►**B**

DECISIÓN (PESC) 2019/797 DEL CONSEJO

de 17 de mayo de 2019

relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

(DO L 129I de 17.5.2019, p. 13)

Modificada por:

		Diario Oficial		
		nº	página	fecha
►**M1**	Decisión (PESC) 2020/651 del Consejo de 14 de mayo de 2020	L 153	4	15.5.2020
►**M2**	Decisión (PESC) 2020/1127 del Consejo de 30 de julio de 2020	L 246	12	30.7.2020
►**M3**	Decisión (PESC) 2020/1537 del Consejo de 22 de octubre de 2020	L 351 I	5	22.10.2020

Rectificada por:

►**C1** Rectificación, DO L 230 de 17.7.2020, p. 36 (2019/797)

▼B

DECISIÓN (PESC) 2019/797 DEL CONSEJO

de 17 de mayo de 2019

relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

Artículo 1

1. La presente Decisión se aplica a los ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto significativo potencial, que constituyan una amenaza externa para la Unión o para sus Estados miembros.

2. Entre los ciberataques que constituyen una amenaza externa se incluyen aquellos que:

a) se originen, o se cometan, desde el exterior de la Unión;

b) utilicen infraestructura fuera de la Unión;

c) hayan sido cometidos por una persona física o jurídica, una entidad o un organismo establecidos o que tengan actividad fuera de la Unión; o

d) hayan sido cometidos con el apoyo, bajo la dirección o bajo el control de una persona física o jurídica que tenga actividad fuera de la Unión.

3. A tal fin, los ciberataques son acciones que implican cualesquiera de los siguientes elementos:

a) acceso a sistemas de información;

b) intromisión en sistemas de información;

c) intromisión en datos; o

d) interceptación de datos,

cuando dichas acciones no estén debidamente autorizadas por el propietario o por otro titular de derechos del sistema o de datos o de parte del mismo, o no estén permitidas por el Derecho de la Unión o de un Estado miembro.

4. Entre los ciberataques que constituyen una amenaza para los Estados miembros se incluyen los que afecten a los sistemas de información relacionados, entre otros aspectos, con:

a) las infraestructuras críticas, incluidos los cables submarinos y los objetos lanzados al espacio ultraterrestre, que resulten esenciales para el mantenimiento de funciones vitales de la sociedad, o para la salud, la seguridad, la protección y el bienestar económico o social de las personas;

b) los servicios necesarios para el mantenimiento de actividades sociales o económicas esenciales, especialmente en los sectores de la energía (electricidad, petróleo y gas); el transporte (aéreo, ferroviario,

▼B

fluvial o marítimo y por carretera); la actividad bancaria; las infraestructuras de los mercados financieros; el sector sanitario (proveedores de asistencia sanitaria, hospitales y clínicas privadas); el suministro y la distribución de agua potable; las infraestructuras digitales; o cualquier otro sector que resulte esencial para el Estado miembro de que se trate;

c) las funciones vitales del Estado, en particular en los ámbitos de la defensa, la gobernanza y el funcionamiento de las instituciones, incluido en el caso de las elecciones públicas o los procesos electorales, el funcionamiento de las infraestructuras económicas y civiles, la seguridad interior, y las relaciones exteriores, también a través de las misiones diplomáticas;

d) el almacenamiento o el tratamiento de información clasificada; o

e) los equipos de respuesta de emergencia del Estado.

5. Los ciberataques que constituyen una amenaza para la Unión incluirán los cometidos contra sus instituciones, órganos y organismos, sus delegaciones en terceros países o ante organizaciones internacionales, sus operaciones y misiones de la política común de seguridad y defensa (PCSD) y sus representantes especiales.

6. Cuando se estimen necesarias para el cumplimiento de los objetivos de la PESC en las disposiciones pertinentes del artículo 21 del Tratado de la Unión Europea, también podrán aplicarse medidas restrictivas con arreglo a la presente Decisión en respuesta a ciberataques que tengan un efecto significativo contra terceros Estados u organizaciones internacionales.

Artículo 2

A efectos de la presente Decisión, se entenderá por:

1) «Sistemas de información»: todo aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos digitales, así como los datos digitales almacenados, tratados, recuperados o transmitidos por dicho aparato o grupo de aparatos para su funcionamiento, utilización, protección y mantenimiento.

