, свързани с лицата по букви а) и б);

които са изброени в приложението.

2. Параграф 1 не задължава никоя държава членка да отказва на собствените си граждани да влязат на нейна територия.

3. Параграф 1 не засяга случаите, когато дадена държава членка е обвързана от задължение по международното право, а именно:

а) в качеството ѝ на приемаща държава на международна междуправителствена организация;

б) като държава домакин на международна конференция, свикана от Организацията на обединените нации или под нейната егида;

в) съгласно многостранно споразумение, предоставящо привилегии и имунитети; или

г) съгласно Договора за помирение от 1929 г. (Латерански договор), сключен от Светия престол (Ватикана) и Италия.

▼B

4. Параграф 3 се смята за приложим и в случаите, когато държава членка е домакин на Организацията за сигурност и сътрудничество в Европа (ОССЕ).

5. Съветът се информира надлежно във всеки един от случаите, когато някоя държава членка предоставя освобождаване от мерките в съответствие с параграф 3 или 4.

6. Държавите членки могат да предоставят освобождаване от мерките, наложени съгласно параграф 1, когато пътуването е обосновано от съображения, свързани със спешни хуманитарни нужди или участие в международни срещи или срещи, провеждани с подкрепата на Съюза или чийто домакин е Съюзът, или чийто домакин е държава членка, която е поела председателството на ОССЕ, на които се води политически диалог, пряко насърчаващ постигането на целите на политиката на ограничителни мерки, включително сигурността и стабилността в киберпространството.

7. Държавите членки могат също да предоставят освобождаване от мерките, наложени съгласно параграф 1, когато влизането или транзитното преминаване е необходимо за провеждането на съдебен процес.

8. Държава членка, която желае да предостави освобождаване от мерките съгласно параграф 6 или 7, уведомява Съвета за това в писмена форма. Счита се, че е предоставено освобождаване, освен ако един или няколко от членовете на Съвета не възразят в писмена форма в срок от два работни дни от получаването на уведомлението за предложеното освобождаване. В случай че един или повече от членовете на Съвета повдигнат възражение, Съветът може да реши с квалифицирано мнозинство да предостави предложеното освобождаване.

9. Когато съгласно параграфи 3, 4, 6, 7 или 8 държава членка разреши влизане или транзитно преминаване през нейна територия на лица, включени в списъка в приложението, разрешението е строго ограничено до целта, за която е дадено, и до лицата, за които се отнася пряко.

Член 5

1. Замразяват се всички финансови средства и икономически ресурси, принадлежащи на, притежавани, държани или контролирани от:

а) физически или юридически лица, образувания или органи, които са отговорни за кибератаки или опити за кибератаки;

б) физически или юридически лица, образувания или органи, които предоставят финансова, техническа или материална подкрепа или са замесени по друг начин в кибератаки или опити за кибератаки, включително чрез планиране, подготовка, участие, ръководене, подпомагане или поощряване на такива атаки или чрез улесняването им посредством действие или бездействие;

в) физически или юридически лица, образувания или органи, свързани с физическите или юридическите лица, образуванията или органите, посочени в букви а) и б);

които са изброени в приложението.

▼B

2. Никакви финансови средства или икономически ресурси не се предоставят пряко или непряко на или в полза на физическите или юридическите лица, образуванията или органите, изброени в приложението.

3. Чрез дерогация от параграфи 1 и 2, компетентните органи на държавите членки може да разрешат освобождаването на определени замразени финансови средства или икономически ресурси или предоставянето на определени финансови средства или икономически ресурси при условията, които преценят за подходящи, след като са установили, че съответните финансови средства или икономически ресурси са:

а) ►C1 необходими за задоволяването на основни нужди на физическите или юридическите лица, образуванията или органите, изброени в приложението, ◄ и на членове на семейството на издръжка на такива физически лица, включително плащания във връзка с хранителни продукти, наем или ипотека, лекарства и медицинско обслужване, данъци, застрахователни премии и такси за комунални услуги;

б) предназначени изключително за заплащането на разумни по размер хонорари за професионални услуги или за възстановяването на направени разходи, свързани с предоставени правни услуги;

в) предназначени изключително за заплащането на хонорари или такси за услуги за текущо съхранение или обслужване на замразени финансови средства или икономически ресурси;

г) необходими за плащането на извънредни разходи, при условие че най-малко две седмици преди да даде разрешение, съответният компетентен орган е уведомил компетентните органи на останалите държави членки и Комисията за съображенията, поради които смята, че следва да бъде дадено конкретното разрешение; или

д) предназначени за плащане по или от банкова сметка на дипломатическо представителство или консулска служба или на международна организация, ползваща се с имунитет съгласно международното право, доколкото тези плащания са предназначени за официални цели на дипломатическото представителство, консулската служба или международната организация.

