

Official Journal of the European Union

L 129 I



English edition

Legislation

Volume 62

17 May 2019

Contents

II *Non-legislative acts*

REGULATIONS

- ★ **Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States** 1

DECISIONS

- ★ **Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States** 13

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

II

(Non-legislative acts)

REGULATIONS

COUNCIL REGULATION (EU) 2019/796

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 the Functioning of the European Union, and in particular Article 215 thereof,

Having regard to Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ⁽¹⁾,

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

Whereas:

- (1) 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.
- (2) On 17 May 2019 the Council adopted Decision (CFSP) 2019/797. Decision (CFSP) 2019/797 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. Persons, entities and bodies subject to the restrictive measures are listed in the Annex to that Decision.
- (3) This Regulation respects the fundamental rights and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular the right to an effective remedy and to a fair trial and the right to the protection of personal data. This Regulation should be applied in accordance with those rights.
- (4) The power to establish and amend the list in Annex I to this Regulation should be exercised by the Council in order to ensure consistency with the process for establishing, amending and reviewing the Annex to Decision (CFSP) 2019/797.
- (5) For the implementation of this Regulation, and in order to ensure maximum legal certainty within the Union, the names and other relevant data concerning natural and legal persons, entities and bodies whose funds and economic resources are to be frozen in accordance with this Regulation should be made public. Any processing of personal data should comply with Regulations (EU) 2016/679 ⁽²⁾ and (EU) 2018/1725 ⁽³⁾ of the European Parliament and of the Council.

⁽¹⁾ See page 13 of this Official Journal.

⁽²⁾ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

⁽³⁾ Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).

- (6) Member States and the Commission should inform each other of the measures taken pursuant to this Regulation and of other relevant information at their disposal in connection with this Regulation.
- (7) Member States should lay down rules on sanctions applicable to infringements of the provisions of this Regulation and make sure that they are implemented. Those sanctions should be effective, proportionate and dissuasive,

HAS ADOPTED THIS REGULATION:

Article 1

1. This Regulation 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; 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 common foreign and security policy (CFSP) objectives in the relevant provisions of Article 21 of the Treaty on European Union, restrictive measures under this Regulation may also be applied in response to cyber-attacks with a significant effect against third States or international organisations.

7. For the purposes of this Regulation, 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.

8. For the purposes of this Regulation, the following additional definitions apply:

- (a) 'claim' means any claim, whether asserted by legal proceedings or not, made before or after the date of entry into force of this Regulation, under or in connection with a contract or transaction, and includes in particular:
 - (i) a claim for performance of any obligation arising under or in connection with a contract or transaction;
 - (ii) a claim for extension or payment of a bond, financial guarantee or indemnity of whatever form;
 - (iii) a claim for compensation in respect of a contract or transaction;
 - (iv) a counterclaim;
 - (v) a claim for the recognition or enforcement, including by the procedure of *exequatur*, of a judgment, an arbitration award or an equivalent decision, wherever made or given;
- (b) 'contract or transaction' means any transaction of whatever form and whatever the applicable law, whether comprising one or more contracts or similar obligations made between the same or different parties; for this purpose, 'contract' includes a bond, guarantee or indemnity, particularly a financial guarantee or financial indemnity, and credit, whether legally independent or not, as well as any related provision arising under, or in connection with, the transaction;
- (c) 'competent authorities' refers to the competent authorities of the Member States as identified on the websites listed in Annex II;
- (d) 'economic resources' means assets of every kind, whether tangible or intangible, movable or immovable, which are not funds, but may be used to obtain funds, goods or services;
- (e) 'freezing of economic resources' means preventing the use of economic resources to obtain funds, goods or services in any way, including, but not limited to, by selling, hiring or mortgaging them;
- (f) 'freezing of funds' means preventing any move, transfer, alteration, use of, access to, or dealing with funds in any way that would result in any change in their volume, amount, location, ownership, possession, character or destination or any other change that would enable the funds to be used, including portfolio management;
- (g) 'funds' means financial assets and benefit of every kind, including, but not limited to:
 - (i) cash, cheques, claims on money, drafts, money orders and other payment instruments;
 - (ii) deposits with financial institutions or other entities, balances on accounts, debts and debt obligations;
 - (iii) publicly-and privately-traded securities and debt instruments, including stocks and shares, certificates representing securities, bonds, notes, warrants, debentures and derivatives contracts;
 - (iv) interest, dividends or other income on or value accruing from or generated by assets;
 - (v) credit, right of set-off, guarantees, performance bonds or other financial commitments;