2) «Intromisión en sistemas de información»: obstaculización o interrupción del funcionamiento de un sistema de información introduciendo datos digitales, transmitiendo, dañando, borrando, deteriorando, alterando o suprimiendo tales datos, o haciéndolos inaccesibles.

3) «Intromisión en datos»: borrado, dañado, deterioro, alteración o supresión de los datos digitales en un sistema de información, o inutilización del acceso a estos datos. También incluirá el robo de datos, fondos, recursos económicos o propiedad intelectual.

4) «Interceptación de datos»: interceptación, por medios técnicos, de transmisiones no públicas de datos digitales con origen o destino en un sistema de información o realizadas en el interior de un sistema de información, incluidas las emisiones electromagnéticas de un sistema de información que contenga dichos datos digitales.

▼B

Artículo 3

Los factores que determinan si un ciberataque tiene un efecto significativo a que se refiere el artículo 1, apartado 1, incluirán cualesquiera de los siguientes elementos:

a) el alcance, la escala, la repercusión, o la gravedad de la perturbación ocasionada, incluido en las actividades económicas y sociales, los servicios esenciales, las funciones vitales del Estado, el orden público o la seguridad pública;

b) el número de personas físicas o jurídicas, entidades u organismos afectados;

c) el número de Estados miembros afectados;

d) el importe de las pérdidas económicas ocasionadas, por ejemplo mediante un robo a gran escala de fondos, recursos económicos o propiedad intelectual;

e) los beneficios económicos obtenidos por el autor, para sí o para otros;

f) la cantidad o la naturaleza de los datos sustraídos o la magnitud de las violaciones de datos; o

g) la naturaleza de los datos comercialmente sensibles a los que se haya tenido acceso.

Artículo 4

1. Los Estados miembros adoptarán las medidas necesarias para impedir la entrada o tránsito por sus territorios de las personas físicas:

a) las personas físicas que sean responsables de los ciberataques o intentos de ciberataques;

b) las personas físicas que presten ayuda financiera, técnica o material o que estén implicadas de alguna otra forma en ciberataques o tentativas de ciberataque, en particular mediante la planificación, preparación, dirección o fomento de dichos ataques, así como la participación en ellos o la ayuda a su comisión [o la facilitación de su comisión por acción u omisión];

c) las personas físicas asociadas a las personas contempladas en las letras a) y b);

y que se enumeran en el anexo.

2. El apartado 1 no obliga a los Estados miembros a denegar la entrada en su territorio a sus propios nacionales.

3. El apartado 1 se entiende sin perjuicio de aquellos casos en los que un Estado miembro esté obligado por una disposición de Derecho internacional, a saber:

a) como país anfitrión de una organización internacional intergubernamental;

b) como país anfitrión de una conferencia internacional convocada o auspiciada por las Naciones Unidas;

c) en virtud de un acuerdo multilateral que confiera privilegios e inmunidades; o

d) en virtud del Concordato de 1929 (Pacto de Letrán) celebrado entre la Santa Sede (Estado de la Ciudad del Vaticano) e Italia.

▼B

4. El apartado 3 también se considerará aplicable cuando un Estado miembro sea país anfitrión de la Organización para la Seguridad y la Cooperación en Europa (OSCE).

5. Se informará debidamente al Consejo en todos los casos en que un Estado miembro conceda una exención de conformidad con los apartados 3 o 4.

6. Los Estados miembros podrán conceder exenciones de las medidas impuestas en el apartado 1 cuando el viaje esté justificado por razones humanitarias urgentes o en razón de la asistencia a reuniones intergubernamentales, a reuniones promovidas u organizadas por la Unión, u organizadas por un Estado miembro que ejerza la Presidencia de la OSCE, en las que se mantenga un diálogo político que fomente directamente los objetivos políticos de las medidas restrictivas, incluidas la seguridad y la estabilidad del ciberespacio.

7. Los Estados miembros también podrán conceder exenciones respecto de las medidas impuestas en virtud del apartado 1 cuando la entrada o el tránsito sean necesarios para el desarrollo de un proceso judicial.

