Council of the European Union

Brussels, 6 February 2019
(OR. en)

5807/19

LIMITE

CYBER 21	**RELEX 66**
COPEN 27	**TELECOM 31**
COPS 22	**DAPIX 23**
COSI 7	**CATS 9**
DATAPROTECT 17	**CSC 39**
IND 21	**CSCI 17**
JAI 64	**IA 26**
JAIEX 3	**CORLX 34**
POLMIL 6	

NOTE

From:	EEAS
To:	Delegations
Subject:	Cyber Diplomacy Toolbox – Options for a restrictive measures framework to respond to or deter cyber activities that threaten the security or foreign policy interests of the Union or its Member States

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (04.11.2020)

Delegations will find in a Annex revised version of the options paper on Restrictive measures that will be discussed at the meeting of the Horizontal Working Party on Cyber Issues on 8 February 2019. The changes introduced reflect the comments and observations received from Member States and following the meeting of the HWP on Cyber Issues on 23 January 2019. Deletions to 14377/2/18 REV 2 are marked with ~~strikethrough~~ and additions with **bold** / underlined.

ANNEX

Cyber Diplomacy Toolbox – Options for a restrictive measures framework to respond to or deter cyber activities that threaten the security or foreign policy interests of the Union or its Member States

1. Introduction

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"). The Framework allows the EU and its Member States to prevent and respond to [~~illicit~~] **malicious** cyber activities. Through the use of (CFSP) measures within the Framework, the EU and its Member States seek "to encourage cooperation, facilitate the mitigation of immediate and long-term threats, and influence the behaviour of potential aggressors in the long term".

One of the tools available in the Cyber Diplomacy Toolbox is the possibility to impose sanctions in response to certain types of cyber activities (as defined in this non-paper).

Following the Council Conclusions work commenced on implementing guidelines, which were agreed in the autumn of 2017 by PSC.

The Council Conclusions of 16 April 2018 on malicious cyber activities underlined that the Cyber Diplomacy Toolbox sets out measures, including restrictive measures, **which** [~~that~~] can be used to prevent and respond to malicious cyber activities.

Further implementation of the Cyber **Diplomacy** Toolbox was mentioned in the European Council Conclusions of June 2018, where the European Council stressed "the need to strengthen capabilities against cybersecurity threats from outside the EU" and asked "the institutions and Member States to implement the measures referred to in the Joint Communication, including the work on attribution of cyber-attacks and the practical use of the cyber diplomacy toolbox".

On Friday 7 September 2018 the Horizontal Working Party on Cyber Issues (HWPCI) held a first exchange of views on the legal framework for restrictive measures. Following this discussion the EEAS was requested to produce a non-paper that would outline the possibilities for "cyber sanctions".

On 18 October 2018 the European Council adopted conclusions which also stated that the "work on the capacity to respond to and deter cyber-attacks through EU restrictive measures should be taken forward, further to the 19 June 2017 Council conclusions".

In line with the tasking of the HWPCI and in follow-up to the European Council conclusions, the EEAS prepared a non-paper which set out options and principles for a new EU regime of restrictive measures to respond to and deter cyber activities that threaten the security or foreign policy interests of the Union or its Member States.[1] Such a regime could target those involved in these types of cyber activity anywhere, regardless of their nationality and location.

DELETED

2. Horizontal regime or country-specific sanctions

The focus of the vast majority of EU autonomous sanctions regimes[2] is country-specific; there are only two regimes which are thematic: 1) the restrictive measures to combat terrorism[3] and 2) the restrictive measures against the proliferation and use of chemical weapons[4].

1 This non-paper is intended to set out the options for the scope of a possible sanctions regime. It does not contain the legal and technical details for any future legislative proposals **(based on Article 29 TEU and Article 215 TFEU)**, which are to be discussed by RELEX in accordance with the division of responsibilities between working groups. The starting point for any such proposals will be the standard wording for legal acts agreed in the Sanctions Guidelines (document 5664/18), unless stated otherwise in this non-paper.

2 These regimes can consist of EU autonomous sanctions alone (EU only regimes) or they can contain both UN and EU restrictive measure (mixed regimes).

3 The restrictive measures to combat terrorism consist of two horizontal regimes: Council Common Position 2001/931/CFSP on the application of specific measures to combat terrorism and Council Decision (CFSP) 1693/2016 concerning restrictive measures against ISIL (Da'esh) and Al-Qaeda and persons, groups, undertakings and entities associated with them.

4 Council Decision (CFSP) 2018/1544 concerning restrictive measures against the proliferation and use of chemical weapons.

These country-specific regimes do not allow for sanctions for cyber activities as such, and would need to be amended to include a listing criteria specific to such activities. A country specific regime could also foresee / include specific sectoral measures in response to certain cyber activities.

DELETED

The focus of this paper is therefore on a horizontal regime which will allow a flexible response which is not dependent on the location (or locations) from which cyber activities are launched. **Such a horizontal regime is without prejudice to the possibility of including "cyber sanctions" in country-specific regimes.**

3. Scope of the regime

The first question to be answered is what type of cyber activities a sanctions regime should target or respond to. As for all sanctions regimes it is necessary to provide in the legal act a sufficiently clear definition of the scope of the activities which may trigger sanctions.

