

This text is meant purely as a documentation tool and has no legal effect. The Union's institutions do not assume any liability for its contents. The authentic versions of the relevant acts, including their preambles, are those published in the Official Journal of the European Union and available in EUR-Lex. Those official texts are directly accessible through the links embedded in this document

► **B**

COUNCIL DECISION (CFSP) 2019/797

of 17 May 2019

concerning restrictive measures against cyber-attacks threatening the Union or its Member States

(OJ L 129I, 17.5.2019, p. 13)

Amended by:

		Official Journal		
		No	page	date
► M1	Council Decision (CFSP) 2020/651 of 14 May 2020	L 153	4	15.5.2020

Corrected by:

► **C1** Corrigendum, OJ L 230, 17.7.2020, p. 36 (2019/797)



COUNCIL DECISION (CFSP) 2019/797

of 17 May 2019

concerning restrictive measures against cyber-attacks threatening the Union or its Member States

Article 1

1. This Decision applies to cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Union or its Member States.

2. Cyber-attacks constituting an external threat include those which:

- (a) originate, or are carried out, from outside the Union;
- (b) use infrastructure outside the Union;
- (c) are carried out by any natural or legal person, entity or body established or operating outside the Union; or
- (d) are carried out with the support, at the direction or under the control of any natural or legal person, entity or body operating outside the Union.

3. For this purpose, cyber-attacks are actions involving any of the following:

- (a) access to information systems;
- (b) information system interference;
- (c) data interference; or
- (d) data interception,

where such actions are not duly authorised by the owner or by another right holder of the system or data or part of it, or are not permitted under the law of the Union or of the Member State concerned.

4. Cyber-attacks constituting a threat to Member States include those affecting information systems relating to, inter alia:

- (a) critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security, and economic or social well-being of people;
- (b) services necessary for the maintenance of essential social and/or economic activities, in particular in the sectors of: energy (electricity, oil and gas); transport (air, rail, water and road); banking;

▼B

financial market infrastructures; health (healthcare providers, hospitals and private clinics); drinking water supply and distribution; digital infrastructure; and any other sector which is essential to the Member State concerned;

- (c) critical State functions, in particular in the areas of defence, governance and the functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations, including through diplomatic missions;
- (d) the storage or processing of classified information; or
- (e) government emergency response teams.

5. Cyber-attacks constituting a threat to the Union include those carried out against its institutions, bodies, offices and agencies, its delegations to third countries or to international organisations, its common security and defence policy (CSDP) operations and missions and its special representatives.

6. Where deemed necessary to achieve CFSP objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Decision may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.

Article 2

For the purposes of this Decision, the following definitions apply:

- (a) ‘information systems’ means a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes digital data, as well as digital data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance.
- (b) ‘information system interference’ means hindering or interrupting the functioning of an information system by inputting digital data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible.
- (c) ‘data interference’ means deleting, damaging, deteriorating, altering or suppressing digital data on an information system, or rendering such data inaccessible; it also includes theft of data, funds, economic resources or intellectual property.
- (d) ‘data interception’ means intercepting, by technical means, non-public transmissions of digital data to, from or within an information system, including electromagnetic emissions from an information system carrying such digital data.

▼B*Article 3*

The factors determining whether a cyber-attack has a significant effect as referred to in Article 1(1) include any of the following:

- (a) the scope, scale, impact or severity of disruption caused, including to economic and societal activities, essential services, critical State functions, public order or public safety;
- (b) the number of natural or legal persons, entities or bodies affected;
- (c) the number of Member States concerned;
- (d) the amount of economic loss caused, such as through large-scale theft of funds, economic resources or intellectual property;
- (e) the economic benefit gained by the perpetrator, for himself or for others;
- (f) the amount or nature of data stolen or the scale of data breaches; or
- (g) the nature of commercially sensitive data accessed.

