Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

COUNCIL DECISION (CFSP) 2019/797

of 17 May 2019

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

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 29 thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 19 June 2017 the Council adopted conclusions on a framework for a joint diplomatic response to malicious cyber activities ('the Cyber Diplomacy Toolbox'), in which the Council expressed concerns about the increased ability and willingness of State and non-State actors to pursue their objectives by undertaking malicious cyber activities and affirmed the growing need to protect the integrity and security of the Union, its Member States and their citizens against cyber threats and malicious cyber activities.

(2) The Council stressed that clearly signalling the likely consequences of a joint Union diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace, thereby reinforcing the security of the Union and its Member States. It also affirmed that measures within the common foreign and security policy (CFSP), including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a framework for a joint Union diplomatic response to malicious cyber activities, with the aim of encouraging cooperation, facilitating the mitigation of immediate and long-term threats, and influencing the behaviour of potential aggressors in the long term.

(3) On 11 October 2017 implementing guidelines for the Cyber Diplomacy Toolbox were approved by the Political and Security Committee. The implementing guidelines refer to five categories of measures, including restrictive measures, within the Cyber Diplomacy Toolbox, and the process for invoking those measures.

(4) The Council conclusions adopted on 16 April 2018 on malicious cyber activities firmly condemned the malicious use of information and communications technologies (ICTs) and stressed that the use of ICTs for malicious purposes is unacceptable as it undermines the stability, security and benefits provided by the internet and the use of ICTs. The Council recalled that the Cyber Diplomacy Toolbox contributes to conflict prevention, cooperation and stability in cyberspace by setting out measures within the CFSP, including restrictive measures, that can be used to prevent and respond to malicious cyber activities. It stated that the Union will continue strongly to uphold that

Changes to legislation: *There are currently no known outstanding effects for the Council Decision (CFSP) 2019/797. (See end of Document for details)*

existing international law is applicable to cyberspace and emphasised that respect for international law, in particular the United Nations Charter, is essential to maintaining peace and stability. The Council also underlined that States are not to use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts as expressed in the 2015 report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

(5) On 28 June 2018 the European Council adopted conclusions which stressed the need to strengthen capabilities against cybersecurity threats from outside the Union. The European Council asked the institutions and Member States to implement the measures referred to in the joint communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 13 June 2018 entitled 'Increasing resilience and bolstering capabilities to address hybrid threats', including the practical use of the Cyber Diplomacy Toolbox.

(6) On 18 October 2018 the European Council adopted conclusions which called for the work on the capacity to respond to and deter cyber-attacks through Union restrictive measures to be taken forward, further to the Council conclusions of 19 June 2017.

(7) In this context, this Decision establishes a framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States. Where deemed necessary to achieve CFSP objectives in the relevant provisions of Article 21 of the Treaty on European Union, this Decision also allows for restrictive measures to be applied in response to cyber-attacks with a significant effect against third States or international organisations.

(8) In order to have a deterrent and dissuasive effect, targeted restrictive measures should focus on cyber-attacks falling within the scope of this Decision that are wilfully carried out.

(9) Targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State. The application of targeted restrictive measures does not amount to such attribution, which is a sovereign political decision taken on a case-by-case basis. Every Member State is free to make its own determination with respect to the attribution of cyber-attacks to a third State.

(10) Further action by the Union is needed in order to implement certain measures,

HAS ADOPTED THIS DECISION:

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;

***Changes to legislation:** There are currently no known outstanding effects for the Council Decision (CFSP) 2019/797. (See end of Document for details)*

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; 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.

Changes to legislation: *There are currently no known outstanding effects for the Council Decision (CFSP) 2019/797. (See end of Document for details)*

(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.

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.

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).

***Changes to legislation:** There are currently no known outstanding effects for the Council Decision (CFSP) 2019/797. (See end of Document for details)*

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.

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 **[**[X1]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