

Brussels, 25 February 2020

**Interinstitutional files:
2018/0331(COD)**

WK 1838/2020 INIT

LIMITE

**CT
ENFOPOL
COTER
JAI**

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Delegations
Subject:	Proposal for a Regulation on preventing the dissemination of terrorist content online - comments by Member States

Delegations will find in Annex comments by Member States on the above mentioned proposal which were received in January 2020.

TABLE OF CONTENTS

	PAGES
AUSTRIA	1
BULGARIA	2
CZECHIA	3
DENMARK	6
ESTONIA	7
FINLAND	8
FRANCE (together with English courtesy translation)	11
HUNGARY	22
IRELAND	25
NL	29
SLOVENIA	32
UK	33

From: Helena.DOBERER@bmeia.gv.at <Helena.DOBERER@bmeia.gv.at>

Sent: Tuesday, January 21, 2020 3:03 PM

To: Marijan.Jelinek@mvep.hr; kmamic@mup.hr; [DL] JAI TWG <twg@consilium.europa.eu>

Subject: AW: TCO - follow-up to today's JHA-counsellors' meeting

Dear Marijan,

Dear Colleagues,

Please find some answers of the questions you raised during the last TCO meeting:

- Competent authority: an important point for AT is to have the possibility to nominate more than one single authority for the different instruments of the regulation
- Art. 5, referrals: AT can show some flexibility in deleting referrals from the scope of this regulation as this instrument will nevertheless be existent
- Article 13(4): AT suggests to limit the scope to relevant information and in this line to go back to previous proposal "an imminent threat to life" or "critical infrastructure"
- Unfortunately I didn't receive any feedback concerning "public" and HSP nor an alternative proposal to "promoting"; I will come back to you if I will receive helpful suggestions from Vienna

Hope this little feedback is still helpful for you.

Best regards,

Helena

Permanent Representation of Austria to the EU

Department Home Affairs

Helena Doberer

Counsellor

+32 2 2345 290

Mobil +32 473 537 193

Avenue de Cortenbergh 30, 1040 Bruxelles

helena.doberer@bmeia.gv.at

bmeia.gv.at

facebook.at/Aussenministerium | twitter.com/MFA_Austria | instagram.com/mfa_austria

From: Dimana DOYNOVA <dimana.doynova@bg-permrep.eu>

Sent: Tuesday, January 21, 2020 2:41 PM

To: Marijan.Jelinek@mvep.hr; kmamic@mup.hr; [DL] JAI TWG <twg@consilium.europa.eu>

Cc: imaleksandrov.14@mvr.bg

Subject: BG comment - TCO

Dear Colleagues,

After the internal consultations back in Sofia on the questions you raised at our last JHA Counsellors meetings, I was informed by my experts that we are not in the position to support the proposal on the definition of "competent authority". We do not have such a functionally independent administrative authority who to review ex officio the decisions of the competent authority. For us this would mean to create a totally new authority and to reorganize our system which we think is unnecessary since we already have an authority that works and that would be best placed to fulfill the obligations under the regulation. We are of the opinion that MS should remain flexible to choose their own authorities and that the status quo of the national institutions is preserved as much as possible. Therefore we prefer sticking to the general approach as far as this issue is concerned.

Regarding the other issues in the email that was sent after our meeting last week – we are quite flexible and we are ready to support your efforts on other issues as well, but the definition of the competent authority is really a red line for us.

Kind regards,

Dimana

CZ comments on draft TCO Regulation

- following JHA Councillors' meeting on January 17, 2020

Article 1:

- FI wording proposals for Articles 1 and 2

Art. 1 – Building blocks

Line 76

While CZ believes that a general exception as requested by EP may be agreed upon, for the purposes of ongoing negotiations, CZ may accept this compromise wording of new Art. 2(2).

- 4 column table

Line 78

CZ supports AM 47.

"public"

Previously, CZ has made following proposal to amend recital 10:

Whatever term is used (public, third parties), the Council should be clear what it wants to cover. CZ proposed following explanation in recital 10, because CZ is among the Member States that do not want to lose all very large and fairly artificial finite groups (e.g. where one may send email request and is always added to recipients of next content):

"Information is considered to have been made available to the public where it is shared with an indeterminate number of potential recipients. Accordingly, information is considered not to have been made available to the public where it is exchanged between a finite number of recipients, determined by the person sharing that information, such as in the case of emails or private messaging. Situations where new recipients can enlist themselves, where any recipient may include other persons to receive whole content, or where the person sharing the information is not genuinely determining the recipients, should not be understood as exchanges between a finite number of recipients."

However, since the position of the Commission is that large closed groups remain uncovered (even though it is debatable whether the person sharing the information does indeed genuinely determine the recipients in such a case), but CZ wishes to address such situations if at all legally feasible, CZ would strongly support additional changes.

Art. 2

- EP proposals on definitions

CZ supports compromise drafts in lines 90 – 94, 96

In line 95, CZ prefers "including by supplying" but may accept "in relation to supplying". As regards "promoting the activities of a terrorist group", it is clear that it is very broad and the EP wording is closer to the 2017/541 Directive. However, in light of operational needs, better operative wording linking "material" to "participation" should be used. CZ proposes:

"promoting/encouraging or soliciting (directly or indirectly) a participation of any person or a group of persons in the activities of a terrorist group ...".

In line 97, we should begin by "**constituting** a threat". More importantly, since terrorist offences are defined in Art. 2(4) to include threats, threats should be excluded in line 97, similarly to line 96. We do not wish to address "threats to threaten" as that would be ridiculed. Consequently, reference should be to Art. 3(1)(a) to (i) of Directive 2017/541 only.

- Presidency proposal of 15 January

Line 83

Presidency proposed this amendment of definition of HSP:

'hosting service provider' means a provider of information society services consisting in the storage of information provided by and at the request of the content provider and in making the information stored available to the public. Electronic communications services as defined in Directive (EU) 2017/1972 are not considered hosting service providers.