Article 4

1. Member States shall take the measures necessary to prevent the entry into, or transit through, their territories of:

- (a) natural persons who are responsible for cyber-attacks or attempted cyber-attacks;
- (b) natural persons who provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;
- (c) natural persons associated with the persons covered by points (a) and (b),

as listed in the Annex.

2. Paragraph 1 shall not oblige a Member State to refuse its own nationals entry into its territory.

3. Paragraph 1 shall be without prejudice to the cases where a Member State is bound by an obligation of international law, namely:

- (a) as a host country of an international intergovernmental organisation;
- (b) as a host country to an international conference convened by, or under the auspices of, the United Nations;
- (c) under a multilateral agreement conferring privileges and immunities; or
- (d) pursuant to the 1929 Treaty of Conciliation (Lateran Pact) concluded by the Holy See (Vatican City State) and Italy.

▼B

4. Paragraph 3 shall be considered to apply also in cases where a Member State is host country of the Organization for Security and Co-operation in Europe (OSCE).

5. The Council shall be duly informed in all cases where a Member State grants an exemption pursuant to paragraph 3 or 4.

6. Member States may grant exemptions from the measures imposed under paragraph 1 where travel is justified on the grounds of urgent humanitarian need, or on grounds of attending intergovernmental meetings or meetings promoted or hosted by the Union, or hosted by a Member State holding the Chairmanship in office of the OSCE, where a political dialogue is conducted that directly promotes the policy objectives of restrictive measures, including security and stability in cyberspace.

7. Member States may also grant exemptions from the measures imposed under paragraph 1 where entry or transit is necessary for the fulfilment of a judicial process.

8. A Member State wishing to grant exemptions referred to in paragraph 6 or 7 shall notify the Council in writing. The exemption shall be deemed to be granted unless one or more of the Council members raises an objection in writing within two working days of receiving notification of the proposed exemption. Should one or more of the Council members raise an objection, the Council, acting by a qualified majority, may decide to grant the proposed exemption.

9. Where, pursuant to paragraphs 3, 4, 6, 7 or 8, a Member State authorises the entry into, or transit through its territory of persons listed in the Annex, the authorisation shall be strictly limited to the purpose for which it is given and to the persons directly concerned thereby.

Article 5

1. All funds and economic resources belonging to, owned, held or controlled by:

- (a) natural or legal persons, entities or bodies that are responsible for cyber-attacks or attempted cyber-attacks;
- (b) natural or legal persons, entities or bodies that provide financial, technical or material support for or are otherwise involved in cyber-attacks or attempted cyber-attacks, including by planning, preparing, participating in, directing, assisting or encouraging such attacks, or facilitating them whether by action or omission;
- (c) natural or legal persons, entities or bodies associated with the natural or legal persons, entities or bodies covered by points (a) and (b),

as listed in the Annex, shall be frozen.

▼B

2. No funds or economic resources shall be made available directly or indirectly to or for the benefit of the natural or legal persons, entities or bodies listed in the Annex.

3. By way of derogation from paragraphs 1 and 2, the competent authorities of the Member States may authorise the release of certain frozen funds or economic resources, or the making available of certain funds or economic resources, under such conditions as they deem appropriate, after having determined that the funds or economic resources concerned are:

- (a) ►**C1** necessary to satisfy the basic needs of the natural or legal persons, entities or bodies listed in the Annex ◀ and dependent family members of such natural persons, including payments for foodstuffs, rent or mortgage, medicines and medical treatment, taxes, insurance premiums, and public utility charges;
- (b) intended exclusively for the payment of reasonable professional fees or the reimbursement of incurred expenses associated with the provision of legal services;
- (c) intended exclusively for the payment of fees or service charges for the routine holding or maintenance of frozen funds or economic resources;
- (d) necessary for extraordinary expenses, provided that the relevant competent authority has notified the competent authorities of the other Member States and the Commission of the grounds on which it considers that a specific authorisation should be granted, at least two weeks prior to the authorisation; or
- (e) to be paid into or from an account of a diplomatic or consular mission or an international organisation enjoying immunities in accordance with international law, insofar as such payments are intended to be used for official purposes of the diplomatic or consular mission or international organisation.