Съответната държава членка информира останалите държави членки и Комисията за всяко разрешение, дадено съгласно настоящия параграф.

4. Чрез дерогация от параграф 1, компетентните органи на държавите членки могат да разрешат освобождаването на определени замразени финансови средства или икономически ресурси, ако са изпълнени следните условия:

а) финансовите средства или икономическите ресурси са предмет на арбитражно решение, постановено преди датата на включване в списъка в приложението на физическото или юридическо лице, образуването или органа по параграф 1, или на съдебно решение или административен акт, постановени в Съюза, или на съдебно решение, подлежащо на изпълнение в съответната държава членка, преди или след тази дата;

▼B

б) финансовите средства или икономическите ресурси ще се използват изключително за удовлетворяване на претенции, уважени с такова решение или акт или признати за основателни в такова решение, в рамките на приложимите законови и подзаконови актове, уреждащи правата на лицата, предявили тези претенции;

в) решението или актът не е в полза на физическо или юридическо лице, образувание или орган, изброени в приложението; и

г) признаването на решението или акта не противоречи на обществения ред в съответната държава членка.

Съответната държава членка информира останалите държави членки и Комисията за всяко разрешение, дадено съгласно настоящия параграф.

5. Параграф 1 не възпрепятства физически или юридически лица, образувания или органи, изброени в приложението, да извършват дължими плащания по договори, сключени от тях преди датата на включване на тези физически или юридически лица, образувания или органи в списъка в приложението, ако съответната държава членка установи, че плащанията не се получават пряко или непряко от посочени в параграф 1 физически или юридически лица, образувания или органи.

6. Параграф 2 не се прилага за добавянето към замразени сметки на:

а) лихви и други приходи по тези сметки;

б) плащания, дължими по договори, споразумения или задължения, които са сключени или възникнали преди датата, на която мерките, предвидени в параграфи 1 и 2, са започнали да се прилагат за тези сметки; или

в) плащания, дължими съгласно съдебни, административни или арбитражни решения, постановени в Съюза или изпълними в съответната държава членка,

при условие че за всички тези лихви, други приходи и плащания продължават да се прилагат мерките, предвидени в параграф 1.

Член 6

1. По предложение на държава членка или на върховния представител на Съюза по въпросите на външните работи и политиката на сигурност Съветът, като действа с единодушие, съставя и изменя списъка, поместен в приложението.

2. Съветът съобщава на засегнатите физически или юридически лица, образувания или органи посоченото в параграф 1 решение, включително основанията за включване в списъка, пряко — ако адресът е известен, или чрез публикуване на известие, като на това физическо или юридическо лице, образувание или орган се дава възможност да представи възражения.

3. Ако бъдат представени възражения или съществени нови доказателства, Съветът прави преглед на посоченото в параграф 1 решение и информира съответното физическо или юридическо лице, образувание или орган за това.

▼B

Член 7

1. В приложението се съдържат основанията за включване в списъка на физическите и юридическите лица, образуванията и органите, посочени в членове 4 и 5.

2. В приложението се съдържа информацията, необходима за идентифициране на съответните физически или юридически лица, образувания или органи, доколкото е налична. По отношение на физическите лица тази информация може да включва имена и псевдоними, дата и място на раждане, гражданство, номер на паспорта и на личната карта, пол, адрес, когато е известен, и длъжност или професия. По отношение на юридическите лица, образуванията или органите тази информация може да включва наименование, място и дата на регистрация, регистрационен номер и място на дейност.

Член 8

Не се удовлетворяват претенции във връзка с договор или сделка, чието изпълнение е засегнато, пряко или непряко, изцяло или частично, от мерките, наложени с настоящото решение, включително претенции за обезщетение или други претенции от този вид, а именно претенции за компенсация или претенции по гаранция, по-специално претенции за удължаване на срокове или плащане във връзка с обезпечение, гаранция или обезщетение, по-специално финансова гаранция или финансово обезщетение под всякаква форма, ако са предявени от:

а) посочени физически или юридически лица, образувания или органи, изброени в приложението;

б) физическо или юридическо лице, образувание или орган, които действат чрез или от името на едно от физическите или юридическите лица, образуванията или органите, посочени в буква а).

Член 9

С цел постигане на максимални резултати с мерките, предвидени в настоящото решение, Съюзът насърчава трети държави да приемат ограничителни мерки, подобни на предвидените в настоящото решение.

▼M1

Член 10

Настоящото решение се прилага до 18 май 2021 г. и подлежи на редовно преразглеждане. Действието на решението се продължава или решението се изменя, в зависимост от случая, ако Съветът прецени, че неговите цели не са постигнати.