And this additional definition:

Available to the public means available on the application layer of a service provided by a hosting service provider. In the sense of this regulation this means the layer of the service which can be perceived directly by any natural person visually, in auditory form or by any other bodily form of perception. The perception of this layer through any natural person must be possible without special means of access to the backend infrastructure of the hosting service provider itself or to technical infrastructures of third companies which are necessary for the functioning of the service provided by the hosting service provider.

CZ comments:

In general, we **strongly recommend** to use already established definitions from other EU instruments. In this regard, new language such as the first part of definition of HSP is problematic because it has no established meaning in the IT industry and may lead to divergences.

Reference to "electronic communication services" should be corrected – the right number of relevant directive is 2018/1972.

Follow-up by Presidency email of January 17:

Article 2 (9a)

PRES proposed this definition:

"competent authority" means a designated judicial authority or functionally independent administrative authority or an administrative authority subject to scrutiny by a functionally independent administrative authority in the Member State.

CZ does not agree to such proposal, in particular to words "functionally independent", because such hybrid agencies do not fit into our institutional setup. Independence of decision-making body is not even requirement under European Convention on Human Rights, as it is enough if the decision is based on law and appealable in courts. CZ can accept "impartial" or "subject to rule of law" or "subject to independent review" instead. (Parallels with prosecutors in contradictory criminal proceedings are misleading.)

CZ could accept "functionally independent administrative authority" and "administrative authority subject to scrutiny by a functionally independent administrative authority" if there is additional alternative - "administrative authority subject to independent/judicial review".

CZ could also accept single such authority.

CZ can accept ex officio review, but not a duty to review decisions systematically.

Article 5 and Line 100

CZ believes that referrals need not be regulated at all, as they work at present without any regulation. Since the draft regulation offers two possible options (removal orders or referrals) for the same case without any distinctions or limitations, it will be fraught with unintended consequences (such as courts ruling that milder option (referral) be always used first etc.). Therefore, we should either make referrals applicable in different set of cases, or leave them to current practice based on e-commerce directive.

Article 13(4)

CZ proposes to focus on "evidence" and "threats", as the first serves to limit the scope of "content" and the second does not need legal qualification and is politically justifiable. The wording could be: "... become aware of any evidence of terrorist offences **or threats thereof**, they shall ...".

(end of file)

The TCO proposal - Comments by the Danish delegation

First, the Danish delegation would like to welcome the Croatian Presidency and wish you the best of luck, especially with regard to the TCO proposal. Denmark supports the overall aim of the proposal, as it is our belief that it will be an important tool in our essential battle against terrorism.

Secondly, the Danish delegation would like to thank the Presidency for the opportunity to submit written comments on Article 1 and 2 of the TCO proposal and for the interest expressed in section 114 e of the Danish Criminal Code.

The Danish delegation hopes, that the description below will answer the questions raised on section 114 e. The Danish Delegation will be at your disposal if you have further questions.

Article 2 (9 a)

The Danish delegation can support the suggested wording on Article 2 (9 a) and especially welcomes, that "a competent authority" can also be an administrative authority subject to scrutiny by a functionally independent administrative authority in the Member State.

Section 114 e of the Danish Criminal Code

Imprisonment for a term not exceeding six years is imposed on any person who otherwise facilitates the activities of a person, a group or an association committing or intending to commit an act falling within section 114 (terrorist acts), 114 a (terror-like acts), 114 b (financing of terrorism), 114 c (recruitment for acts of terrorism, terror-like acts or financing of terrorism) or 114 d (training for terrorist acts, terror-like acts or financing of terrorism) of the Danish Criminal Code. If the relevant person is a member of armed forces, the sentence may increase to imprisonment for a term not exceeding ten years, or in particularly aggravating circumstances to imprisonment for a term not exceeding 16 years. Especially situations in which the relevant person has participated in combat are considered particularly aggravating circumstances.

Section 114 e of the Danish Criminal Code is a special provision on liability for participation. The provision includes any support or aid to a person, a group or an association committing or intending to commit the acts falling within the above-mentioned sections 114-114 d of the Danish Criminal Code. Decisive is whether the action is designed to promote the criminal activities. Criminal liability is limited by the fact that the person who facilitates the activities must have intent for the person, the group or the association to commit criminal activities of the before mentioned character as part of their business or general purpose.

The provision is subsidiary in relation to the general responsibility for participation in criminal activities covered by section 23 of the Danish Criminal Code. This entails that if a person has a concrete intention to participate in one of the acts mentioned in sections 114-114 d of the Danish Criminal Code, penalties must be imposed under that provision instead of section 114 e.

Examples of actions that may be covered by the provision are professional general advice, not directly related to a specific terrorist act, to an organization committing or intending to commit terrorist acts, which is known to the advisor. Pure expressions of sympathy with terrorist organizations are on the other hand not prohibited by the provision.

From: Liina Pello <Liina.Pello@siseministeerium.ee>

Sent: Wednesday, January 22, 2020 12:42 PM

To: Marijan.Jelinek@mvep.hr; kmamic@mup.hr; [DL] JAI TWG <twg@consilium.europa.eu>

Cc: Anni Aleksandrov <Anni.Aleksandrov@mfa.ee>

Subject: TCO

Dear Presidency team,

Wish you all the best for a fruitful and productive Presidency!

We are sorry for the late reply, but these articles raised a debate and some of the experts responsible were unavailable for comments in the past days. These are our initial thoughts regarding the ideas presented at the TCO counsellors meeting on 16.01:

- 1) With regards to the definition of "made available to the public" we are afraid that it would narrow the scope of action by competent authorities that is currently allowed for by the AVMD (EU) 2018/18, recitals 17 and 18 and articles 6(b) and 28(b)(1c). Does this text proposal encompasses messaging groups of a certain size, password-protected blogs/forums/groups etc? If it would not, we would have to work further with the text. Additionally, we are on the opinion that technological terms (such as the "application layer") should not be used in the text of the regulation. It is not certain what exactly does "application layer" mean and technology is in constant change. It would be better if the text is technologically neutral.
- 2) With regards to the definition of competent authority, there should be the possibility to appoint more than one authority. This actually guarantees better compliance with fundamental rights – that is, if the competent authority issuing removal orders and the competent authority enforcing the penalties and overseeing the implementation of proactive measures are different. It is our opinion that to the greatest extent possible the MS should be free to choose the competent authority depending on their size or legal system. This is not just a matter of principle, especially for smaller MS.

