

Bruxelas, 10 de março de 2026
(OR. en)

5134/26

LIMITE

CORLX 10
CFSP/PESC 17
CYBER 4
JAI 21
FIN 8

ATOS LEGISLATIVOS E OUTROS INSTRUMENTOS

Assunto: DECISÃO DO CONSELHO que altera a Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros

DECISÃO (PESC) 2026/... DO CONSELHO

de ...

que altera a Decisão (PESC) 2019/797 relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado da União Europeia, nomeadamente o artigo 29.º,

Tendo em conta a proposta da alta representante da União para os Negócios Estrangeiros e a Política de Segurança,

Considerando o seguinte:

- (1) Em 17 de maio de 2019, o Conselho adotou a Decisão (PESC) 2019/797¹.
- (2) No âmbito da ação sustentada, adaptada e coordenada da União contra os responsáveis por ciberameaças persistentes, duas pessoas singulares e três entidades deverão ser incluídas na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo da Decisão (PESC) 2019/797. Essas pessoas e entidades são responsáveis ou estão envolvidas em ciberataques com um efeito significativo, que constituem uma ameaça externa para a União ou os seus Estados-Membros.
- (3) Por conseguinte, a Decisão (PESC) 2019/797 deverá ser alterada em conformidade,

ADOTOU A PRESENTE DECISÃO:

¹ Decisão (PESC) 2019/797 do Conselho, de 17 de maio de 2019, relativa a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros (JO L 129 I de 17.5.2019, p. 13, ELI: <http://data.europa.eu/eli/dec/2019/797/oj>).

Artigo 1.º

O anexo da Decisão (PESC) 2019/797 é alterado nos termos do anexo da presente decisão.

Artigo 2.º

A presente decisão entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

Feito em ...,

Pelo Conselho

O Presidente / A Presidente

ANEXO

O anexo da Decisão (PESC) 2019/797 é alterado do seguinte modo:

1) São aditadas as seguintes entradas à rubrica «A. Pessoas singulares»:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«18.	CHEN Cheng	陈诚 (grafia chinesa) Pseudónimos: Jesse Chen lengmo l3n6m0 Data de nascimento: 20.10.1984 Local de nascimento: Yancheng, Jiangsu, China Nacionalidade: chinesa Sexo: masculino	Chen Cheng é um empresário chinês, cofundador e um dos diretores gerais (diretor de operações) da Anxun Information Technology Co. Ltd. É também um representante legal da sucursal de Sichuan da empresa. A Anxun Information Technology Co. Ltd., também conhecida por i-Soon, é uma empresa sediada na República Popular da China que oferece serviços de «pirataria informática». A Anxun Information Technology Co. Ltd. atacou infraestruturas críticas e funções cruciais de um Estado de Estados-Membros e acedeu a informações classificadas, tendo-as vendido. Além disso, a Anxun Information Technology Co. Ltd. atacou governos de vários Estados terceiros, constituindo assim uma ameaça para os objetivos da política externa e de segurança comum (PESC) da União, tal como enunciados no artigo 21.º, n.º 2, alíneas a) a c), do Tratado da União Europeia. A Anxun Information Technology Co. Ltd. obtém um importante benefício económico dos serviços prestados	+

+ JO: inserir a data de entrada em vigor da presente decisão.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			<p>Por conseguinte, a Anxun Information Technology Co. Ltd. é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para a União e os seus Estados-Membros, bem como ataques contra Estados terceiros.</p> <p>Nessa qualidade, Chen Cheng é responsável e está implicado em ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como em ciberataques com um efeito significativo contra Estados terceiros.</p>	

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
19.	WU Haibo	<p>吴海波 (grafia chinesa)</p> <p>Pseudónimos: shutdown shutd0wn</p> <p>Local de nascimento: China</p> <p>Nacionalidade: chinesa</p> <p>Sexo: masculino</p>	<p>Wu Haibo é um empresário chinês, cofundador e um dos diretores gerais (diretor executivo) da Anxun Information Technology Co. Ltd. É também representante legal, presidente e diretor-geral da sucursal de Xangai («empresa-mãe») da Anxun Information Technology Co. Ltd. Para além disso, atua também como representante legal da sucursal de Sichuan dessa empresa.</p> <p>A Anxun Information Technology Co. Ltd., também conhecida por i-Soon, é uma empresa sediada na República Popular da China que oferece serviços de «pirataria informática». A Anxun Information Technology Co. Ltd. atacou infraestruturas críticas e funções cruciais de um Estado de Estados-Membros e acedeu a informações classificadas, tendo-as vendido. Além disso, a Anxun Information Technology atacou governos de vários Estados terceiros, constituindo assim uma ameaça para os objetivos da política externa e de segurança comum (PESC) da União, tal como enunciados no artigo 21.º, n.º 2, alíneas a) a c), do Tratado da União Europeia.</p> <p>A Anxun Information Technology Co. Ltd. obtém um importante benefício económico dos serviços prestados.</p>	+»;