The following considerations are relevant for defining the scope:

i. As a sanctions regime would be a CFSP instrument, the sanctions must apply to situations which threaten the security or foreign policy interests of the Union or its Member States. In other words, the regime should further strengthen the goals of the CFSP as provided for in Article 21 (2) TEU. As with all restrictive measures, the regime (and the listings adopted on the basis of the regime) should be in conformity with international law.

ii. [~~It should be kept in mind as well that~~] **Furthermore,** each listing needs to adhere to the principle of proportionality.

iii. The scope of the cyber activity targeted should be limited to cyber activities "without right" with a significant effect related to **one or more of the following**:

- access to information systems;
- information system interference;
- information system data interference;
- interception of computer data from an information system;

This includes but is not limited to **("non-exhaustive list")**:

- theft of funds or economic resources through an information system;
- theft of data and major **data** breaches through an information system;
- large scale intellectual property theft through an information system;
- cyber activities that affect the information system related to:
  - (European) critical infrastructure;
  - essential services, including State essential services such as information systems used for elections;
  - **classified information;**
  - **government** emergency response teams.[5]
- cyber activities that access through an information system commercially sensitive data.

iv. The definitions of information systems, system interference, data interference and data interceptions can be taken from Directive 2013/40 on attacks against information systems. The same Directive can provide inspiration for the definition of "without right".

[5] See also the recommendations of the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) agreed on 26 June 2015.

v. For the concept of "significant effect" inspiration could be taken from Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the "NIS Directive"), but also other factors could be taken into account when determining whether such a significant effect occurred such as the amount of economic loss, including to the Member State concerned, or the disruption **caused by** [~~that followed after~~] the cyber activities [~~occurred~~].

vi. For the definition of (European) critical infrastructure reference could be made to Council Directive 2008/114/EC on the identification and designation of European critical infrastructure and the assessment of the need to improve their protection. The NIS Directive could provide guidance for the definition of essential services.

vii. With regard to State essential services the focus could be on key functions such as the provision of information systems used for elections or the functioning of institutions.

viii. **DELETED**

ix. It should be possible to apply sanctions for cyber activities directed against [~~the EU, its Member States, or~~] third States (on a case by case basis, keeping in mind that sanctions are a CFSP instrument).

x. **DELETED** The focus should first and foremost be on the effect[~~,~~] **and** the actual significant harm, of the cyber activities. It could be clarified in the preamble that, as the objective of the regime is to bring about a change in the behaviour of individuals or entities who are **involved in sanctionable cyber activities** [~~seeking to destabilise cyberspace~~], and to have a deterrent and dissuasive effect, the focus should be on cyber activities that are wilfully carried out.

xi. Nevertheless, the scope should also include attempted damaging cyber activities [~~that were unsuccessful but~~] which could have had a significant effect **("the attempt")**. Whether this is the case should be decided by the Council on a case by case basis, **DELETED**

xii. **DELETED**

xiii. [~~A list of non-exhaustive illustrative examples could be added to the description of cyber activities that could be the object of sanctions.~~]

4. Scope of the regime - continued

In line with section 3, the following suggested elements could be used to define the scope[6]:

1. 'Cyber activities' could mean cyber activities without right with a significant effect related to **one or more of the following activities**:

a) access to the whole or to any part of an information system;

b) hindering or interrupting the functioning of an information system;

c) deleting, damaging, deteriorating, altering or suppressing data on an information system;

d) interception of non-public transmissions to, from or within an information system;

[6] **Paragraph 3 provides the foreseen scope of the regime. Paragraph 4 gives further detail and clarifications on definitions and formulations. Unavoidably, there is some overlap between the two paragraphs. Paragraph 4 is without prejudice to the final proposal of the High Representative to be submitted to the Council for discussion in RELEX.**

This includes the following non-exhaustive list of cyber activities [~~These cyber activities include but are not limited to:~~]

a) theft of funds or economic resources, including theft from a Member State, through an information system;

b) theft of data and major data breaches through an information system;

c) large scale intellectual property theft through an information system;

d) cyber activities that affect information systems relating to critical infrastructure in a Member State or a European critical infrastructure;

e) cyber activities that affect information systems relating to the provision of essential services;

f) cyber activities that have an adverse effect on the information systems related to the provision of essential services by Member States, in particular information systems used for:

   a. Elections;

   b. State defence;

   c. State Governance and functioning of institutions;

   d. Functioning of economic and civil infrastructure;

   e. Meeting vital needs of population;

   f. Internal security;

   g. External relations.

g) cyber activities that affect the information systems of [~~the~~] **government** emergency response teams;

h) <u>cyber activities that affect information systems relating to classified information;</u>

i) cyber activities aimed at accessing through an information system commercially sensitive data which, by its nature, procures a significant economic and/or commercial benefit.

2. 'Without right' could mean access to information systems, system interference, data interference or 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 EU or an EU Member State (Article 2 (d), Directive 2013/40).

