2025/887

13.5.2025

DECISÃO (PESC) 2025/887 DO CONSELHO

de 12 de maio de 2025

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) 2019/797 ([1]).

(2) A Decisão (PESC) 2019/797 é aplicável até 18 de maio de 2025. Com base numa reapreciação dessa decisão, o Conselho considera que a sua aplicação deverá ser prorrogada até 18 de maio de 2028.

(3) Com base numa reapreciação do anexo da Decisão (PESC) 2019/797, a aplicação das medidas previstas nos artigos 4.º e 5.º dessa decisão relativamente às pessoas singulares e coletivas, entidades e organismos enumerados nesse anexo deverá ser prorrogada até 18 de maio de 2026. Além disso, deverão ser atualizados os motivos da inclusão de seis pessoas na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas.

(4) A Decisão (PESC) 2019/797deverá, pois, ser alterada em conformidade,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

A Decisão (PESC) 2019/797 é alterada do seguinte modo:

1) O artigo 10.º passa a ter a seguinte redação:

«*Artigo 10.º*

A presente decisão é aplicável até 18 de maio de 2028 e fica sujeita a reapreciação permanente. As medidas previstas nos artigos 4.º e 5.º aplicam-se até 18 de maio de 2026 às pessoas singulares e coletivas, entidades e organismos que figuram no anexo.»;

2) O anexo é alterado em conformidade com o anexo da presente decisão.

Artigo 2.º

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

Feito em Bruxelas, em 12 de maio de 2025.

Pelo Conselho

A Presidente

B. NOWACKA

([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).

ANEXO

No anexo da Decisão (PESC) 2019/797, na secção «A. Pessoas singulares», as entradas 3 a 8 passam a ter a seguinte redação:

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
«3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data de nascimento: 27.5.1972 Local de nascimento: Oblast de Perm, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 120017582 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17.4.2017 a 17.4.2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Alexey Minin participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos, e em ciberataques com um efeito significativo contra Estados terceiros. Como agente de apoio em matéria de informações humanas da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Alexey Minin fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede *wi-fi* da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede *wi-fi* da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (Militaire Inlichtingen- en Veiligheidsdienst) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ. Um grande júri do Tribunal do Distrito Ocidental da Pensilvânia (Estados Unidos da América) acusou Alexey Minin, enquanto agente da GRU, de pirataria informática, fraude com recurso a meios de comunicação eletrónica, roubo de identidade agravado e branqueamento de capitais. A GRU continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Enquanto membro da GRU, Alexey Minin está, portanto, envolvido em ciberataques com um efeito significativo, nomeadamente tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data de nascimento: 31.7.1977 Local de nascimento: Oblast de Murmanskaya, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 100135556 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17.4.2017 a 17.4.2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Aleksei Morenets participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos, e em ciberataques com um efeito significativo contra Estados terceiros. Como "ciberoperador" da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Aleksei Morenets fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede *wi-fi* da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede *wi-fi* da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (Militaire Inlichtingen- en Veiligheidsdienst) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ. Um grande júri do Tribunal do Distrito Ocidental da Pensilvânia (Estados Unidos da América) acusou Aleksei Morenets, enquanto membro da Unidade Militar 26165, de pirataria informática, fraude com recurso a meios de comunicação eletrónica, roubo de identidade agravado e branqueamento de capitais. A GRU continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Enquanto membro da GRU, Aleksei Morenets está, portanto, envolvido em ciberataques com um efeito significativo, nomeadamente tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data de nascimento: 26.7.1981 Local de nascimento: Kursk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 100135555 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17.4.2017 a 17.4.2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Evgenii Serebriakov participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos, e em ciberataques com um efeito significativo contra Estados terceiros. Como "ciberoperador" da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Evgenii Serebriakov fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede *wi-fi* da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede *wi-fi* da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (Militaire Inlichtingen- en Veiligheidsdienst) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ. Desde a primavera de 2022, Evgenii Serebriakov lidera o "Sandworm" (também conhecido por "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" e "Telebots"), um grupo de intervenientes e piratas informáticos afeto à Unidade 74455 da Direção-Geral de Informações da Rússia. O Sandworm levou a cabo ciberataques contra a Ucrânia, incluindo agências governamentais ucranianas, na sequência da guerra de agressão da Rússia contra a Ucrânia. A GRU continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Enquanto membro da GRU, Evgenii Serebriakov está, portanto, envolvido em ciberataques com um efeito significativo, nomeadamente tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros.	30.7.2020