▼B

Член 11

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

▼B

ПРИЛОЖЕНИЕ

Списък на физическите и юридическите лица, образуванията и органите, посочени в членове 4 и 5

▼M2

А. Физически лица

	Име	Идентификационни данни	Основания	Дата на вписване
▼M4				
1.	GAO Qiang	Дата на раждане: 4 октомври 1983 г. 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 е работил 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 е свързан както с Huaying Haitai, така и с Zhang Shilong.	30.7.2020 г.
2.	ZHANG Shilong	Дата на раждане: 10 септември 1981 г. Място на раждане: Китай 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.	30.7.2020 г.

▼M4

	Име	Идентификационни данни	Основания	Дата на вписване
			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“). 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 е работил 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 е свързан както с Huaying Haitai, така и с Gao Qiang.	
▼M2 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.

▼M2

	Име	Идентификационни данни	Основания	Дата на вписване
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.

▼M2

	Име	Идентификационни данни	Основания	Дата на вписване
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.

▼M3

7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Дата на раждане: 15 ноември 1990 г. Място на раждане: Kursk (Курск), РСФСР (днес Руска федерация) Гражданство: руско Пол: мъжки	Дмитрий Бадин участва в кибератака със значително въздействие срещу Германския федерален парламент (Deutscher Bundestag). В качеството си на офицер от военното разузнаване от 85-и Главен център за специални услуги (ГЦСУ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ) Дмитрий Бадин е бил част от екипа на офицерите от руското военно разузнаване, които извършиха кибератаката срещу Германския федерален парламент (Deutscher Bundestag) през април и май 2015 г. Кибератаката беше насочена срещу информационната система на парламента и наруши нейното функциониране за няколко дни. Бяха откраднати значително количество данни и бяха засегнати електронните пощи на няколко членове на парламента, както и на канцлера Ангела Меркел.	22.10.2020 г.

▼M3

	Име	Идентификационни данни	Основания	Дата на вписване
8.	Igor Olegovich KOSTYUKOV	Игор Олегович КОСТЮКОВ Дата на раждане: 21 февруари 1961 г. Гражданство: руско Пол: мъжки	Игор Костюков е настоящият началник на Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ), където преди това е служил като първи заместник-началник. Една от единиците под негово командване е 85-и Главен център за специални услуги (ГЦСУ), известен също като „военно подразделение 26165“ (известен в сектора с прозвищата: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“ и „Strontium“). В това си качество Игор Костюков е отговорен за кибератаките, извършени от ГЦСУ, включително за тези със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки. По-специално офицерите от военното разузнаване от ГЦСУ са взели участие в кибератаките срещу Германския федерален парламент (Deutscher Bundestag), извършени през април и май 2015 г., и в опита за кибератака, която е имала за цел включване в безжичната мрежа на Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия през април 2018 г. Кибератаката срещу Германския федерален парламент беше насочена срещу информационната система на парламента и наруши нейното функциониране за няколко дни. Бяха откраднати значително количество данни и бяха засегнати електронните пощи на няколко членове на парламента, както и на канцлера Ангела Меркел.	22.10.2020 г.

▼M2

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.

▼M2

	Наименование	Идентификационни данни	Основания	Дата на вписване
			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.

▼M2

	Наименование	Идентификационни данни	Основания	Дата на вписване
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. „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.	30.7.2020 г.

▼M3

4.	85-и Главен център за специални услуги (ГЦСУ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ)	Адрес: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation (Комсомольский пр., 20, Москва, 119146, Руска федерация)	85-и Главен център за специални услуги (ГЦСУ) към Главното управление на Генералния щаб на Въоръжените сили на Руската федерация (ГУ/ГРУ), известен също като „военно подразделение 26165“ (известен в сектора с прозвищата: „APT28“, „Fancy Bear“, „Sofacy Group“, „Pawn Storm“, „Strontium“), е отговорен за кибератаки със значително въздействие, които представляват външна заплаха за Съюза или за неговите държави членки.	22.10.2020 г.

▼M3

	Наименование	Идентификационни данни	Основания	Дата на вписване
			По-специално офицерите от военното разузнаване от ГЦСУ са взели участие в кибератаките срещу Германския федерален парламент (Deutscher Bundestag), извършени през април и май 2015 г., и в опита за кибератака, която е имала за цел включване в безжичната мрежа на Организацията за забрана на химическото оръжие (ОЗХО) в Нидерландия през април 2018 г. Кибератаката срещу Германския федерален парламент беше насочена срещу информационната система на парламента и наруши нейното функциониране за няколко дни. Бяха откраднати значително количество данни и бяха засегнати електронните пощи на няколко членове на парламента, както и на канцлера Ангела Меркел.	