8. Todo Estado miembro que desee conceder las exenciones a que se refiere el apartado 6 o 7 lo notificará por escrito al Consejo. Se considerarán concedidas las exenciones a menos que uno o varios miembros del Consejo presenten objeciones por escrito antes de transcurridos dos días hábiles desde la recepción de la notificación de la exención propuesta. En caso de que algún miembro del Consejo formule una objeción, el Consejo, por mayoría cualificada, podrá decidir la concesión de la exención propuesta.

9. Cuando, en virtud de los apartados 3, 4, 6, 7 u 8, un Estado miembro autorice la entrada en su territorio o el tránsito por él de alguna de las personas enumeradas en el anexo, la autorización quedará estrictamente limitada a la finalidad para la cual fue concedida y a las personas a las que atañe directamente.

Artículo 5

1. Serán inmovilizados todos los fondos y recursos económicos cuya propiedad, titularidad, tenencia o control correspondan a:

a) las personas físicas o jurídicas, entidades u organismos que sean responsables de los ciberataques o intentos de ciberataques;

b) las personas físicas o jurídicas, entidades u organismos que presten ayuda financiera, técnica o material o que estén implicadas de alguna otra forma en ciberataques o tentativas de ciberataque, en particular mediante la planificación, preparación, participación en ellos, dirección, ayuda o fomento de dichos ataques, o la facilitación de su comisión por acción u omisión;

c) las personas físicas o jurídicas, entidades u organismos asociadas con las personas físicas o jurídicas, entidades y organismos a que se refieren las letras a) y b),

y que se enumeran en el anexo.

▼B

2. En ningún caso se pondrán fondos o recursos económicos a disposición directa o indirecta de las personas físicas o jurídicas, entidades u organismos enumerados en el anexo, ni se utilizarán en su beneficio.

3. Como excepción a lo dispuesto en los apartados 1 y 2, las autoridades competentes del Estado miembro podrán autorizar la liberación de ciertos fondos o recursos económicos inmovilizados, o la puesta a disposición de ciertos fondos o recursos económicos, en las condiciones que estimen oportunas, tras haber constatado que dichos fondos o recursos económicos:

a) ►C1 son necesarios para satisfacer las necesidades básicas de las personas físicas o jurídicas, entidades u organismos enumerados en el anexo ◄ y de los miembros de la familia que dependan de esas personas físicas, como el pago de alimentos, alquileres o hipotecas, medicamentos y tratamientos médicos, impuestos, primas de seguros y tasas de servicios públicos;

b) se destinan exclusivamente al pago de honorarios profesionales razonables o al reembolso de gastos correspondientes a la prestación de servicios jurídicos;

c) se destinan exclusivamente al pago de tasas o gastos ocasionados por servicios ordinarios de custodia o mantenimiento de fondos o recursos económicos inmovilizados;

d) son necesarios para sufragar gastos extraordinarios, siempre y cuando que la autoridad competente que corresponda haya notificado a las autoridades competentes de los demás Estados miembros y a la Comisión, al menos dos semanas antes de la autorización, los motivos por los cuales considera que debe concederse una autorización específica; o

e) se ingresan en la cuenta o se pagan con cargo a la cuenta de una misión diplomática o consular o de una organización internacional que goce de inmunidad con arreglo al Derecho internacional, en la medida en que dichos pagos estén destinados a ser utilizados para los fines oficiales de la misión diplomática o consular o de la organización internacional.

El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida con arreglo al presente apartado.

4. Como excepción a lo dispuesto en el apartado 1, las autoridades competentes del Estado miembro podrán autorizar la liberación de determinados fondos o recursos económicos inmovilizados siempre que concurran las condiciones siguientes:

a) que los fondos o recursos económicos sean objeto de una resolución arbitral pronunciada antes de la fecha en que la persona física o jurídica, entidad u organismo a que se refiere el apartado 1 haya sido incluido en la lista del anexo, o de una resolución judicial o administrativa adoptada en la Unión, o de una resolución judicial con fuerza ejecutiva en el Estado miembro de que se trate, dictada antes o después de esa fecha;

▼B

b) que los fondos o recursos económicos vayan a utilizarse exclusivamente para satisfacer las demandas derivadas de tales resoluciones o reconocidas como válidas en ellas, en los límites establecidos por las disposiciones legales y reglamentarias aplicables a los derechos de las personas que presenten dichas demandas;

c) que la resolución no beneficie a ninguna de las personas físicas o jurídicas, entidades u organismos enumerados en el anexo; y

d) que el reconocimiento de la resolución no sea contrario al orden público en el Estado miembro de que se trate.