- (vi) letters of credit, bills of lading and bills of sale; and
- (vii) documents showing evidence of an interest in funds or financial resources;
- (h) 'territory of the Union' means the territories of the Member States to which the Treaty is applicable, under the conditions laid down in the Treaty, including their airspace.

Article 2

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 3

1. All funds and economic resources belonging to, owned, held or controlled by any natural or legal person, entity or body listed in Annex I shall be frozen.
2. No funds or economic resources shall be made available, directly or indirectly, to or for the benefit of natural or legal persons, entities or bodies listed in Annex I.
3. Annex I shall include, as identified by the Council in accordance with Article 5(1) of Decision (CFSP) 2019/797:
 - (a) natural or legal persons, entities or bodies who are responsible for cyber-attacks or attempted cyber-attacks;
 - (b) natural persons 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) of this paragraph.

Article 4

1. By way of derogation from Article 3, 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) necessary to satisfy the basic needs of the natural persons listed in Annex I 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.

2. The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Article 5

1. By way of derogation from Article 3(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 Article 3 was listed in Annex I, 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) 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 Annex I; and
- (d) recognition of the decision is not contrary to public policy in the Member State concerned.

2. The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Article 6

1. By way of derogation from Article 3(1) and provided that a payment by a natural or legal person, entity or body listed in Annex I is due under a contract or agreement that was concluded by, or an obligation that arose for, the natural or legal person, entity or body concerned before the date on which that natural or legal person, entity or body was included in Annex I, the competent authorities of the Member States may authorise, under such conditions as they deem appropriate, the release of certain frozen funds or economic resources, provided that the competent authority concerned has determined that:

- (a) the funds or economic resources will be used for a payment by a natural or legal person, entity or body listed in Annex I; and
- (b) the payment is not in breach of Article 3(2).

2. The Member State concerned shall inform the other Member States and the Commission of any authorisation granted under paragraph 1 within two weeks of the authorisation.

Article 7

1. Article 3(2) shall not prevent the crediting of frozen accounts by financial or credit institutions that receive funds transferred by third parties onto the account of a listed natural or legal person, entity or body, provided that any additions to such accounts will also be frozen. The financial or credit institution shall inform the relevant competent authority about any such transaction without delay.

2. Article 3(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 before the date on which the natural or legal person, entity or body referred to in Article 3(1) was included in Annex I; or
- (c) payments due under judicial, administrative or arbitral decisions rendered in a Member State or enforceable in the Member State concerned,

provided that any such interest, other earnings and payments remain subject to the measures provided for in Article 3(1).

Article 8

1. Without prejudice to the applicable rules concerning reporting, confidentiality and professional secrecy, natural and legal persons, entities and bodies shall:
 - (a) supply immediately any information which would facilitate compliance with this Regulation, such as information on accounts and amounts frozen in accordance with Article 3(1), to the competent authority of the Member State where they are resident or located, and transmit such information, directly or through the Member State, to the Commission; and
 - (b) cooperate with the competent authority in any verification of the information referred to in point (a).
2. Any additional information received directly by the Commission shall be made available to the Member States.
3. Any information provided or received in accordance with this Article shall be used only for the purposes for which it was provided or received.

Article 9

It shall be prohibited to participate, knowingly and intentionally, in activities the object or effect of which is to circumvent the measures referred to in Article 3.