+ JO: inserir a data de entrada em vigor da presente decisão.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			<p>Por conseguinte, a Anxun Information Technology é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como contra Estados terceiros.</p> <p>Wu Haibo esteve implicado na direção e no incentivo a tentativas de ciberataques com um efeito significativo contra Estados-Membros.</p> <p>Nessa qualidade, é responsável e está implicado em ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como em ciberataques com efeitos significativos contra Estados terceiros.</p>	

2) São aditadas as seguintes entradas à rubrica «B. Pessoas coletivas, entidades e organismos»:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (grafia chinesa) Pseudónimos: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Endereço: Fenghao East Road, Room 103, Building 6, N.º 9, Beijing Haidian District, China	A Integrity Technology Group é uma empresa de cibersegurança, sediada na República Popular da China (RPC), que facilitou ciberataques relacionados com o Advanced Persistent Threat (APT) Flax Typhoon. Esse APT usou os produtos e a tecnologia da Integrity Technology Group para levar a cabo as suas atividades de exploração de redes informáticas. Desde então, os produtos da Integrity Technology Group têm sido utilizados para comprometer e aceder a dispositivos da Internet das coisas nos Estados-Membros, em países por toda a Europa e em todo o mundo. Entre 2022 e 2023, a a Flax Typhoon acedeu a, pelo menos, 65.600 dispositivos da Internet das coisas em seis Estados-Membros usando produtos da Integrity Technology Group. Por conseguinte, os produtos e infraestruturas comerciais da Integrity Technology Group foram usados regularmente em ciberataques contra Estados-Membros e países terceiros. Consequentemente, ao afetar sistemas de informação relacionados com infraestruturas digitais, a Integrity Technology Group presta apoio técnico e material a ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros e Estados terceiros.	+

+ JO: inserir a data de entrada em vigor da presente decisão.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
		Local de registo: Pequim, China Data de registo: 2.9.2010 Código Unificado de Crédito Social: 91110108562135265P		

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
6.	Emennet Pasargad	<p>Pseudónimos: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten</p> <p>Local de registo: Teerão, Irão</p> <p>Número de registo: 554267</p> <p>Estabelecimento principal: Teerão, Irão</p>	<p>Emennet Pasargad é um interveniente (empresa) iraniano no domínio cibernético que atacou numerosas entidades, nomeadamente em Estados-Membros e nos Estados Unidos.</p> <p>Emennet Pasargad, que opera sob o pseudónimo «Anzu Team», atacou infraestruturas digitais na Suécia e comprometeu um serviço sueco de SMS, afetando um grande número de pessoas. Além disso, atuando sob o pseudónimo «Holy Souls», a entidade comprometeu a base de dados de assinantes da revista satírica francesa Charlie Hebdo, tendo-a publicitado para venda na Web obscura. Emennet Pasargad comprometeu painéis publicitários durante os Jogos Olímpicos de Paris e levou a cabo campanhas de desinformação. Emennet Pasargad tentou também interferir nas eleições presidenciais de 2020 nos Estados Unidos, ameaçando a democracia e o Estado de direito, obtendo informações confidenciais sobre os eleitores americanos e obtendo acesso não autorizado à rede informática de uma empresa de comunicação social dos Estados Unidos.</p> <p>Por conseguinte, Emennet Pasargad é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, e por ciberataques com efeitos significativos contra um Estado terceiro.</p>	+

+ JO: inserir a data de entrada em vigor da presente decisão.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
7.	Anxun Information Technology Co. Ltd	<p>安洵信息技术有限公司 (grafia chinesa)</p> <p>Pseudónimos: I-Soon</p> <p>Endereço: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai</p> <p>Código Unificado de Crédito Social: 91510105332025597A (sucursal de Sichuan)</p> <p>Código Unificado de Crédito Social: 91310116561906136G (sucursal de Xangai)</p>	<p>A Anxun Information Technology Co. Ltd. é uma empresa sediada na República Popular da China que oferece serviços de «pirataria informática». Atacou infraestruturas críticas e funções cruciais de um Estado de Estados-Membros e acedeu a informações classificadas, tendo-as vendido. Além disso, a Anxun Information Technology Co. Ltd. atacou governos de vários Estados terceiros, constituindo assim uma ameaça para os objetivos da política externa e de segurança comum (PESC) da União, tal como enunciados no artigo 21.º, n.º 2, alíneas a) a c), do Tratado da União Europeia. A Anxun Information Technology Co. Ltd. obtém um importante benefício económico dos serviços prestados.</p> <p>Por conseguinte, a Anxun Information Technology Co. Ltd. é responsável por ciberataques com efeitos significativos, que constituem uma ameaça externa para os Estados-Membros, bem como por ciberataques com efeitos significativos contra Estados terceiros.</p>	+».

+ JO: inserir a data de entrada em vigor da presente decisão.

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
		<p>Sítio Web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win</p> <p>Números de telefone: +862161119992, +8605645893417, +8613761671735, +864000665915</p> <p>Endereço eletrónico: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net</p>		

PUBLIC