Kind Regards

Liina Pello

Adviser

Estonian Ministry of the Interior

+372612 5040 | +3725886 5352

Pikk 61, 15065 Tallinn

From: Puiro Johanna SM

Sent: Tuesday, January 21, 2020 3:19 PM

To: JAI INTERNAL SECURITY

Cc: paivi pietarinen UM ; Mari Hämäläinen

Subject: VS: TCO - follow-up to today's JHA-counsellors' meeting

Dear Anne Cecilie and Croatian Presidency team,

The Finnish comments are the following:

1. Article 1 line 76

In order to accommodate EP's concern in AM 45 Finland supports the idea of adding a new para 2 to Article 2. This new paragraph would give guidance to those who determine whether the content is terrorist content or not. Finland does not support an exemption clause that would leave all the artistic etc content outside the scope of this Regulation.

Wording supported:

A new para 2 to Art 2:

When determining whether an item of information provided by a content provider constitutes 'terrorist content' within the meaning of point (5) of paragraph 1, account shall be taken of in particular the need to adequately protect, in accordance with Union law, the freedom of expression and information, the freedom and pluralism of the media as well as information disseminated for educational, journalistic or research purposes or for the purposes of preventing or countering terrorism.

2. Definition of the word public

Finland appreciates the efforts to find a definition for the word "public". In this proposal it is said: *"This means the layer of the service which can be perceived directly by any natural person"* - what does "directly" mean in this context? What happens if a login is required and thereafter all the content is available? Is that covered by the Regulation?

If in need of additional wording, one idea might be:

Recital 10:

In order to cover online hosting services through which terrorist content is disseminated, this Regulation should apply to information society services that store information and material provided by a recipient of the service at his or her request and that make such information and material available to the public irrespective of whether the storing or making available to the public of such information [and material] is of a mere technical, automatic or passive nature. Storing content consists of holding data in the memory of a physical or virtual server; this should exclude from the scope of this Regulation mere conduits and other electronic communication services within the meaning of [European Electronic Communication Code], providers of caching services, as well as other services provided in other layers of the Internet infrastructure, such as registries and registrars, and DNS (domain name system) and adjacent services, such as payment services or DDoS (distributed denial of service) protection services.

Information is considered to have been made available to the public where it is shared with an indeterminate number of potential recipients. Accordingly, information is considered not to have been made available to the public where it is exchanged between a finite number of recipients determined by the person sharing that information, such as in the case of emails or private messaging.

Situations where new recipients can enlist themselves, where any recipient may include other persons to receive whole content, or where the person sharing the information is not genuinely determining the recipients, should not be understood as exchanges between a finite number of recipients.

3. Definition of “hosting service provider”

In the Presidency proposal we find it a bit unclear what is meant with “Electronic communications services as defined in Directive (EU) 2017/1972 are not considered hosting service providers.” In AM 49 the wording was “It does not apply either to electronic communications services as defined in Directive (EU) 2017/1972.” Should we refer to electronic services as such like proposed by the EP. It very important that this definition is clear.

4. Competent authority

Presidency proposal seems acceptable as long as MS can designate different authorities for different tasks in this Regulation.

5. Referrals

Finland can accept deleting all the references to referrals.

Best regards,

Johanna Puiro

Note de commentaires

Commentaires de la France sur le projet de règlement relatif à la prévention de la diffusion de contenus à caractère terroriste en ligne – récapitulatifs des positions françaises.

Les autorités françaises expriment leur satisfaction à l'égard du calendrier ambitieux proposé par la Présidence croate illustrant notre volonté commune de faire aboutir ce texte dans les meilleurs délais.

A la suite de l'adoption de la position en première lecture du Parlement européen, les autorités françaises souhaitent faire valoir les points prioritaires suivants. L'objectif est de faire aboutir un texte qui ne soit pas moins-disant par rapport à la pratique opérationnelle actuellement constatée par les services. Les autorités françaises ont donc à cœur d'apporter une contribution constructive dans les débats afin d'en faciliter le cours.

Dans ce contexte, les autorités françaises souhaitent faire part des observations suivantes qui visent à enrichir encore cette proposition.

1. Points d'attention prioritaires aux yeux des autorités françaises :

1.1. Sur le prononcé des mesures d'injonction de suppression (articles 4 et 15)

- ne pas revenir sur la mention « dans l'heure après réception de la demande d'injonction de retrait » contenu dans l'orientation générale du Conseil. Compte tenu de la vitesse de propagation des contenus sur internet, il est en effet impératif de supprimer les contenus terroristes dûment signalés par les autorités habilitées au plus vite afin de limiter leur viralité. Au-delà d'une heure, 30 % des contenus sont déjà disséminés sur internet. Nous saluons la consécration de ce respect de retrait dans l'heure arrêté dans la position en première lecture du Parlement, même si l'introduction d'un contact préalable de 12 heures avant l'envoi d'une première injonction de suppression semble à cet égard introduire une certaine lourdeur.

- soutenir l'orientation générale du Conseil qui permet à toute autorité compétente nationale au sein de l'UE d'émettre une injonction de suppression, là où la position du Parlement limite ce pouvoir à la seule autorité compétente de l'État d'établissement. À titre d'exemple, lors de la diffusion en direct de l'attaque de Christchurch, la plateforme française PHAROS a reçu des signalements relatifs à 37 mises en ligne distinctes de la vidéo qui nécessitaient de prendre autant d'injonctions de retrait. Ces signalements ne concernaient pour l'essentiel que des sites utilisés majoritairement par des internautes français. À l'échelle de l'Union, c'est contre des centaines de mises en ligne effectuées en quelques minutes qu'il faut pouvoir lutter si l'on veut pouvoir contrer ce type de vidéos. Cela requiert une action simultanée de plusieurs autorités nationales, chacune prenant des injonctions pour l'ensemble du territoire de l'Union. Aucune autorité nationale ne peut y faire face seule. Pour gagner en réactivité, il est donc nécessaire que chaque État membre puisse directement imposer une demande de retrait, sans passer par l'intermédiaire de l'État membre hébergeur du service Internet concerné par cette demande.