Article 10

1. The freezing of funds and economic resources or the refusal to make funds or economic resources available, carried out in good faith on the basis that such action is in accordance with this Regulation, shall not give rise to liability of any kind on the part of the natural or legal person or entity or body implementing it, or its directors or employees, unless it is proved that the funds and economic resources were frozen or withheld as a result of negligence.
2. Actions by natural or legal persons, entities or bodies shall not give rise to any liability of any kind on their part if they did not know, and had no reasonable cause to suspect, that their actions would infringe the measures set out in this Regulation.

Article 11

1. 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 Regulation, 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 Annex I;
 - (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).
2. In any proceedings for the enforcement of a claim, the onus of proving that satisfying the claim is not prohibited by paragraph 1 shall be on the natural or legal person, entity or body seeking the enforcement of that claim.
3. This Article is without prejudice to the right of the natural or legal persons, entities and bodies referred to in paragraph 1 to judicial review of the legality of the non-performance of contractual obligations in accordance with this Regulation.

Article 12

1. The Commission and Member States shall inform each other of the measures taken under this Regulation and share any other relevant information at their disposal in connection with this Regulation, in particular information in respect of:
 - (a) funds frozen under Article 3 and authorisations granted under Articles 4, 5 and 6;
 - (b) violation and enforcement problems and judgments handed down by national courts.
2. The Member States shall immediately inform each other and the Commission of any other relevant information at their disposal which might affect the effective implementation of this Regulation.

Article 13

1. Where the Council decides to subject a natural or legal person, entity or body to the measures referred to in Article 3, it shall amend Annex I accordingly.
2. The Council shall communicate the decision 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 decision referred to in paragraph 1 and inform the natural or legal person, entity or body concerned accordingly.
4. The list in Annex I shall be reviewed at regular intervals and at least every 12 months.
5. The Commission shall be empowered to amend Annex II on the basis of information supplied by Member States.

Article 14

1. Annex I shall include the grounds for the listing of natural or legal persons, entities or bodies concerned.
2. Annex I 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 15

1. Member States shall lay down the rules on penalties applicable to infringements of the provisions of this Regulation and shall take all measures necessary to ensure that they are implemented. The penalties provided for shall be effective, proportionate and dissuasive.
2. Member States shall notify the Commission of the rules referred to in paragraph 1 without delay after the entry into force of this Regulation and shall notify it of any subsequent amendment.

Article 16

1. The Commission shall process personal data in order to carry out its tasks under this Regulation. These tasks include:
 - (a) adding the contents of Annex I to the electronic, consolidated list of persons, groups and entities subject to Union financial sanctions and to the interactive sanctions map, both publicly available;
 - (b) processing information on the impact of the measures of this Regulation such as the value of frozen funds and information on authorisations granted by the competent authorities.
2. For the purposes of this Regulation, the Commission service listed in Annex II is designated as 'controller' for the Commission within the meaning of Article 3(8) of Regulation (EU) 2018/1725, in order to ensure that the natural persons concerned can exercise their rights under that Regulation.

Article 17

1. Member States shall designate the competent authorities referred to in this Regulation and identify them on the websites listed in Annex II. Member States shall notify the Commission of any changes in the addresses of their websites listed in Annex II.
2. Member States shall notify the Commission of their competent authorities, including the contact details of those competent authorities, without delay after the entry into force of this Regulation, and shall notify it of any subsequent amendment.
3. Where this Regulation sets out a requirement to notify, inform or otherwise communicate with the Commission, the address and other contact details to be used for such communication shall be those indicated in Annex II.

Article 18

This Regulation shall apply:

- (a) within the territory of the Union, including its airspace;
- (b) on board any aircraft or vessel under the jurisdiction of a Member State;
- (c) to any natural person inside or outside the territory of the Union who is a national of a Member State;
- (d) to any legal person, entity or body, inside or outside the territory of the Union, which is incorporated or constituted under the law of a Member State;
- (e) to any legal person, entity or body in respect of any business done in whole or in part within the Union.

Article 19

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels, 17 May 2019.

