DECISIONES

DECISIÓN (PESC) 2020/1537 DEL CONSEJO

de 22 de octubre de 2020

por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea, y en particular su artículo 29,

Vista la propuesta del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad,

Considerando lo siguiente:

(1) El 17 de mayo de 2019, el Consejo adoptó la Decisión (PESC) 2019/797 ([1]).

(2) Las medidas restrictivas selectivas contra los ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros forman parte de las medidas previstas en el marco de la Unión para una respuesta diplomática conjunta a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia») y son un instrumento crucial de disuasión y de respuesta frente a tales actividades.

(3) A fin de evitar, desalentar e impedir los comportamientos malintencionados en el ciberespacio, constantes y en aumento, y de reaccionar ante tales comportamientos, procede incluir a dos personas físicas y un organismo en la lista de personas físicas o jurídicas, entidades y organismos sujetos a medidas restrictivas que figura en el anexo de la Decisión (PESC) 2019/797. Dichas personas y dicho organismo son responsables de ciberataques o participaron en ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros, en particular el ciberataque contra el Parlamento federal alemán (Bundestag) ocurrido en abril y mayo de 2015.

(4) Procede, por tanto, modificar la Decisión (PESC) 2019/797 en consecuencia.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

El anexo de la Decisión (PESC) 2019/797 se modifica de conformidad con el anexo de la presente Decisión.

Artículo 2

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

Hecho en Bruselas, el 22 de octubre de 2020.

Por el Consejo
El Presidente
M. ROTH

([1]) 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).

ANEXO

Se añaden las siguientes entradas a la lista de personas físicas o jurídicas, entidades y organismos que figura en el anexo de la Decisión (PESC) 2019/797:

A. Personas físicas

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«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
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».

B. Personas jurídicas, entidades y organismos

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«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. 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.	22.10.2020».