1.2. Sur la nature de l'autorité compétente pour émettre des injonctions de retrait (article 17)

Conformément à l'orientation générale adoptée par le Conseil, le choix de l'autorité compétente, administrative ou judiciaire, pour émettre des injonctions de retrait devrait être laissé aux États membres. En effet, certains pays disposent déjà d'une telle autorité et de procédures efficaces mises en place pour signaler les contenus à caractère terroriste qui ont apporté des résultats, en lien notamment avec Europol (c'est le cas de la plateforme PHAROS pour la France souvent érigée en exemple). Cette autorité compétente devra respecter la protection des données personnelles et faire l'objet d'un contrôle par une autorité indépendante.

S'agissant de la plateforme de signalement PHAROS, ayant le statut d'autorité administrative, son activité de retrait et de blocage est contrôlée par une personnalité qualifiée, désignée par la CNIL (autorité administrative indépendante) et toutes ses décisions peuvent être contestées devant le juge administratif, avec possibilité de référé en 24 heures. Cette procédure administrative fournit des résultats convaincants. La France dans ce cadre n'est pas défavorable à une distinction entre autorité opérationnelle chargée des injonctions de retrait et des mesures préventives et autorité judiciaire ou administrative indépendante chargée des sanctions.

1.3. Sur les mesures préventives obligatoires (article 6)

Les mesures préventives permettent de prévenir la dissémination de contenus terroristes déjà référencés comme tels, notamment à l'aide d'algorithmes de filtrage, en limitant les risques de récurrence. Elles permettraient aussi de lutter contre la diffusion en direct de nouveaux contenus partageant les références déjà identifiées, en conduisant à leur blocage avant même leur diffusion. Le recours à la technologie, comme les bases de données de référencement de contenus terroristes (notamment celle mise en place au sein d'Europol) permet de reconnaître, avant leur publication sur Internet, les contenus qui ont la même « signature numérique ». À titre d'exemple, depuis 2015, de nombreux contenus terroristes ont été diffusés sous le sigle « 19HH », en référence aux 19 terroristes impliqués dans les attentats du 11 septembre 2011 et aux deux tours jumelles, sur différents services d'hébergement (YouTube, Archives, Telegram, Dailymotion, Files.fm,...). La mise en place de mesures préventives utilisant le mot clé « 19HH » aurait permis aux opérateurs concernés de retirer d'eux-mêmes ces contenus, après vérification, sans avoir à recevoir de signalement ou d'injonction pour ce faire.

Nous demandons donc de soutenir l'orientation générale du Conseil, qui prévoit explicitement la possibilité pour l'État d'établissement d'imposer des mesures préventives en cas d'inaction d'une plateforme. Pour mémoire, cette possibilité est également dans la position du PE mais sur un mode dégradé.

De plus, il convient de signaler qu'Europol prévoit d'affecter près de 20 millions d'euros au soutien aux petites entreprises via la mise en place d'outils automatisés (mise à disposition de moyens et outils techniques, faciliter l'accès à son unité de référencement, etc.). Pour tenir compte des contraintes de ces petits opérateurs, il est nécessaire, à l'article 9, de conserver la rédaction du Conseil et de la Commission, dans laquelle les vérifications humaines ne doivent pas être systématiques mais uniquement « quand cela est approprié ». A tout le moins, il conviendrait de restreindre la restriction voulue par le Parlement en précisant que le retrait d'initiative peut être automatisé dès lors que le contenu a déjà été qualifié par un autre opérateur ou une autorité nationale comme terroriste après intervention d'une personne humaine.

2. Points nécessitant une attention particulière

2.1. Sur la différenciation entre petites et grandes plateformes

Les autorités françaises estiment que l'article 18 sur les sanctions contient déjà des dispositions relatives à la proportionnalité (jusqu'à 4% du C.A) et que dans les faits, lors de l'instruction, il sera tenu compte de la taille de la plateforme et de ses moyens. Il est donc inutile d'alourdir le texte sur ce point. Enfin, les autorités françaises insistent sur le fait que la phase de sanctions sera nécessairement précédée d'une phase pédagogique. Cette dernière doit être vue comme un outil de reprise d'un dialogue rompu.

2.2. Sur l'articulation du règlement avec d'autres textes

Les autorités françaises font part de leurs interrogations sur l'articulation proposée à l'article 3 § 2(b) avec la directive SMA.

Pour mémoire, la directive SMA prévoit que les services de médias sociaux peuvent être assimilés à des plateformes de partage de vidéo s'il est avéré que la « fourniture de programmes et de vidéos créées par l'utilisateur » constitue, à défaut de l'objet principal, une « fonctionnalité essentielle » du service de médias sociaux en question.

Or, l'articulation proposée par le Parlement européen semble indiquer que lorsqu'un fournisseur de services d'hébergement en ligne relèverait de la définition de plateforme de partage de vidéos, ses obligations se limiteraient à celles prévues par l'article 28b §1(c) et §3 de la directive SMA.

Les autorités françaises soulignent que ces obligations ne peuvent concerner par définition que des contenus audiovisuels, et non les autres contenus (écrits, images, sons) ; la proposition du Parlement européen pourrait donc engendrer une exclusion des plateformes de réseaux sociaux. Les autorités françaises font part de leur grande vigilance à cet égard, en ce qu'elles considèrent essentiel d'assurer un haut niveau de protection des populations à l'égard des contenus terroristes.

Elles considèrent donc utile de reformuler la proposition du Parlement européen afin de permettre une plus grande clarté quant aux configurations où les deux textes pourraient trouver à s'appliquer.

S'agissant plus particulièrement de la mention de la directive e-commerce, les autorités françaises sont d'avis de conserver la rédaction initiale du Conseil et d'éviter d'inscrire que le projet de règlement est sans préjudice de la directive e-commerce. En effet d'une part il n'y a pas de hiérarchie juridique entre les deux textes et d'autre part le projet de règlement va plus loin que la directive qui mentionne seulement une mise en jeu de la responsabilité des plateformes dès lors que les fournisseurs de service et d'hébergement suppriment rapidement un contenu dès lors qu'ils en ont connaissance.