For the Council
The President
E.O. TEODOROVICI

ANNEX I

List of natural and legal persons, entities and bodies referred to in Article 3

[...]

ANNEX II

Websites for information on the competent authorities and address for notifications to the Commission

BELGIUM

https://diplomatie.belgium.be/nl/Beleid/beleidsthemas/vrede_en_veiligheid/sancties

https://diplomatie.belgium.be/fr/politique/themes_politiques/paix_et_securite/sanctions

https://diplomatie.belgium.be/en/policy/policy_areas/peace_and_security/sanctions

BULGARIA

<https://www.mfa.bg/en/101>

CZECHIA

www.financnianalytickyurad.cz/mezinarodni-sankce.html

DENMARK

<http://um.dk/da/Udenrigspolitik/folkeretten/sanktioner/>

GERMANY

<http://www.bmwi.de/DE/Themen/Aussenwirtschaft/aussenwirtschaftsrecht,did=404888.html>

ESTONIA

http://www.vm.ee/est/kat_622/

IRELAND

<http://www.dfa.ie/home/index.aspx?id=28519>

GREECE

<http://www.mfa.gr/en/foreign-policy/global-issues/international-sanctions.html>

SPAIN

<http://www.exteriores.gob.es/Portal/en/PoliticaExteriorCooperacion/GlobalizacionOportunidadesRiesgos/Paginas/SancionesInternacionales.aspx>

FRANCE

<http://www.diplomatie.gouv.fr/fr/autorites-sanctions/>

CROATIA

<http://www.mvep.hr/sankcije>

ITALY

https://www.esteri.it/mae/it/politica_estera/politica_europea/misure_deroghe

CYPRUS

http://www.mfa.gov.cy/mfa/mfa2016.nsf/mfa35_en/mfa35_en?OpenDocument

LATVIA

<http://www.mfa.gov.lv/en/security/4539>

LITHUANIA

<http://www.urm.lt/sanctions>

LUXEMBOURG

<https://maee.gouvernement.lu/fr/directions-du-ministere/affaires-europeennes/mesures-restrictives.html>

HUNGARY

http://www.kormany.hu/download/9/2a/f0000/EU%20szankci%C3%B3s%20t%C3%A1j%C3%A9koztat%C3%B3_20170214_final.pdf

MALTA

<https://foreignaffairs.gov.mt/en/Government/SMB/Pages/Sanctions-Monitoring-Board.aspx>

NETHERLANDS

<https://www.rijksoverheid.nl/onderwerpen/internationale-sancties>

AUSTRIA

http://www.bmeia.gv.at/view.php3?f_id=12750&LNG=en&version=

POLAND

<https://www.gov.pl/web/dyplomacja>

PORTUGAL

<http://www.portugal.gov.pt/pt/ministerios/mne/quero-saber-mais/sobre-o-ministerio/medidas-restritivas/medidas-restritivas.aspx>

ROMANIA

<http://www.mae.ro/node/1548>

SLOVENIA

http://www.mzz.gov.si/si/omejevalni_ukrepi

SLOVAKIA

https://www.mzv.sk/europske_zalezitosti/europske_politiky-sankcie_eu

FINLAND

<http://formin.finland.fi/kvyhteisty/pakotteet>

SWEDEN

<http://www.ud.se/sanktioner>

UNITED KINGDOM

<https://www.gov.uk/sanctions-embargoes-and-restrictions>

Address for notifications to the European Commission:

European Commission
Service for Foreign Policy Instruments (FPI)
EEAS 07/99
B-1049 Brussels, Belgium
E-mail: relex-sanctions@ec.europa.eu

DECISIONS

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 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;
 - (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.
- (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).
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) necessary to satisfy the basic needs of the natural persons 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) 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.

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.

Article 10

This Decision shall apply until 18 May 2020 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.

Article 11

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

Done at Brussels, 17 May 2019.

For the Council
The President
E.O. TEODOROVICI

ANNEX

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

[...]

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)



Publications Office of the European Union
2985 Luxembourg
LUXEMBOURG

EN