The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under this paragraph.

4. By way of derogation from paragraph 1, the competent authorities of the Member States may authorise the release of certain frozen funds or economic resources, provided that the following conditions are met:

- (a) the funds or economic resources are the subject of an arbitral decision rendered prior to the date on which the natural or legal person, entity or body referred to in paragraph 1 was listed in the Annex, or of a judicial or administrative decision rendered in the Union, or a judicial decision enforceable in the Member State concerned, prior to or after that date;

▼B

- (b) the funds or economic resources will be used exclusively to satisfy claims secured by such a decision or recognised as valid in such a decision, within the limits set by applicable laws and regulations governing the rights of persons having such claims;
- (c) the decision is not for the benefit of a natural or legal person, entity or body listed in the Annex; and
- (d) recognition of the decision is not contrary to public policy in the Member State concerned.

The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under this paragraph.

5. Paragraph 1 shall not prevent a natural or legal person, entity or body listed in the Annex from making a payment due under a contract entered into prior to the date on which that natural or legal person, entity or body was listed therein, provided that the Member State concerned has determined that the payment is not, directly or indirectly, received by a natural or legal person, entity or body referred to in paragraph 1.

6. Paragraph 2 shall not apply to the addition to frozen accounts of:

- (a) interest or other earnings on those accounts;
- (b) payments due under contracts, agreements or obligations that were concluded or arose prior to the date on which those accounts became subject to the measures provided for in paragraphs 1 and 2; or
- (c) payments due under judicial, administrative or arbitral decisions rendered in the Union or enforceable in the Member State concerned,

provided that any such interest, other earnings and payments remain subject to the measures provided for in paragraph 1.

Article 6

1. The Council, acting by unanimity upon a proposal from a Member State or from the High Representative of the Union for Foreign Affairs and Security Policy, shall establish and amend the list set out in the Annex.

2. The Council shall communicate the decisions referred to in paragraph 1, including the grounds for listing, to the natural or legal person, entity or body concerned, either directly, if the address is known, or through the publication of a notice, providing that natural or legal person, entity or body with an opportunity to present observations.

3. Where observations are submitted, or where substantial new evidence is presented, the Council shall review the decisions referred to in paragraph 1 and inform the natural or legal person, entity or body concerned accordingly.

▼B*Article 7*

1. The Annex shall include the grounds for listing the natural and legal persons, entities and bodies referred to in Articles 4 and 5.

2. The Annex shall contain, where available, the information necessary to identify the natural or legal persons, entities or bodies concerned. With regard to natural persons, such information may include: names and aliases; date and place of birth; nationality; passport and identity card numbers; gender; address, if known; and function or profession. With regard to legal persons, entities or bodies, such information may include names, place and date of registration, registration number and place of business.

Article 8

No claims in connection with any contract or transaction the performance of which has been affected, directly or indirectly, in whole or in part, by the measures imposed under this Decision, including claims for indemnity or any other claim of this type, such as a claim for compensation or a claim under a guarantee, in particular a claim for extension or payment of a bond, guarantee or indemnity, in particular a financial guarantee or financial indemnity, of whatever form, shall be satisfied, if they are made by:

- (a) designated natural or legal persons, entities or bodies listed in the Annex;
- (b) any natural or legal person, entity or body acting through or on behalf of one of the natural or legal persons, entities or bodies referred to in point (a).

Article 9

In order to maximise the impact of the measures set out in this Decision, the Union shall encourage third States to adopt restrictive measures similar to those provided for in this Decision.

▼M1*Article 10*

This Decision shall apply until 18 May 2021 and shall be kept under constant review. It shall be renewed, or amended as appropriate, if the Council deems that its objectives have not been met.

▼B*Article 11*

This Decision shall enter into force on the day following that of its publication in the *Official Journal of the European Union*.

▼B

ANNEX

**List of natural and legal persons, entities and bodies referred to in Articles 4
and 5**

[...]