REGULAMENTO DE EXECUÇÃO (UE) 2020/1125 DO CONSELHO

de 30 de julho de 2020

que dá execução ao Regulamento (UE) 2019/796 relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para União ou os seus Estados-Membros

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2019/796 do Conselho, de 17 de maio de 2019, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para a União ou os seus Estados-Membros ([1]), nomeadamente o artigo 13.º, n.º 1,

Tendo em conta a proposta do alto-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 o Regulamento (UE) 2019/796.

(2) As medidas restritivas específicas contra os ciberataques com um efeito significativo que constituem uma ameaça externa para a União ou para os seus Estados-Membros integram as medidas incluídas no quadro da União para uma resposta diplomática conjunta às ciberatividades maliciosas (conjunto de instrumentos de ciberdiplomacia), assumindo-se como um instrumento vital para dissuadir e dar resposta a tais atividades. Podem também ser aplicadas medidas restritivas em resposta aos ciberataques com um efeito significativo contra Estados terceiros ou organizações internacionais, sempre que considerado necessário para atingir os objetivos da política externa e de segurança comum estabelecidos nas disposições pertinentes do artigo 21.º do Tratado da União Europeia.

(3) Em 16 de abril de 2018, o Conselho adotou conclusões nas quais condenou veementemente a utilização mal intencionada de tecnologias da informação e da comunicação, nomeadamente nos ciberataques conhecidos por «WannaCry» e «NotPetya», que causaram importantes prejuízos e perdas na União e não só. Em 4 de outubro de 2018, os presidentes do Conselho Europeu e da Comissão Europeia e a alta-representante da União para os Negócios Estrangeiros e a Política de Segurança («alta-representante») manifestaram, numa declaração comum, sérias preocupações sobre uma tentativa de ciberataque que visou pôr em causa a integridade da Organização para a Proibição de Armas Químicas (OPAQ), com sede nos Países Baixos, um ato de agressão que demonstrou desprezo pelo objetivo solene da OPAQ. Numa declaração feita em nome da União em 12 de abril de 2019, a alta-representante instou os intervenientes a porem termo às ciberatividades maliciosas que visam comprometer a integridade, a segurança e a competitividade económica da União, nomeadamente aos atos de roubo de propriedade intelectual possibilitado pelo ciberespaço. Tais roubos possibilitados pelo ciberespaço incluem os realizados pelo interveniente conhecido por «APT10» («Advanced Persistent Threat 10»).

(4) Neste contexto, e a fim de prevenir, desencorajar, dissuadir e responder aos continuados e crescentes casos de comportamentos maliciosos no ciberespaço, seis pessoas singulares e três entidades ou organismos deverão ser incluídos na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo I do Regulamento (UE) 2019/796. Essas pessoas e entidades são responsáveis por ciberataques ou tentativas de ciberataques, nomeadamente pela tentativa de ciberataque contra a OPAQ e pelos ciberataques conhecidos por «WannaCry» e «NotPetya», bem como por «Operation Cloud Hopper», ou participaram nesses ataques ou tentativas ou facilitaram-nos ou deram-lhes o seu apoio.

(5) Por conseguinte, o Regulamento (UE) 2019/796 deverá ser alterado em conformidade,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

O anexo I do Regulamento (UE) 2019/796 é alterado em conformidade com o anexo do presente regulamento.

([1]) JO L 129 I de 17.5.2019, p. 1.

Artigo 2.º

O presente regulamento entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 30 de julho de 2020.

Pelo Conselho
O Presidente
M. ROTH

ANEXO

As seguintes pessoas e entidades ou organismos são aditadas à lista de pessoas singulares e coletivas, entidades e organismos constante do anexo I do Regulamento (UE) 2019/796:

«A. Pessoas singulares

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
1.	GAO Qiang	Local de nascimento: Província de Shandong, China Endereço: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nacionalidade: chinesa Sexo: masculino	Zhang Shilong está envolvido na "Operation Cloud Hopper", uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A "Operação Cloud Hopper" atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. O interveniente conhecido por "APT10" ("Advanced Persistent Threat 10") (t.c.p. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") realizou a "Operation Cloud Hopper". Pode estabelecer-se uma ligação entre Zhang Shilong e o interveniente "APT10", nomeadamente através do programa malicioso que Zhang Shilong desenvolveu e testou em ligação com os ciberataques levados a cabo pelo interveniente "APT10". Além disso, a Huaying Haitai, entidade designada por apoiar e facilitar a "Operation Cloud Hopper", empregou Zhang Shilong. Zhang Shilong tem ligações a Gao Qiang, também designado pela sua ligação à "Operation Cloud Hopper". Por conseguinte, Zhang Shilong está associado à Huaying Haitai e a Gao Qiang	30.7.2020
2.	ZHANG Shilong	Endereço: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidade: chinesa Sexo: masculino	Zhang Shilong está envolvido na "Operation Cloud Hopper", uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A "Operação Cloud Hopper" atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. O interveniente conhecido por "APT10" ("Advanced Persistent Threat 10") (t.c.p. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") realizou a "Operation Cloud Hopper". Pode estabelecer-se uma ligação entre Zhang Shilong e o interveniente "APT10", nomeadamente através do programa malicioso que Zhang Shilong desenvolveu e testou em ligação com os ciberataques levados a cabo pelo interveniente "APT10". Além disso, a Huaying Haitai, entidade designada por apoiar e facilitar a "Operation Cloud Hopper", empregou Zhang Shilong. Zhang Shilong tem ligações a Gao Qiang, também designado pela sua ligação à "Operation Cloud Hopper". Por conseguinte, Zhang Shilong está associado à Huaying Haitai e a Gao Qiang.	30.7.2020

