►B

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 129I de 17.5.2019, p. 13)

Alterada por:

		Jornal Oficial		
		n.º	página	data
►M1	Decisão (PESC) 2020/651 do Conselho de 14 de maio de 2020	L 153	4	15.5.2020
►M2	Decisão (PESC) 2020/1127 do Conselho de 30 de julho de 2020	L 246	12	30.7.2020
►M3	Decisão (PESC) 2020/1537 do Conselho de 22 de outubro de 2020	L 351 I	5	22.10.2020

Retificada por:

►C1	Retificação, JO L 230 de 17.7.2020, p. 36 (2019/797)

▼B

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

Artigo 1.º

1. A presente decisão aplica-se aos ciberataques com um efeito significativo, nomeadamente a tentativas de ciberataques com um efeito potencialmente significativo, que constituam uma ameaça externa para a União ou para os seus Estados-Membros.

2. Os ciberataques que constituem uma ameaça externa incluem os que:

a) tenham origem no exterior da União ou sejam realizados a partir do exterior da União;

b) façam uso de infraestruturas fora da União;

c) sejam realizados por qualquer pessoa singular ou coletiva, entidade ou organismo estabelecido ou que opere fora da União; ou

d) sejam realizados com o apoio, sob a direção ou sob o controlo de qualquer pessoa singular ou coletiva, entidade ou organismo que opere fora da União.

3. Para este efeito, consideram-se ciberataques as ações que envolvam qualquer das seguintes ações:

a) acesso aos sistemas de informação;

b) interferência nos sistemas de informação;

c) interferência nos dados; ou

d) interceção de dados,

se essas ações não forem devidamente autorizadas pelo proprietário ou por outro titular dos direitos do sistema ou dos dados, ou de parte deles, ou não forem permitidas pelo direito da União ou do Estado-Membro em causa.

4. Os ciberataques que constituem uma ameaça aos Estados-Membros incluem os que afetam os sistemas de informação relacionados, nomeadamente, com:

a) infraestruturas críticas, incluindo cabos submarinos e objetos lançados no espaço extra-atmosférico, essenciais para a manutenção de funções vitais da sociedade, da saúde, da segurança e do bem-estar económico e social das pessoas;

b) serviços necessários para a manutenção de atividades sociais e/ou económicas essenciais, em especial nos setores da energia (eletricidade, petróleo e gás); dos transportes (aéreos, ferroviários, por água e rodoviários); da banca; das infraestruturas do mercado financeiro;

▼B

da saúde (prestadores de cuidados de saúde, hospitais e clínicas privadas); do fornecimento e distribuição de água potável; das infraestruturas digitais; e qualquer outro setor que seja essencial para o Estado-Membro em causa;

c) funções cruciais de um Estado, em especial nos domínios da defesa, da governação e do funcionamento das instituições, nomeadamente em eleições públicas ou no processo de votação, do funcionamento das infraestruturas económicas e civis, da segurança interna e as relações externas, nomeadamente nas missões diplomáticas;

d) o armazenamento ou o tratamento de informações classificadas; ou

e) equipas da administração pública de resposta a emergências.

5. Os ciberataques que constituem uma ameaça à União incluem os perpetrados contra as suas instituições, órgãos, organismos e agências, as suas delegações em países terceiros ou organizações internacionais, as suas operações e missões da política comum de segurança e defesa (PCSD) e os seus representantes especiais.

6. Sempre que for considerado necessário para atingir os objetivos da PESC nas disposições pertinentes do artigo 21.º do Tratado da União Europeia, podem ser aplicadas medidas restritivas nos termos da presente decisão em resposta aos ciberataques com um efeito significativo contra Estados terceiros ou organizações internacionais.

Artigo 2.º

Para efeitos da presente decisão, entende-se por:

a) «Sistemas de informação», um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados digitais, bem como de dados digitais armazenados, tratados, extraídos ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção;

b) «Interferência no sistema de informação», o impedimento ou interrupção do funcionamento de um sistema de informação introduzindo dados digitais, transmitindo, danificando, apagando, deteriorando, alterando ou suprimindo esses dados, ou tornando-os inacessíveis;

c) «Interferência nos dados», a eliminação, danificação, deterioração, alteração ou supressão de dados digitais de um sistema de informação, ou o impedimento do acesso a esses dados. Esta definição inclui igualmente o furto de dados, de fundos, de recursos económicos ou de propriedade intelectual.