2.3. S'agissant de l'article 11 : information du fournisseur de contenus

Les autorités françaises font valoir qu'il semble plus adapté de prévoir une suspension de l'information de l'auteur du contenu terroriste durant 6 semaines, renouvelable une fois lorsque c'est justifié, en cas de risque d'interférences avec une enquête judiciaire, que de prévoir un délai de suspension global maximum de 6 semaines. En ce sens, elles accueillent favorablement la proposition de compromis soumise par la présidence finlandaise en décembre 2019.

2.4. Sur la conservation des contenus

Tant lors de la phase du renseignement que lors des enquêtes judiciaires, il est nécessaire que les services de renseignement puissent avoir accès aux contenus terroristes retirés. À ce titre, les autorités françaises remercient la Présidence pour la conservation de la formulation obtenue lors de l'orientation générale ("*the prevention, detection, investigation and prosecution of terrorist offences*" ; ligne 158).

3. Points qui pourraient faire l'objet de compromis

3.1. Sur la question des contenus terroristes dans les CGU

Les autorités françaises indiquent qu'il serait souhaitable de voir figurer l'interdiction des contenus terroristes dans les CGU des plateformes de manière explicite, cette démarche étant un premier pas intéressant dans la régulation des CGU par le législateur européen. Cela obligera les opérateurs à tenir compte des signalements adressés par les particuliers, lesquels constituent un complément nécessaire à l'action des autorités nationales. L'expérience de PHAROS montre en effet que la prévention des contenus terroristes en ligne ne peut reposer sur les épaules des seuls pouvoirs publics. Cela doit être l'affaire de tous.

3.2. Sur les signalements (article 5)

Outre le fait que ce dispositif (en complément des injonctions de retrait émanant des autorités compétentes aux articles 4 et 17) permet d'inclure les agences européennes (notamment l'EU IRU d'Europol) et de favoriser des synergies et une meilleure coopération dans la lutte contre la propagation des contenus terroristes en ligne, les autorités françaises considèrent que ce point participe à l'efficacité du dispositif.

Évaluer en priorité des signalements venant d'Europol et des autorités compétentes à l'aune de leurs propres CGU constitue un moyen efficace et rapide d'alerter les fournisseurs quant à la présence éventuelle de contenus terroristes sur leurs plateformes. Enfin, les autorités françaises attirent l'attention sur le fait que les signalements de l'article 5 constituent un régime intermédiaire entre les

signalements des particuliers se référant aux CGU des FSH (qui ne sont pas traités dans le projet de règlement) et les injonctions de retrait. En cela, les signalements de l'article 5 sont un outil de gradation de la réponse publique et de proportionnalité, principes auxquels la France et de nombreux États membres sont attachés et qui furent des points d'attention majeurs lors des négociations au Conseil. Les autorités françaises estiment donc utile de reconsidérer une telle suppression de l'article 5.

3.3. S'agissant du caractère public de la diffusion

Les autorités françaises soulignent qu'elles s'accommodent du caractère public de la diffusion des contenus à caractère terroriste si tant est que le caractère public couvre bien toute diffusion de contenus à caractère terroristes via les réseaux sociaux, tel que cela avait été le cas pour l'attentat de Christchurch.

3.4. Points divers

Le rappel de l'importance des libertés fondamentales à l'article 1^{er} proposé par le Parlement peut être de nature à rappeler la nécessité absolue de prendre en compte ces principes dans la mise en œuvre du règlement. Toutefois, concernant les contenus éducatifs, de recherches, journalistiques, radicales, polémiques ou controversés, la rédaction proposée par le Parlement doit nécessairement être revue. Telle quelle, elle conduirait à permettre la dissémination de contenus visant clairement à de la propagande terroriste dès lors que ses relais prennent la précaution d'afficher un pseudo-but éducatif ou polémique.

Les termes du considérant 9 dans la version du Conseil sur ce sujet (les deux dernières phrases) sont exempts de ce risque et devraient donc être repris tels quels, les propositions du PE sur ce même considérant pouvant pour la plupart être utilement incorporés dans le compromis final.

S'agissant de la définition des contenus terroristes, si les autorités françaises accueillent favorablement l'alignement de la définition sur la directive 2017/541, elles indiquent leur préférence pour le maintien du texte de l'orientation générale du Conseil. À titre de compromis, elles peuvent accepter l'ajout du point (da) sur la description de la commission d'une infraction terroriste (amendement 57, ligne 97).

Enfin, s'agissant de l'introduction d'une signature électronique, il faut veiller à ce qu'elle n'implique pas la désignation du nom et du prénom d'un agent public, ce qui revient à désigner une cible aux groupes terroristes. La France, qui a déjà vu plusieurs de ses policiers être assassinés chez eux par des terroristes, ne peut accepter de leur faire courir un tel risque, et le compromis retenu devra tenir compte de ce risque.



Council of the
European Union

Brussels, 22 January 2020
(OR. fr)

SN 1273/20

LIMITE

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Comments by France concerning the draft Regulation on preventing the dissemination of terrorist content online – overview of French positions

The French authorities wish to express their satisfaction with the ambitious timetable proposed by the Croatian Presidency, which demonstrates our shared desire to bring this text to a conclusion as swiftly as possible.

Further to the adoption of the European Parliament's first-reading position, we wish to raise the key issues below. The aim is to produce a text which does not lag too far behind the operational practices currently observed by the services concerned. We are therefore keen to make a constructive contribution to the discussions in order to facilitate the process.

In that context, we wish to make the following observations, which are designed to further enhance this proposal.