El Estado miembro de que se trate informará a los demás Estados miembros y a la Comisión de cualquier autorización concedida con arreglo al presente apartado.

5. El apartado 1 no impedirá que una persona física o jurídica, entidad u organismo incluido en el anexo pueda efectuar pagos adeudados en virtud de contratos suscritos antes de la fecha en que se haya incluido en el anexo a dicha persona física o jurídica, entidad u organismo, siempre y cuando el Estado miembro correspondiente haya considerado que el pago no es percibido directa ni indirectamente por una de las personas físicas o jurídicas, entidades u organismos a que se refiere el apartado 1.

6. El apartado 2 no se aplicará al ingreso en las cuentas inmovilizadas de:

a) intereses u otros beneficios correspondientes a dichas cuentas;

b) pagos en virtud de contratos o acuerdos celebrados u obligaciones contraídas antes de la fecha en que dichas cuentas hayan pasado a estar sujetas a las medidas reguladas en los apartados 1 y 2; o

c) pagos adeudados en virtud de una resolución judicial, administrativa o arbitral adoptada en la Unión, o que tenga fuerza ejecutiva en el Estado miembro de que se trate,

siempre que las medidas establecidas en el apartado 1 sigan siendo de aplicación a cualquiera de dichos intereses, otros beneficios y pagos.

Artículo 6

1. El Consejo, por unanimidad y a propuesta de un Estado miembro o de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, establecerá y modificará la lista que figura en el anexo.

2. El Consejo comunicará la decisión a que se refiere el apartado 1, y los motivos de la inclusión en la lista, a la persona física o jurídica, entidad u organismo afectados, bien directamente, si se conoce su domicilio, o mediante la publicación de un anuncio, y ofrecerá a dicha persona física o jurídica, entidad u organismo la oportunidad de presentar observaciones al respecto.

3. Cuando se presenten observaciones o nuevas pruebas sustanciales, el Consejo reconsiderará la decisión a que se refiere el apartado 1 e informará en consecuencia a la persona física o jurídica, entidad u organismo afectados.

▼B

Artículo 7

1. El anexo incluirá los motivos de la inscripción en la lista de las personas físicas o jurídicas, entidades u organismos a que se refieren los artículos 4 y 5.

2. El anexo contendrá, cuando se disponga de ella, la información necesaria para identificar a las personas físicas o jurídicas, entidades u organismos de que se trate. Respecto de las personas físicas, esa información podrá incluir el nombre, apellidos y los alias, el lugar y fecha de nacimiento, la nacionalidad, el número de pasaporte o de documento de identidad, el sexo, la dirección, si se conoce, y el cargo o la profesión. En el caso de las personas jurídicas, entidades u organismos, la información podrá incluir el nombre, el lugar y la fecha de registro, el número de registro y el domicilio social.

Artículo 8

No se estimará demanda alguna relacionada con un contrato o transacción cuya ejecución se haya visto afectada, directa o indirectamente, total o parcialmente, por las medidas impuestas por la presente Decisión, incluidas las demandas de indemnización o cualquier otra pretensión de este tipo, tales como una demanda de compensación o una demanda a título de garantía, en particular cualquier demanda que tenga por objeto la prórroga o el pago de una fianza, una garantía o una indemnización, en particular financieras, independientemente de la forma que adopte, si la presentan:

a) personas físicas o jurídicas, entidades u organismos designados que figuren en la lista del anexo;

b) cualquier persona física o jurídica, entidad u organismo que actúe a través o en nombre de una de las personas físicas o jurídicas, entidades u organismos a que se refiere la letra a).

Artículo 9

Para que las medidas establecidas en la presente Decisión tengan el mayor impacto posible, la Unión animará a terceros Estados a que adopten medidas restrictivas similares a las establecidas en la presente Decisión.

▼M1

Artículo 10

La presente Decisión será aplicable hasta el 18 de mayo de 2021 y estará sujeta a revisión continua. Se prorrogará o modificará, según proceda, si el Consejo estima que no se han cumplido sus objetivos.

