Conselho da
União Europeia

Bruxelas, 13 de maio de 2024
(OR. en)

8502/24

LIMITE

CORLX 356
CFSP/PESC 512
RELEX 467
CYBER 110
JAI 572
FIN 341

ATOS LEGISLATIVOS E OUTROS INSTRUMENTOS

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

REGULAMENTO DE EXECUÇÃO (UE) 2024/… DO CONSELHO

de …

que dá execução ao Regulamento (UE) 2019/796 relativo 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 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,

[1] JO L 129 I de 17.05.2019, p. 1.

Considerando o seguinte:

(1) Em 17 de maio de 2019, o Conselho adotou o Regulamento (UE) 2019/796.

(2) Tendo em conta a persistência e o aumento de comportamentos mal-intencionados no ciberespaço, incluindo comportamentos dirigidos contra Estados terceiros, os motivos que levaram à inclusão de seis pessoas e duas entidades na lista de pessoas singulares e coletivas, entidades e organismos sujeitos a medidas restritivas constante do anexo I do Regulamento (UE) 2019/796 deverão ser atualizados.

(3) O anexo I do Regulamento (UE) 2019/796 deverá, pois, 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.

Artigo 2.º

O presente regulamento entra em vigor no dia seguinte ao 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 …, em

Pelo Conselho
O Presidente / A Presidente

ANEXO

O Anexo I do Regulamento (UE) 2019/796 («Lista de pessoas singulares e coletivas, entidades e organismos a que se refere o artigo 3.º») é alterado do seguinte modo:

1) Na lista que tem por título «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 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 (*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 oficial da Direção-Geral de Informações da Rússia(GRU), de pirataria informática, fraude com recurso a meios de comunicação eletrónica, roubo de identidade agravado e branqueamento de capitais.	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 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 (*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.	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 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 (*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.	30.7.2020

	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 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 (*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 acusou Oleg Sotnikov, enquanto oficial da Direção-Geral de Informações da Rússia (GRU), de pirataria informática, fraude com recurso a meios de comunicação eletrónica, roubo de identidade agravado e branqueamento de capitais.	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 do Estado-Maior 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.	22.10.2020

	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 do Estado-Maior 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.	22.10.2020»;

2) Na lista que tem por título «B. Pessoas coletivas, entidades e organismos», as entradas 3 e 4 passam a ter a seguinte redação:

	Nome	Elementos de identificação	Motivos
«3.	*Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)* [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: Endereço: 22 Kirova Street, Moscow, 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, está envolvido em 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 em 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.

	Nome	Elementos de identificação	Motivos
			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 Sandworm levou a cabo ciberataques contra a Ucrânia, incluindo agências governamentais ucranianas e infraestruturas críticas ucranianas, na sequência da guerra de agressão da Rússia contra a Ucrânia. Esses ciberataques incluem campanhas de ciberiscagem personalizada, ataques com *software* mal-intencionado e *software* de sequestro. 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.

	Nome	Elementos de identificação	Motivos
4.	*85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)* [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)]	Endereço: Komsomol'skiy Prospekt, 20, Moscow, 119146, Federação da Rússia	O 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) (t.c.p. "unidade militar 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" e "Strontium"), está envolvido em ciberataques com um efeito significativo e que constituem uma ameaça externa para a União ou os seus Estados-Membros e em ciberataques com um efeito significativo contra Estados terceiros. 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. Na sequência da guerra de agressão da Rússia contra a Ucrânia, foram levados a cabo pelo GTsSS ciberataques (ciberiscagem personalizada e ataques baseados em *software* mal-intencionado) contra a Ucrânia.