SN 1273/20

JAL.1

yes/ets/sto/LB/fc

LIMITE

1
EN

1. Key focus areas for the French authorities:

1.1. Imposition of measures relating to a removal order (Articles 4 and 15)

- The wording ‘within one hour from receipt of the removal order’ in the Council’s general approach should be maintained. Given the speed with which content spreads on the internet, it is imperative to remove terrorist content duly reported by the competent authorities as quickly as possible in order to prevent it from going viral. After an hour, 30 % of content has already spread online. We welcome the fact that the Parliament’s first-reading position preserves the requirement to remove content within the hour, although in that respect the added requirement to make contact 12 hours before issuing a first removal order would appear to be somewhat of a hindrance.
- We support the Council’s general approach, which allows any competent national authority in the EU to issue a removal order, while the Parliament’s position limits that power to the competent authority of the Member State of establishment only. By way of example, when the Christchurch attack was being live streamed, the French platform PHAROS received reports concerning 37 separate video posts, which required an equal number of removal orders to be issued. For the most part these reports concerned sites visited mainly by French internet users. At EU level, it must be possible to take action against hundreds of posts made in a handful of minutes if we want to be able to tackle this kind of video. That requires simultaneous action by several national authorities, each one issuing removal orders for anywhere in the EU. No national authority can deal with this on its own. In order to become more responsive, each Member State needs to be able to impose a removal order directly without going through the Member State in which the relevant internet service is established.

1.2. Nature of the authority competent to issue removal orders (Article 17)

In accordance with the Council's general approach, the choice of the administrative or judicial authority competent to issue removal orders should be left to the Member States. Certain countries already have such an authority and effective procedures in place for reporting terrorist content which have yielded results, in particular as regards Europol (such as France's PHAROS platform, for example). This competent authority will have to comply with the protection of personal data and be subject to control by an independent authority.

As regards the PHAROS alert platform, which has the status of an administrative authority, its activities in relation to the removal and blocking of content are overseen by a qualified person designated by the French data protection authority, CNIL (an independent administrative authority), and any of its decisions may be challenged before the administrative court, with the possibility of referral within 24 hours. This administrative procedure delivers convincing results. In this context, France is not opposed to a distinction between an operational authority responsible for removal orders and preventive measures and an independent judicial or administrative authority responsible for penalties.

1.3. Mandatory preventive measures (Article 6)

Preventive measures make it possible to prevent terrorist content that has already been flagged as such from spreading, in particular by means of filtering algorithms, limiting the risk of recurrence. They would also help to prevent live streaming of new content which includes references to anything that has already been flagged, causing that content to be blocked even before it is published. The use of technology, such as databases of flagged terrorist content (including Europol's), makes it possible to recognise content with the same 'digital signature' before it is published online. As an example, since 2015 an array of terrorist content has been published under the acronym '19HH' – a reference to the 19 terrorists involved in the attacks on 11 September 2001 and to the Twin Towers – on various hosting services (YouTube, Archives, Telegram, Dailymotion, Files.fm, etc.). If preventive measures using the keyword '19HH' had been in place, the operators concerned would have been able to remove this content themselves, after it had been checked, without having to receive a report or an order to do so.

We therefore call for the Council's general approach to be maintained. This explicitly provides that the Member State of establishment may impose preventive measures if a platform fails to take action. For the record, the EP's position also includes such a provision, but there it is weaker.

It should also be pointed out that Europol plans to allocate nearly EUR 20 million to supporting small enterprises through the setting up of automated tools (making available technical tools and resources, facilitating access to its Internet Referral Unit, etc.). To take account of the constraints on these small operators, the Council's and Commission's wording in Article 9, stating that human verifications should not be carried out systematically but only 'where appropriate', should be retained. At the very least, the restriction sought by the Parliament should be limited by specifying that removal action may be automated if the content has already been characterised, by another operator or a national authority, as terrorist following an intervention by a human being.

2. Points requiring particular attention

2.1. The differentiation between small and large platforms

We believe that Article 18 on penalties already contains provisions relating to proportionality (up to 4 % of turnover) and that in practice, the size of the platform and its resources will be taken into account during the investigation. There is therefore no point in making the text more cumbersome on that count. Lastly, we would stress that the penalties stage must be preceded by a fact-finding stage. This should be seen as a means of resuming a dialogue which has been interrupted.

2.2. Coordinating the Regulation with other texts

We would like to voice our doubts about the proposed link between Article 3(2b) and the Audiovisual Media Services (AVMS) Directive.

For the record, the AVMS Directive provides that social media services may be treated as video-sharing platforms if 'providing programmes' and 'user-generated videos' constitutes, if not the principal purpose, 'an essential functionality' of the social media service in question.

However, it would seem that according to the structure proposed by the European Parliament, where an online hosting service provider comes under the definition of a video-sharing platform, its obligations would be limited to those provided for under point (c) of paragraph 1 and paragraph 3 of Article 28b of the AVMS Directive.

We must stress that, by definition, those obligations can only relate to audiovisual content, and not to other kinds of content (text, images, sound); the European Parliament's proposal could therefore lead to social media platforms being excluded. The French authorities would like to underline that we are very attentive to this issue, since we consider it vital to ensure that the public are granted a high level of protection from terrorist content.

We would therefore consider it wise to reword the European Parliament's proposal in order to make it clear to which types of content both texts could be applicable.

As regards the reference to the e-Commerce Directive in particular, we are in favour of keeping the Council's initial wording, and not stating that the draft Regulation is without prejudice to the e-Commerce Directive. Firstly, there is no legal hierarchy between the two texts, and secondly the draft Regulation goes further than the Directive, which merely refers to platforms' liability coming into play when service and hosting providers take down content quickly when they become aware of it.

2.3. Article 11: Information to content providers

We would argue that it seems more appropriate to provide that disclosure of information to the author of terrorist content be deferred for a period of six weeks – renewable once where justified – if there is a risk of interference with a criminal investigation, rather than providing for a maximum total deferral period of six weeks. We welcome the compromise proposal made by Finland's Presidency in December 2019 in this respect.

2.4. Preservation of content

Intelligence services must have access to removed terrorist content, both during the intelligence-gathering phase and during criminal investigations. We would therefore like to thank the Presidency for keeping the wording of the general approach ('the prevention, detection, investigation and prosecution of terrorist offences'; line 158).