d) «Interceção de dados», a interceção, através de meios técnicos, das transmissões não públicas de dados digitais para, a partir de ou no interior de um sistema de informação, incluindo as emissões eletromagnéticas de um sistema de informação que transmita esses dados digitais;

▼B

Artigo 3.º

Os fatores que determinam se um ciberataque tem um efeito significativo, tal como referido no artigo 1.º, n.º 1, incluem qualquer um dos seguintes elementos:

a) o âmbito, a dimensão, o impacto ou a gravidade da perturbação causada, nomeadamente sobre as atividades económicas e societais, os serviços essenciais, as funções cruciais do Estado, a ordem pública ou a segurança pública;

b) o número de pessoas singulares ou coletivas, entidades ou organismos afetados;

c) o número de Estados-Membros afetados;

d) a escala das perdas económicas causadas, por exemplo, com a apropriação, em grande escala, de fundos, recursos económicos ou propriedade intelectual;

e) os benefícios económicos obtidos pelo infrator para si próprio ou para terceiros;

f) a quantidade ou a natureza dos dados furtados ou a dimensão das violações de dados; ou

g) a natureza dos dados comercialmente sensíveis a que se teve acesso.

Artigo 4.º

1. Os Estados-Membros tomam as medidas necessárias para prevenir a entrada nos seus territórios, ou o trânsito através deles:

a) das pessoas singulares que são responsáveis por ciberataques ou tentativas de ciberataques;

b) das pessoas singulares que prestem assistência financeira, técnica ou material ou estejam de qualquer outro modo envolvidas em ciberataques ou tentativas de ciberataques, nomeadamente planeando tais ataques, preparando-os, participando neles, dirigindo-os, prestando assistência na sua execução ou incentivando-os [ou tornando-os possíveis, por ação ou omissão];

c) das pessoas singulares associadas às pessoas abrangidas pelas alíneas a) e b),

cujos nomes figuram na lista reproduzida em anexo.

2. O n.º 1 não obriga os Estados-Membros a recusarem a entrada dos seus próprios nacionais no seu território.

3. O n.º 1 não prejudica os casos em que um Estado-Membro esteja sujeito a uma obrigação de direito internacional, a saber:

a) enquanto país anfitrião de uma organização intergovernamental internacional;

b) enquanto país anfitrião de uma conferência internacional organizada pelas Nações Unidas ou sob os auspícios desta;

c) nos termos de um acordo multilateral que confira privilégios e imunidades; ou

d) nos termos do Tratado de Latrão, de 1929, celebrado entre a Santa Sé (Estado da Cidade do Vaticano) e a Itália.

▼B

4. Considera-se que o n.º 3 se aplica também nos casos em que um Estado-Membro seja o país anfitrião da Organização para a Segurança e a Cooperação na Europa (OSCE).

5. O Conselho deve ser devidamente informado em todos os casos em que um Estado-Membro conceda uma isenção ao abrigo do n.º 3 ou 4.

6. Os Estados-Membros podem conceder isenções das medidas impostas nos termos do n.º 1 caso a viagem se justifique por razões humanitárias urgentes ou para efeitos de participação em reuniões intergovernamentais e reuniões promovidas ou organizadas pela União, ou organizadas por um Estado-Membro que exerça a presidência da OSCE, em que se desenvolva um diálogo político que promova diretamente os objetivos políticos das medidas restritivas, incluindo a segurança e a estabilidade no ciberespaço.

7. Os Estados-Membros podem também conceder isenções às medidas impostas nos termos do n.º 1, caso a entrada ou o trânsito se justifiquem para efeitos de processo judicial.

8. Os Estados-Membros que desejem conceder as isenções previstas no n.º 6 ou 7 informam o Conselho por escrito. Considera-se concedida a isenção se um ou mais membros do Conselho não levantarem objeções por escrito no prazo de dois dias úteis a contar da receção da notificação da isenção proposta. Caso um ou mais membros do Conselho levantem objeções, o Conselho, deliberando por maioria qualificada, pode decidir conceder a isenção proposta.

9. Caso, nos termos do n.º 3, 4, 6, 7 ou 8, um Estado-Membro autorize a entrada ou o trânsito no seu território de pessoas incluídas na lista do anexo, a autorização fica estritamente limitada à finalidade para que foi concedida e às pessoas a que diga diretamente respeito.

