II

(Незаконодателни актове)

РЕГЛАМЕНТИ

РЕГЛАМЕНТ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2020/1744 НА СЪВЕТА

от 20 ноември 2020 година

за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2019/796 от 17 май 2019 г., относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки ([1]), и по-специално член 13, параграф 1 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 Регламент (ЕС) 2019/796.

(2) На 30 юли 2020 г. Съветът прие Регламент за изпълнение (ЕС) 2020/1125 ([2]), с който шест физически лица и три образувания или органи бяха включени в списъка на подлежащите на ограничителни мерки физически и юридически лица, образувания и органи, посочени в приложение I към Регламент (ЕС) 2019/796.

(3) За две вписвания на физически лица беше получена актуализирана информация.

(4) Поради това Регламент (ЕС) 2019/796 следва да бъде съответно изменено,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Приложение I към Регламент (ЕС) 2019/796 се изменя в съответствие с приложението към настоящия регламент.

Член 2

Настоящият регламент влиза в сила в деня след публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 20 ноември 2020 година.

За Съвета
Председател
M. ROTH

([1]) ОВ L 129I, 17.5.2019 г., стр. 1.
([2]) Регламент за изпълнение (ЕС) 2020/1125 на Съвета от 30 юли 2020 г. за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 246, 30.7.2020 г., стр. 4).

ПРИЛОЖЕНИЕ

В приложение I към Регламент (ЕС) 2019/796, в подраздел „А. Физически лица“ вписвания 1 и 2 се заменят със следните вписвания:

	Име	Идентификационни данни	Основания	Дата на вписване
„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. 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.	30.7.2020 г.“