3. Items on which a compromise could be reached

3.1. Terrorist content in the terms and conditions

In our view, it would be desirable to explicitly include the ban on terrorist content in platforms' terms and conditions as that would be a useful initial step towards the regulation of terms and conditions by the Union legislator. It would force operators to take account of referrals sent by private individuals, which are a necessary complement to action by national authorities. Experience of PHAROS has, after all, shown that we cannot rely solely on the public authorities to prevent terrorist content online. Everyone must play their part.

3.2. Referrals (Article 5)

Beyond the fact that this system (combined with removal orders from the competent authorities under Articles 4 and 17) makes it possible to include European agencies (in particular Europol's EU IRU) and to boost synergies and better cooperation in combating the dissemination of terrorist content online, we feel that this point contributes to the effectiveness of the system.

Assessing referrals from Europol and the competent authorities against their own terms and conditions as a matter of priority is a swift and effective way of alerting providers to the possible presence of terrorist content on their platforms. Lastly, we would draw attention to the fact that referrals under Article 5 are an intermediate system between referrals from individuals with reference to the terms and conditions of HSPs, which are not dealt with in the draft Regulation, and removal orders. That being the case, referrals under Article 5 constitute an instrument which would allow progressive degrees of public response and ensure proportionality, principles by which France and many other Member States set great store, and which were the focus of close attention during negotiations within the Council. We therefore consider it useful to revisit the proposed deletion of Article 5.

3.3. The public nature of the dissemination

We would stress that we can agree regarding the public nature of the dissemination of terrorist content if 'public' is understood to cover any dissemination of terrorist content via social media, as was the case with the Christchurch attack.

3.4. Other items

The emphasis on the importance of fundamental freedoms in Article 1 which the Parliament proposes may serve as a reminder of the imperative need to take these principles into account in the implementation of the Regulation. However, as regards educational, research, journalistic, radical, polemical or controversial content, the wording proposed by the Parliament must be revised. As it stands, it would allow content clearly intended as terrorist propaganda to be disseminated, if those who do so take the precaution of indicating a purportedly educational or polemical purpose.

The wording of the Council's version of recital 9 on this subject (the last two sentences) does not carry this risk and should therefore be adopted verbatim, since most of the EP's proposals on this recital can appropriately be incorporated in the final compromise.

As for the definition of terrorist content, although we welcome the fact that the definition is in line with Directive 2017/541, our preference would be for the text of the Council's general approach to be kept. As a compromise, we could accept the addition of point (d a) on the description of the commission of a terrorist offence (amendment 57, line 97).

Lastly, as regards the introduction of an electronic signature, care must be taken to ensure that it does not involve stating the surname and first name of a public official, which would be tantamount to indicating a target for terrorist groups. France, several of whose police officers have already been murdered in their homes by terrorists, cannot accept exposing them to such a risk, and the compromise adopted must take account of this risk.

NOTE

from the Hungarian delegation to Terrorism Working Party (TWP)

Subject: Proposal for a Regulation on preventing the dissemination of terrorist content online

Specific comments regarding the draft compromise proposal by the Presidency issued on 17th of January 2020 on JHA CGUNSELLORS meeting

Line 72, AM

Hungary has concerns regarding the expression of "public" in line 72 AM41, since it would substantially hinder the effectiveness of the TCO Regulation. If this change would be accepted, then hosting providers could not be obliged to remove terrorist contents circulated within closed user groups. Terrorist propaganda contents are in many cases hidden behind a fully legal, innocuous looking public front page and they are available for download only after a registration. If there are proper tools available for the hosting providers for the identification terrorist contents within their infrastructure, it is not reasonable to limit the use of such tools only to the removal of contents available to the full public.

In our view, the definition drawn up by the Presidency still does not solve the problem outlined above, since the definition interprets public access only to subscriptions to the service as a whole, and not to content with specific authentication within the service.

Line 76, AM 45

Line 78, AM 48

Hungary basically supports the compromise text proposal. However, we can be flexible in order to reach the compromise on the issue.

Line 90-94, AM 51, 52, 53, 54.

Hungary basically supports the compromise text proposal of the Finnish Presidency.

Line 95, AM 55

Regarding line 95 we prefer to keep the reference to the Article 2(3) of Directive (EU) 2017/541, which is in the general approach.

Line 96, AM 56

Hungary basically can support the compromise text proposal. However, we can be flexible in order to reach the compromise on the issue.

Line 97, AM 57

Hungary basically supports the compromise text proposal of the Finnish Presidency.

Line 83, AM 49

Earlier the GSMA and ETNO gave a clear interpretation on the position of service providers regarding exempting cloud services, considering the purpose of the Regulation, the cloud services shall not be excluded from the scope of the Regulation as they are involved in the dissemination of terrorist content online to the same extent as other hosting service providers. Recital 10 of the draft regulation states that the removal orders do not apply to CDN providers (cache providers, DDoS protection providers, etc.). In our view, this is a *loophole* for terrorist content distributors, because hidden behind the network of CDN providers (such as CloudFlare) they can host terrorist content on a self and low-performance hosting server. If the CDN network exemption remains part of the draft, in our view the regulation will not be an effective tool against the dissemination of terrorist content. Regarding line 83 we prefer to keep the text of the general approach.

Line 100, AM 59

Hungary prefers to keep the text of the general approach. We suggest to discuss the issue of line 100 in accordance with Article 5.

Line 102, AM 60

Hungary suggests the following amendment regarding the PRES proposal in order to the relevant bodies, which may be designated as competent authorities in the future, are clearly included in the scope of the provision according to the specific Hungarian constitutional system:

Article 2(9a): 'competent authority' means a designated judicial authority or functionally independent administrative authority or an administrative authority subject to scrutiny by a judicial or a judicial or a functionally independent administrative authority in the Member State.

An Roinn Dlí agus Cirt
 agus Comhionannais
 Department of Justice
 and Equality



Proposed Regulation on preventing the dissemination of terrorist content online

Comments from Ireland

23 January 2020

Ireland would like to welcome the Croatian Presidency, and to thank it for the opportunity to contribute our views on the latest proposals regarding the Regulation, which were discussed at the JHA Counsellors' meeting of 17 January 2020.