Artigo 5.º

1. São congelados todos os fundos e recursos económicos que sejam propriedade, estejam na posse ou se encontrem à disposição ou sob controlo:

a) das pessoas singulares ou coletivas, entidades ou organismos que são responsáveis por ciberataques ou tentativa de ciberataques;

b) das pessoas singulares ou coletivas, entidades ou organismos que prestem apoio financeiro, técnico ou material ou estejam de qualquer outro modo envolvidos em ciberataques ou em tentativas de ciberataques, nomeadamente planeando tais ataques, preparando-os, participando neles, dirigindo-os, prestando assistência na execução ou incentivando-os [ou tornando-os possíveis, por ação ou omissão];

c) das pessoas singulares ou coletivas, entidades ou organismos associados às pessoas singulares ou coletivas, entidades ou organismos abrangidos pelas alíneas a) e b),

cujos nomes figuram na lista reproduzida em anexo.

▼B

2. É proibido colocar, direta ou indiretamente, fundos ou recursos económicos à disposição das pessoas singulares ou coletivas, entidades ou organismos incluídos na lista do anexo, ou disponibilizá-los em seu benefício.

3. Em derrogação do disposto nos n.os 1 e 2, as autoridades competentes de um Estado-Membro podem autorizar o desbloqueamento de determinados fundos ou recursos económicos congelados ou a disponibilização de determinados fundos ou recursos económicos, nas condições que considerem adequadas, após terem determinado que os fundos ou recursos económicos em causa:

a) ►C1 são necessários para satisfazer as necessidades básicas das pessoas singulares ou coletivas, entidades ou organismos incluídos na lista do anexo ◄ e dos familiares dependentes das pessoas singulares em causa, incluindo os pagamentos de géneros alimentícios, rendas ou empréstimos hipotecários, medicamentos e tratamentos médicos, impostos, apólices de seguro e serviços públicos;

b) se destinam exclusivamente ao pagamento de honorários profissionais razoáveis ou ao reembolso de despesas associadas à prestação de serviços jurídicos;

c) se destinam exclusivamente ao pagamento de encargos ou taxas de serviço correspondentes à manutenção ou gestão normal de fundos ou recursos económicos congelados;

d) são necessários para cobrir despesas extraordinárias, desde que a autoridade competente pertinente tenha comunicado às autoridades competentes dos outros Estados-Membros e à Comissão, pelo menos duas semanas antes da concessão da autorização, os motivos por que considera que deve ser concedida uma autorização específica; ou

e) Devem ser creditados ou debitados numa conta de uma missão diplomática ou consular ou de uma organização internacional que goze de imunidades de acordo com o direito internacional, desde que esses pagamentos se destinem a ser utilizados para fins oficiais da missão diplomática ou consular ou da organização internacional.

O Estado-Membro em causa informa os restantes Estados-Membros e a Comissão sobre as autorizações concedidas nos termos do presente número.

4. Em derrogação do n.º 1, as autoridades competentes dos Estados-Membros podem autorizar o desbloqueamento de determinados fundos ou recursos económicos congelados, se estiverem preenchidas as seguintes condições:

a) os fundos ou recursos económicos são objeto de uma decisão arbitral proferida antes da data em que a pessoa singular ou coletiva, entidade ou organismo a que se refere o n.º 1 foram incluídos na lista do anexo, ou de uma decisão judicial ou administrativa proferida na União ou de uma decisão judicial executória no Estado-Membro em causa, anterior ou posterior a essa data;

▼B

b) os fundos ou recursos económicos serão exclusivamente utilizados para satisfazer créditos garantidos por tal decisão ou por ela reconhecidos como válidos, nos limites fixados pelas disposições legislativas e regulamentares que regem os direitos dos titulares desses créditos;

c) o beneficiário da decisão não é uma das pessoas singulares ou coletivas, entidades ou organismos incluídos na lista do anexo; e

d) o reconhecimento da decisão não é contrário à ordem pública no Estado-Membro em causa.

O Estado-Membro em causa informa os restantes Estados-Membros e a Comissão sobre as autorizações concedidas nos termos do presente número.

5. O n.º 1 não impede que as pessoas singulares ou coletivas, entidades ou organismos incluídos na lista constante do anexo efetuem pagamentos devidos por força de contratos celebrados antes da data em que nela foram incluídos, desde que o Estado-Membro em causa tenha determinado que o pagamento não é recebido, direta ou indiretamente, por uma das pessoas singulares ou coletivas, entidades ou organismos referidos no n.º 1.

6. O n.º 2 não é aplicável ao crédito em contas congeladas de:

a) juros ou outros rendimentos dessas contas;

b) pagamentos devidos nos termos de contratos ou acordos celebrados ou de obrigações contraídas antes da data em que essas contas ficaram sujeitas às medidas previstas nos n.ºs 1 e 2; ou

c) pagamentos devidos por força de decisões judiciais, administrativas ou arbitrais proferidas na União ou executórias no Estado-Membro em causa;

desde que os referidos juros, outros rendimentos e pagamentos continuem sujeitos às medidas previstas no n.º 1.