▼B

Artículo 11

La presente Decisión entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

▼B

ANEXO

Lista de personas físicas o jurídicas, entidades y organismos a que se refieren los artículos 4 y 5

▼M2

A. Personas físicas

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
1.	GAO Qiang	Lugar de nacimiento: provincia de Shandong (China) Dirección: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nacionalidad: china Sexo: masculino	Gao Qiang está implicado en la operación «Cloud Hopper», una serie de ciberataques con un efecto significativo realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados. La operación «Cloud Hopper» se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas. El grupo conocido como «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» y «Potassium») llevó a cabo la operación «Cloud Hopper». Puede relacionarse a Gao Qiang con el APT10, entre otras cosas por su relación con la infraestructura de mando y control del grupo. Además, Gao Qiang estuvo empleado en Huaying Haitai, entidad incluida en la lista por facilitar y prestar apoyo a la operación «Cloud Hopper». Tiene vínculos con Zhang Shilong, que también ha sido incluido en la lista en relación con la operación «Cloud Hopper». Por lo tanto, Gao Qiang está relacionado tanto con Huaying Haitai como con Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Dirección: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidad: china Sexo: masculino	Zhang Shilong está implicado en la operación «Cloud Hopper», una serie de ciberataques con un efecto significativo, realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados.	30.7.2020

▼M2

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			La operación «Cloud Hopper» se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas. El grupo conocido como «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» y «Potassium») llevó a cabo la operación «Cloud Hopper». Puede relacionarse a Zhang Shilong con APT10, entre otras cosas por el software malicioso que desarrolló y probó en relación con los ciberataques llevados a cabo por APT10. Además, Zhang Shilong estuvo empleado en Huaying Haitai, entidad incluida en la lista por facilitar y prestar apoyo a la operación «Cloud Hopper». Tiene vínculos con Gao Qiang, que también ha sido incluido en la lista en relación con la operación «Cloud Hopper». Por lo tanto, Zhang Shilong está relacionado tanto con Huaying Haitai como con Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fecha de nacimiento: 27 de mayo de 1972 Lugar de nacimiento: Oblast Perm, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 120017582, Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Alexey Minin participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como agente auxiliar de inteligencia humana del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Alexey Minin formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020

▼M2

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fecha de nacimiento: 31 de julio de 1977 Lugar de nacimiento: Oblast Murmanskaya, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 100135556 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Aleksei Morenets participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como informático especializado en ciberseguridad del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Aleksei Morenets formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Fecha de nacimiento: 26 de julio de 1981 Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 100135555 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Evgenii Serebriakov participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como informático especializado en ciberseguridad del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Evgenii Serebriakov formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020

▼M2

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Fecha de nacimiento: 24 de agosto de 1972 Lugar de nacimiento: Ulyanovsk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 120018866 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Oleg Sotnikov participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como agente auxiliar de inteligencia humana del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Oleg Sotnikov formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020
▼M3 7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич Бадин Fecha de nacimiento: 15 de noviembre de 1990 Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Nacionalidad: rusa Sexo: masculino	Dmitry Badin participó en un ciberataque con un efecto significativo contra el Parlamento federal alemán (Bundestag). Como agente de inteligencia militar del 85.º Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Dmitry Badin formó parte de un equipo de agentes rusos de inteligencia militar que dirigieron un ciberataque contra el Parlamento federal alemán (Bundestag) en abril y mayo de 2015. Este ciberataque iba dirigido contra el sistema de información del Parlamento y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como de la canciller Angela Merkel.	22.10.2020

▼M3

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович Костюков Fecha de nacimiento: 21 de febrero de 1961 Nacionalidad: rusa Sexo: masculino	Igor Kostyukov es el actual jefe del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), después de haber sido primer jefe adjunto del mismo. Una de las unidades bajo su mando es el 85.º Centro Principal de Servicios Especiales (GTsSS), conocido también como «unidad militar 26165» (sobrenombres en el sector: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» y «Strontium»). Como tal, Igor Kostyukov es responsable de los ciberataques perpetrados por el GTsSS, entre ellos los ciberataques con un efecto significativo constitutivos de amenaza externa para la Unión o sus Estados miembros. En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Bundestag) ocurrido en abril y mayo de 2015 y la tentativa de ciberataque dirigido a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos en abril de 2018. El ciberataque contra el Parlamento federal alemán iba dirigido contra su sistema de información y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como de la canciller Angela Merkel.	22.10.2020.