ELI: http://data.europa.eu/eli/dec/2025/887/oj

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data de nascimento: 24.8.1972 Local de nascimento: Ulyanovsk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Número de passaporte: 120018866 Emitido por: Ministério dos Negócios Estrangeiros da Federação da Rússia Validade: de 17.4.2017 a 17.4.2022 Localização: Moscovo, Federação da Rússia Nacionalidade: russa Sexo: masculino	Oleg Sotnikov participou numa tentativa de ciberataque com um efeito potencialmente significativo contra a Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos, e em ciberataques com um efeito significativo contra Estados terceiros. Como agente de apoio em matéria de informações humanas da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Oleg Sotnikov fez parte de uma equipa de quatro agentes de informações militares russos que tentaram obter acesso não autorizado à rede *wi-fi* da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede *wi-fi* da OPAQ, o que, a ter acontecido, teria comprometido a segurança da rede e os trabalhos de investigação em curso na OPAQ. O Serviço de Segurança e Informações de Defesa dos Países Baixos (Militaire Inlichtingen- en Veiligheidsdienst) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ. Um grande júri do Tribunal do Distrito Ocidental da Pensilvânia (Estados Unidos da América) acusou Oleg Sotnikov, enquanto agente da GRU, de pirataria informática, fraude com recurso a meios de comunicação eletrónica, roubo de identidade agravado e branqueamento de capitais. A GRU continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Enquanto membro da GRU, Oleg Sotnikov está, portanto, envolvido em ciberataques com um efeito significativo, nomeadamente tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros.	30.7.2020

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data de nascimento: 15.11.1990 Local de nascimento: Kursk, República Socialista Federativa Soviética da Rússia (atualmente Federação da Rússia) Nacionalidade: russa Sexo: masculino	Dmitry Badin participou num ciberataque com um efeito significativo contra o Parlamento Federal alemão (Deutscher Bundestag) e em ciberataques com um efeito significativo contra Estados terceiros. Enquanto agente dos serviços de informação militares do 85.º Centro Principal de Serviços Especiais (GTsSS) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), Dmitry Badin fez parte de uma equipa de agentes dos serviços de informações militares russos que lançaram um ataque contra o Parlamento Federal alemão em abril e maio de 2015. O referido ciberataque visou o sistema informático do Parlamento Federal alemão e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da antiga chanceler federal Angela Merkel. Um grande júri do Tribunal do Distrito Ocidental da Pensilvânia (Estados Unidos da América) acusou Dmitry Badin, enquanto membro da Unidade Militar 26165, de pirataria informática, fraude com recurso a meios de comunicação eletrónica, roubo de identidade agravado e branqueamento de capitais. A GRU continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Enquanto membro da GRU, Dmitry Badin está, portanto, envolvido em ciberataques com um efeito significativo, nomeadamente tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros.	22.10.2020

ELI: http://data.europa.eu/eli/dec/2025/887/oj

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data de nascimento: 21.2.1961 Nacionalidade: russa Sexo: masculino	Igor Kostyukov é o atual chefe da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), tendo anteriormente ocupado o cargo de primeiro chefe adjunto. Uma das unidades sob o seu comando é o 85.º Centro Principal de Serviços Especiais (GTsSS) (t.c.p. "unidade militar 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" e "Strontium"). No exercício desse cargo, Igor Kostyukov é responsável por ciberataques lançados pelo GTsSS, incluindo ataques com um efeito significativo que constituem uma ameaça externa para a União ou para os seus Estados-Membros. Mais especificamente, agentes de informações militares do GTsSS participaram no ciberataque contra o Parlamento Federal alemão (Deutscher Bundestag) de abril e maio de 2015, bem como na tentativa de ciberataque que visou piratear a rede Wi-Fi da Organização para a Proibição de Armas Químicas (OPAQ) ocorrida em abril de 2018, nos Países Baixos. O ciberataque contra o Parlamento Federal alemão visou o seu sistema informático e perturbou o seu funcionamento durante vários dias. Foi roubada uma importante quantidade de dados e foram afetadas as contas de correio eletrónico de vários deputados e da antiga chanceler federal Angela Merkel. A GRU continua a levar a cabo ciberataques contra a União ou os seus Estados-Membros. Enquanto membro da GRU, Igor Kostyukov está, portanto, envolvido em ciberataques com um efeito significativo, nomeadamente tentativas de ciberataques com um efeito potencialmente significativo, que constituem uma ameaça externa para a União ou para os seus Estados-Membros	22.10.2020»