Artigo 6.º

1. O Conselho, deliberando por unanimidade sob proposta de um Estado-Membro ou do alto representante da União para os Negócios Estrangeiros e a Política de Segurança, elabora a lista constante do anexo e altera-a.

2. O Conselho comunica a decisão referida no n.º 1, incluindo os motivos que fundamentam a sua inclusão na lista, à pessoa singular ou coletiva, entidade ou organismo em causa, quer diretamente, se o seu endereço for conhecido, quer através da publicação de um aviso, dando-lhe a oportunidade de apresentar as suas observações.

3. Caso sejam apresentadas observações ou novos elementos de prova substanciais, o Conselho reaprecia a decisão referida no n.º 1 e informa do facto a pessoa singular ou coletiva, entidade ou organismo em causa.

▼B

Artigo 7.º

1. O anexo contém os motivos para a inclusão na lista das pessoas singulares e coletivas, entidades e organismos referidos nos artigos 4.º e 5.º.

2. O anexo contém, sempre que estejam disponíveis, as informações necessárias para identificar as pessoas singulares ou coletivas, as entidades e os organismos em causa. Essas informações podem compreender, no que se refere às pessoas singulares, o nome e os pseudónimos, a data e o local de nascimento, a nacionalidade, os números do passaporte e do bilhete de identidade, o sexo, o endereço, se for conhecido, e as funções ou a profissão exercidas. Tratando-se de pessoas coletivas, entidades ou organismos, essas informações podem incluir o nome, o local e a data de registo, o número de registo e o local da atividade.

Artigo 8.º

Não é satisfeito qualquer pedido relacionado com contratos ou transações cuja execução tenha sido afetada, direta ou indiretamente, total ou parcialmente, pelas medidas impostas ao abrigo da presente decisão, incluindo pedidos de indemnização ou qualquer outro pedido desse tipo, tais como um pedido de compensação ou um pedido ao abrigo de uma garantia, em especial um pedido de prorrogação ou de pagamento de uma garantia ou contragarantia, nomeadamente financeira, independentemente da forma que assuma, se for apresentado por:

a) pessoas singulares ou coletivas, entidades ou organismos designados incluídos na lista do anexo;

b) pessoas singulares ou coletivas, entidades ou organismos que atuem por intermédio ou em nome das pessoas singulares ou coletivas, entidades ou organismos referidos na alínea a).

Artigo 9.º

Para que o impacto das medidas estabelecidas na presente decisão seja o maior possível, a União incentiva os Estados terceiros a adotarem medidas restritivas semelhantes às previstas na presente decisão.

▼M1

Artigo 10.º

A presente decisão é aplicável até 18 de maio de 2021 e fica sujeita a reapreciação permanente. É prorrogada ou alterada, consoante necessário, se o Conselho considerar que os seus objetivos não foram atingidos.

▼B

Artigo 11.º

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

▼B

ANEXO

Lista de pessoas singulares e coletivas, entidades e organismos referidos nos artigos 4.º e 5.º

▼M2

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.	30.7.2020

▼M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			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.	
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 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

▼M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
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

▼M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
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

▼M3

7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data de nascimento: 15 de novembro de 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 efeitos importantes contra o Parlamento Federal alemão (*Deutscher Bundestag*). 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 (*Deutscher Bundestag*) 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 chanceler federal, Angela Merkel.	22.10.2020

▼M3

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data de nascimento: 21 de fevereiro de 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), também chamada «unidade militar 26165» (outros nomes por que é conhecida no setor da cibersegurança: «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 efeitos importantes 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 destinado a 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 chanceler federal, Angela Merkel.	22.10.2020

▼M2

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.	30.7.2020

▼M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			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.	
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. 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.	30.7.2020

▼M2

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
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. 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.	30.7.2020
▼M3				
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]	Endereço: Komsomol'skiy Prospekt, 20, Moscovo, 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), também chamada «unidade militar 26165» (outros nomes por que é conhecida no setor da cibersegurança: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» e «Strontium»), é responsável por ciberataques com efeitos importantes que constituem uma ameaça externa para a União ou para os seus Estados-Membros.	22.10.2020

▼M3

	Nome	Elementos de identificação	Motivos	Data de inclusão na lista
			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 destinado a 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 chanceler federal, Angela Merkel.	