Council of the European Union

Brussels, 8 March 2019
(OR. en)

7298/19

LIMITE

CORLX 105
CFSP/PESC 190
CYBER 80
JAI 263
FIN 215

PROPOSAL

From:	High Representative of the Union for Foreign Affairs and Security Policy, signed by Ms Helga Schmid, Secretary General
date of receipt:	7 March 2019
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
Subject:	Proposal of the High Representative of the Union for Foreign Affairs and Security Policy to the Council for a Council Decision concerning restrictive measures to counter cyber-attacks threatening the Union or its Member States

Delegations will find attached document HR(2019) 20.

Encl.: HR(2019) 20

EUROPEAN EXTERNAL ACTION SERVICE

GREFFE

Proposal of the High Representative of the Union for Foreign Affairs and Security Policy to the Council

of 07/03/2019

for a Council Decision
concerning restrictive measures to counter cyber-attacks threatening the Union or its Member States

HR(2019) 20
Limited

COUNCIL DECISION (CFSP) 2019/…

of …

concerning restrictive measures to counter 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 agreed on Council conclusions on a Framework for a Joint Diplomatic Response to Malicious Cyber Activities (the "Cyber Diplomacy Toolbox"), in which the Council expressed concerns by 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 EU, 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 EU diplomatic response to such malicious cyber activities influences the behaviour of potential aggressors in cyberspace thus reinforcing the security of the EU and its Member States and affirmed that measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures, adopted under the relevant provisions of the Treaties, are suitable for a Framework for a joint EU diplomatic response to malicious cyber activities, with the aim of encouraging cooperation, facilitating mitigation of immediate and long-term threats, and influencing the behaviour of potential aggressors in a long term.

(3) 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 EU's Common Foreign and Security Policy, including restrictive measures, that can be used to prevent and respond to malicious cyber activities.

(4) On 28 June 2018, the European Council adopted conclusions which stressed the need to strengthen capabilities against cybersecurity threats from outside the EU. The European Council asked the institutions and Member States to implement the measures referred to in the Joint Communication, including the practical use of the cyber diplomacy toolbox.

(5) 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 EU restrictive measures to be taken forward, further to the 19 June 2017 Council conclusions. Moreover, in order to strengthen EU resilience against cyber-attacks, the same conclusions called for negotiations on all cybersecurity proposals to be concluded before the end of the legislature.

(6) In this context, this Decision establishes a framework for targeted restrictive measures to prevent and respond to cyber-attacks with a significant effect which threaten the integrity and security of the EU, its Member States and their citizens.

(7) 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.

(8) Targeted restrictive measures should be differentiated from attribution of responsibility for cyber activities to a third State. The application of targeted restrictive measures does not amount to such attribution.

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

HAS ADOPTED THIS DECISION:

Article 1

1. For the purpose of this Decision, 'cyber-attacks' means activities without right with a significant effect related to one or more of the following:

   (a) access to information systems;

   (b) information system interference;

   (c) data interference; or

   (d) data interception.

2. The activities referred to in paragraph 1 include but are not limited to activities that:

   (a) affect information systems relating to critical infrastructure in a Member State or a European critical infrastructure;

   (b) affect information systems relating to the provision of essential services;

   (c) affect information systems relating to critical State functions, in particular:

      (i) Defence;

      (ii) Governance and functioning of institutions; including the organisation of elections;

      (iii) Functioning of economic and civil infrastructure;

      (iv) Vital needs of population;

      (v) Internal security;

      (vi) External relations.

   (d) affect information systems relating to the storage or processing of classified information; or

   (e) affect information systems relating to government emergency response teams.

3. The cyber-attacks referred to in paragraph 1 may include activities which result in:

   (a) large scale theft of funds or economic resources;

   (b) large scale theft of data and major data breaches;

   (c) large scale intellectual property theft;

(d) access to commercially sensitive data which, by its nature, procures a significant economic and/or commercial benefit for the perpetrator or for others to whom the perpetrator passes this data; or

(e) significantly hindering or interrupting the functioning of information systems or deleting, damaging, deteriorating, altering or suppressing data on those systems.

Article 2

For the purpose of this Decision, the following definitions shall apply:

(1) "Without right" means access to information systems, information system interference, data interference or data interception which is not authorised by the owner or by another right holder of the system or part of it, or not permitted under the law of the Union or a Member State.

(2) "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.

(3) "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.

(4) "Data interference" means deleting, damaging, deteriorating, altering or suppressing digital data on an information system, or rendering such data inaccessible. It shall also include theft of data, funds, economic resources or intellectual property rights.

(5) "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.

(6) "Critical infrastructure" means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people.

(7) "European critical infrastructure" means critical infrastructure as defined in paragraph 6 located in two or more Member States.

(8) "Essential services" means services essential for the maintenance of critical societal and/or economic activities, which depend on information systems. Essential services include services provided in the following sectors and subsectors:

(a) Energy: electricity, oil and gas;

(b) Transport: air transport, rail transport, water transport, road transport;

(c) Banking;

(d) Financial market infrastructures;

(e) Health sector: health care settings (including hospitals and private clinics);

(f) Drinking water supply and distribution; and

(g) Digital infrastructure.

Article 3

1. The factors to consider when determining a significant effect as referred to in Article 1 (1) could include but are not limited to:

(a) the scope, scale, duration, intensity, complexity, sophistication, impact, severity of or disruption caused by the cyber-attack, including on economic and societal activities, essential services, critical State functions, public order or public safety;

(b) the number of people affected;

(c) the number of Member States concerned;

(d) the amount of economic loss; or

(e) the economic benefit gained by the perpetrator, for himself or for others.

2. To determine that there has been a significant effect as referred to in Article 1(1), the Council does not need to determine that the effects have been significant in relation to each of the individual factors listed in paragraph 1.

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, including by participating, planning, directing, assisting, facilitating, preparing, contributing, encouraging, knowingly allowing or supporting cyber-attacks or attempted cyber-attacks;

(c) natural persons associated with the natural persons covered by points (a) and (b) of this paragraph;

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 as applying also in cases where a Member State is host country of the Organisation for Security and Cooperation 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 and those promoted or hosted by the European 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 the restrictive measures, including stability in cyber space.

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 or 7 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 who are responsible for cyber-attacks or attempted cyber-attacks;

(b) natural persons or legal persons, entities or bodies who provide financial, technical or material support for or are otherwise involved in, including by participating, planning, directing, assisting, facilitating, preparing, contributing, encouraging, knowingly allowing or supporting cyber-attacks or attempted cyber-attacks;

(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;

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 authority of a Member State 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 it deems 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 and 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 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 a Member State 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, an entity or body listed in the Annex from making a payment due under a contract entered into prior to the date on which such 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 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 in the Annex.

2. The Council shall communicate the decision referred to in paragraph 1, including the grounds for the 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 such 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.

Article 7

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

2. The Annex shall also 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, including 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 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 … [12 months after adoption date]. This Decision 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…, …

For the Council

The President

ANNEX

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