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data de nascimento: 27 de maio de 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 de abril de 2017 a 17 de abril de 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. 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 WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data de nascimento: 31 de julho de 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 de abril de 2017 a 17 de abril de 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. 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 WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data de nascimento: 26 de julho de 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 de abril de 2017 a 17 de abril de 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. 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 WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst — MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020

6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data de nascimento: 24 de agosto de 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 de abril de 2017 a 17 de abril de 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. 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 WiFi da OPAQ na Haia, nos Países Baixos, em abril de 2018. A tentativa de ciberataque visou piratear a rede WiFi 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 (DISS) (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustrou a tentativa de ciberataque, impedindo assim danos graves para a OPAQ.	30.7.2020

B. Pessoas coletivas, entidades e organismos

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Tcp Haitai Technology Development Co. Ltd Localização: Tianjin, China	A Huaying Haitai prestou apoio financeiro, técnico ou material e facilitou a "Operation Cloud Hopper", uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros. A "Operação Cloud Hopper" atacou os sistemas de informação de empresas multinacionais em seis continentes, incluindo empresas localizadas na União, e obteve acesso não autorizado a dados sensíveis do ponto de vista comercial, o que resultou em significativos prejuízos económicos. O interveniente conhecido por "APT10" ("Advanced Persistent Threat 10") (t.c.p. "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") realizou a "Operation Cloud Hopper". Pode estabelecer-se uma ligação entre a Huaying Haitai e o interveniente "APT10". Além disso, a Huaying Haitai empregou Gao Qiang e Zhang Shilong, ambos designados pela sua ligação à "Operation Cloud Hopper". Por conseguinte, a Huaying Haitai está associada a Gao Qiang e a Zhang Shilong.	30.7.2020
2.	Chosun Expo	Tcp Chosen Expo; Korea Export Joint Venture Localização: RPDC	A Chosun Expo prestou apoio financeiro, técnico ou material e facilitou uma série de ciberataques com um efeito significativo, proveniente do exterior da União e que constitui uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros, incluindo os ciberataques conhecidos por "WannaCry" e os ciberataques contra a autoridade polaca de supervisão financeira e a Sony Pictures Entertainment, bem como o roubo informático do Banco do Bangladexe e a tentativa de roubo informático do Banco Tien Phong do Vietname.	30.7.2020

			O ciberataque “WannaCry” perturbou os sistemas de informação em todo o mundo, atacando os sistemas de informação com programas sequestradores e bloqueando o acesso aos dados. Afetou os sistemas de informação de empresas na União, incluindo os sistemas de informação relativos aos serviços necessários para a manutenção de serviços essenciais e de atividades económicas nos Estados-Membros. O interveniente conhecido por “APT38” (“Advanced Persistent Threat 38”) ou o “Lazarus Group” realizaram o ciberataque “WannaCry”. Pode estabelecer-se uma ligação entre a Chosun Expo e o interveniente “APT38” e o grupo “Lazarus”, nomeadamente através das contas utilizadas para os ciberataques.	
3.	Centro Principal de Tecnologias Especiais (GTsST) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU)	Endereço: 22 Kirova Street, Moscovo, Federação da Rússia	O Centro Principal de Tecnologias Especiais (GTsST) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU), também conhecido pelo seu código postal de campanha 74455, é responsável por ciberataques com um efeito significativo, provenientes do exterior da União e que constituem uma ameaça externa para a União ou os seus Estados-Membros, e de ciberataques com um efeito significativo contra Estados terceiros, incluindo os ciberataques publicamente conhecidos por “NotPetya” ou “EternalPetya”, em junho de 2017, e os ciberataques que visaram uma rede elétrica ucraniana no inverno de 2015 e 2016. Os ciberataques “NotPetya” ou “EternalPetya” impediram o acesso aos dados em várias empresas da União, da Europa em geral e de todo o mundo, atacando os computadores com programas sequestradores e bloqueando o acesso aos dados, o que resultou, nomeadamente, em significativos prejuízos económicos. O ciberataque a uma rede de energia ucraniana teve como resultado o não funcionamento de partes da referida rede durante o inverno.	30.7.2020»
			O interveniente conhecido por “Sandworm” (t.c.p. “Sandworm Team”, “BlackEnergy Group”, “Voodoo Bear”, “Quedagh”, “Olympic Destroyer” e “Telebots”), também responsável pelo ataque à rede elétrica ucraniana, realizou os ciberataques “NotPetya” ou “EternalPetya”. O Centro Principal de Tecnologias Especiais (GTsST) da Direção-Geral de Informações do Estado-Maior-General das Forças Armadas da Federação da Rússia (GU/GRU) tem um papel ativo nas ciberatividades realizadas pelo interveniente “Sandworm”, pelo que pode estabelecer-se uma ligação entre ambos.	