▼M2

B. Personas jurídicas, entidades y organismos

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Lugar: Tianjin, China	Huaying Haitai prestó apoyo financiero, técnico o material para la operación «Cloud Hopper», una serie de ciberataques con un efecto significativo, realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados, y facilitó dicha operación.	30.7.2020

▼M2

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			La operación «Cloud Hopper» se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas. El grupo conocido como «APT10» («Advanced Persistent Threat 10») (alias «Red Apollo», «CVNX», «Stone Panda», «MenuPass» y «Potassium») llevó a cabo la operación «Cloud Hopper». Puede relacionarse a Huaying Haitai con APT10. Además, Huaying Haitai tuvo en su nómina a Gao Qiang y a Zhang Shilong, ambos incluidos en la lista en relación con la operación «Cloud Hopper». Por ello se relaciona a Huaying Haitai con Gao Qiang y Zhang Shilong.	
2.	Chosun Expo	Alias: Chosen Expo; Korea Export Joint Venture Lugar: RPDC	Chosun Expo prestó apoyo financiero, técnico o material para una serie de ciberataques con un efecto significativo realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados, y facilitó su realización; entre ellos se incluye el ciberataque conocido como «WannaCry» y varios ciberataques contra la Autoridad de Supervisión Financiera de Polonia y Sony Pictures Entertainment, así como el ciberrobo al Banco de Bangladesh y la tentativa de ciberrobo al Banco Tien Phong de Vietnam. «WannaCry» perturbó sistemas de información de todo el mundo mediante ataques con programas de secuestro y el bloqueo del acceso a los datos. Afectó a los sistemas de información de empresas de la Unión, entre ellos diversos sistemas de información relativos a servicios necesarios para el mantenimiento de servicios y actividades económicas esenciales en los Estados miembros. El ciberataque «WannaCry» fue llevado a cabo por el grupo conocido como «APT38» («Advanced Persistent Threat 38») o el «Grupo Lazarus». Puede relacionarse a Chosun Expo con APT38/Grupo Lazarus, entre otras cosas a través de las cuentas utilizadas para los ciberataques.	30.7.2020

▼M2

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
3.	Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU)	Dirección: 22 Kirova Street, Moscú, Federación de Rusia	El Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), también conocido por el código 74455, es responsable de diversos ciberataques con un efecto significativo llevados a cabo desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados; entre ellos se incluyen los ciberataques conocidos como «NotPetya» o «EternalPetya» en junio de 2017 y los ciberataques dirigidos contra una red eléctrica ucraniana en el invierno de 2015 y 2016. El ciberataque «NotPetya» o «EternalPetya» impidió el acceso a los datos en una serie de empresas de la Unión, de Europa en general y de todo el mundo, mediante ataques a ordenadores con programas de secuestro y el bloqueo del acceso a los datos, lo que causó, entre otros efectos, importantes pérdidas económicas. El ciberataque contra una red eléctrica ucraniana provocó el apagado de partes de dicha red durante el invierno. El ciberataque «NotPetya» o «EternalPetya» fue llevado a cabo por el grupo conocido como «Sandworm» (alias «Sandworm Team», «BlackEnergy Group», «Vodoo Bear», «Quedagh», «Olympic Destroyer» y «Telebots»), que también está detrás del ataque contra la red eléctrica ucraniana. El Centro Principal de Tecnologías Especiales del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia desempeña un papel activo en las actividades informáticas llevadas a cabo por Sandworm, por lo que es posible relacionarlo con dicho grupo.	30.7.2020

▼M3

4.	85.° Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU)	Dirección: Komsomol'skiy Prospekt, 20, Moscú, 119146, Federación de Rusia	El 85.º Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), conocido también como «unidad militar 26165» (sobrenombres en el sector: «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» y «Strontium»), es responsable de ciberataques con un efecto significativo constitutivos de amenaza externa para la Unión o sus Estados miembros.	22.10.2020

▼M3

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Bundestag) ocurrido en abril y mayo de 2015 y en la tentativa de ciberataque dirigido a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos en abril de 2018. El ciberataque contra el Parlamento federal alemán iba dirigido contra su sistema de información y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como de la canciller Angela Merkel.	