3. 'Information systems', 'system interference', 'data interference' and 'data interception' could mean:

Information systems: a device or group of interconnected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer 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 (Article 2 (a), Directive 2013/40).

System interference: seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible (Article 4, Directive 2013/40).

Data interference: deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible (Article 5, Directive 2013/40).

Data interceptions: intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data (Article 6, Directive 2013/40.

4. 'Critical infrastructure' and 'European critical infrastructure' could mean:

Critical infrastructure: 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, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions (Article 2 (a), Directive 2008/114).

European critical infrastructure: critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States (Article 2 (b), Directive 2008/114).

5. 'Essential services' could mean:

Essential services: services essential for the maintenance of critical societal and/or economic activities, which depend on network and information systems (article 5 (2) of Directive 2016/1148).

6. When determining the significant effect, the following non-cumulative factors could be taken into account:

a) the scope, scale, duration, intensity, complexity, sophistication, impact, severity of and/or disruption caused by the cyber activity, including on critical society and /or economic activities, essential services, including State essential services, public order or public safety;

b) the number of people **affected** [~~concerned~~];

c) the number of Member States concerned;

d) the amount of economic loss, including for the Member State concerned;

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

DELETED

5. [~~4.~~] Measures

With regard to the measures, such a horizontal regime could consist of targeted measures: designation of those natural persons or entities identified as being responsible for or involved in the described cyber activities (travel ban and/or asset freeze).

DELETED First of all, sectoral measures are country specific. **DELETED**

Secondly, as restrictive measures are always targeted, it would be difficult in advance to specify which sectoral measures would be effective in a particular case. **DELETED**

6.[~~5.~~] Targeted measures (designations)

Designation by the Council usually has the effect of applying:

1. A travel ban;
2. An asset freeze – this applies a freeze to all the assets held in the EU of the designated person/entity and prohibits making any funds or economic resources available.

Standard exemptions and or derogations may be provided for, as is common when a travel ban or asset freeze is imposed[7].

Natural persons can be subject to both a travel ban and an asset freeze. In case of entities only an asset freeze can be applied. **DELETED**

It is therefore proposed to follow the usual practice that if a natural person is designated they will be made subject to an asset freeze and travel ban and that entities should be subject to an asset freeze.

In addition to the standard exemptions foreseen for the travel ban it should be mentioned that Member states may grant exemptions where travel is justified for the purpose of a judicial process.

[7] Such as entries into the territory of a Member State on grounds of attending intergovernmental meetings, or the release of frozen funds to satisfy basic needs.

7. [~~6.~~] Criteria for targeted measures (designations)

Designations by the Council are only possible if the legal acts provide for designation criteria. The Council has broad discretion in establishing these criteria. Here, the criteria could target:

a) Persons and entities responsible for or otherwise involved in (e.g. by participating, facilitating, allowing, preparing, encouraging**, contributing** or supporting) committing the activities referred to in paragraph 3;

b) Persons and entities that have attempted [~~to commit~~] a cyber activity referred to in paragraph 3;

c) [~~State actors from third countries that have allowed or contributed, including indirectly or by encouraging, to the carrying out of cyber activities referred to in paragraph 3~~.]

As for all EU autonomous designations, **the regime should ensure a robust review process and the Council should take into account all relevant elements with respect to de-listing.** The usual approach is **that the Decision foresees** an annual review.

DELETED **Essentially, de-listing is appropriate when the criteria for listing are no longer met**[8]. **DELETED**

[8] **See also section III of the EU Best Practices for the effective implementation of restrictive measures (document 8519/18).**

8. [~~7.~~] Targeted measures (designations) - evidence

As with all designations under any existing sanctions regime, listings for cyber activities must be legally robust, **DELETED**. This means, in accordance with the case law of the Court of Justice, the following:

- Listings should be accompanied by **an** accurate, up-to-date**, defendable** and clear statement of reasons and include the necessary identifying information;
- Statements of reasons must identify the individual, specific and concrete reasons for the listings;
- Listings must respect human rights and fundamental freedoms;
- Listings must be proportionate to their objective (principle of proportionality).

The right to effective judicial protection requires the Council to provide, in the event of a challenge, information or evidence substantiating the reasons for the adoption of restrictive measures against natural or legal persons.

DELETED The Rules of Procedure of the General Court also foresee a specific procedure for the handling of classified information, but this specific procedure has so far not been used.

It should also be kept in mind that review by the Court of Justice is not limited to procedural requirements; it is a full review to ensure that a listing is taken on a sufficiently solid factual basis. That entails a verification of the factual allegations in the summary of reasons underpinning the listing, whereby at least one of the reasons provided should support the listing.

The designation of a person or entity should be distinguished from attribution of responsibility for cyber activities to a third State. Attribution remains a sovereign political decision and a national prerogative. Every Member State is free to make its own determination with respect to attribution. Designation is possible when the Council considers, in the exercise of its jurisdiction that the person / entity falls under the designation criteria of the legal act, taking into consideration the objectives of the measures as expressed in the preamble of the legal act.

DELETED