In relation to these proposals, we wish to make a number of comments, supplementing those previously submitted by Ireland to the Presidency regarding the proposed Regulation. These observations are motivated by our desire to continue to engage constructively in order to reach agreement on a Regulation that is as effective and efficient as possible.

Definition of "competent authority"

Based upon the discussions at the meeting of 17 January 2020, we understand that the European Parliament's (EP's) concerns regarding the definition of a competent authority (CA) arise from the need to ensure that CAs are independent and, in particular, free of any political interference. We agree that it is important to ensure the independence of CAs and hope that the negotiations will lead to text which satisfactorily addresses these concerns.

However, in the context of these concerns, we believe that the purpose of the EP's proposal to oblige MS to appoint a single CA for the purposes of the Regulation has still not been sufficiently clarified. Ireland has consistently emphasised that the ability of MS to determine the number and form of their CAs is of critical importance. For this reason, we would also have concerns regarding the Presidency's proposal for a hybrid system with a single CA. We are unable to take a formal position on this proposal at this time, and would welcome the circulation of draft text at the earliest opportunity.

It has been suggested that there is a lack of understanding in the EP as to why the ability to designate more than one CA is critical for many MS, including Ireland. We would like to offer a concrete example which may facilitate understanding.

In December, the Government of Ireland gave its formal approval for the drafting of the Online Safety and Media Regulation Bill, and published the General Scheme of this Bill¹. It must be emphasised that specific elements of the Bill may undergo changes as it makes its way through the legislative process, however it is worth outlining some relevant features.

The Bill proposes to establish a Media Commission which, as part of its responsibilities will undertake certain functions in relation to regulation of online service providers. For example, the Media Commission will be tasked with issuing online safety codes which will provide for a wide range of matters, including measures to be taken by designated online services in relation to:

- Harmful online content (including “material which it is a criminal offence to disseminate”);
- User complaints; and
- Reporting obligations.

The Media Commission will also be tasked with assessing compliance with these codes, and auditing the handling of complaints by service providers. Where a service provider fails to comply with its obligations, the Media Commission will have significant powers to enforce compliance through a range of measures, including

- Issuing compliance notices
- Imposing administrative sanctions
- Seeking leave of the High Court to compel compliance by a service provider
- Seeking leave of the High Court to block access to a service provider

No decision has been taken regarding the designation of Ireland’s CAs for the purposes of the Regulation, including whether or not the Media Commission will be one of these authorities. It will not be possible to do so until the final text of the Regulation is agreed.

However, it is clear that there could be a future alignment of the Media Commission’s role and responsibilities with regard to regulating industry obligations and those that the Regulation assigns to CAs, namely:

- Ensuring that hosting service providers meet their obligations;
- Supporting them in doing so; and
- Imposing penalties should they fail to do so.

At the same time, in the Irish context it would not be appropriate for such a body to be the CA for assessing terrorist content and issuing referrals and removal orders. Indeed, as

¹ <https://www.dcae.gov.ie/en-ie/communications/legislation/Pages/General-Scheme-Online-Safety-Media-Regulation.aspx>



a regulatory body, individual notice and takedown will not be part of the Media Commission's responsibilities.

These are functions which would likely be assigned to law enforcement and judicial authorities, as is currently the case in the majority of MS which have already established Internet Referral Units.

While these authorities are undoubtedly the experts in relation to terrorism and terrorist content, they are clearly not the right authorities for regulating industry. Indeed, if the authority competent for issuing referrals and removal orders was also competent for assessing whether hosting service providers' systematic response to them was appropriate, it could be argued that there was a significant conflict of interest.

It must be stressed that Ireland has not made a decision on the bodies that will be designated as our CAs. We hope, however, that this brief example helps to illustrate how the EP's proposal would be difficult for us, and perhaps for other MS, in practice.

This is a very important issue for Ireland. We hope that the key to resolution lies in developing a common understanding at the trilogues, and that this example will be useful to the Presidency in doing so.

As noted above, we would welcome the opportunity to examine draft text regarding the Presidency's proposal.


Proposed deletion of Article 5

Regarding the proposal to delete Article 5 "Referrals", we would recall that throughout the discussions on the proposed Regulation, we have emphasised that referrals are a critical tool in the fight against terrorist content online. We would also recall that referrals have, to date, been a highly effective and efficient means of securing the removal of terrorist content by providers which accept them.

We have attempted at all stages during negotiations to maintain a constructive approach, with a focus on developing a Regulation that is both practical and efficient. As such, bearing in mind their proven effectiveness, we have advocated for referrals to continue to be the tool of choice for the removal of terrorist content, and strengthening the referral process by requiring all hosting service providers (HSPs) to engage with it, as provided for in Article 5. At the same time, we have supported the inclusion of binding removal orders with direct, cross-border effect, as provided by Article 4 of the initial proposal.

While we recognise the concerns that have been voiced by the European Parliament (EP) regarding the use of referrals to secure the speedy removal of terrorist content, and the EP's strong opposition to the inclusion of such a provision in the Regulation, we must ensure that we do not undermine the Regulation's purpose of creating a more efficient and practical framework for preventing the dissemination of terrorist content online.

We note that the EP has adopted a position on several provisions of the Regulation that are of critical importance in meeting this purpose. For example, the EP has proposed to



remove the ability of CAs to issue binding removal orders to service providers located in any MS, and has also proposed to limit the ability of MS to designate their CAs appropriately. Based upon discussions to date, it does not appear that the EP has shown any flexibility on its position on these issues, which Ireland has consistently argued would go against the objectives of the Regulation.

For these reasons, we would not agree with any proposal to remove Article 5 at this time. However, we could consider such a proposal if this major concession by the Council, representing a significant departure from its General Approach, was met with reciprocal compromise by the EP ensuring that the Regulation can still meet its goals. In particular, this would mean retaining the ability of CAs to issue removal orders directly to HSPs in any MS, and retaining the ability of MS to determine the number and form of their CAs. In this event, and on the understanding that the Article's removal would not preclude the operation of a referral system similar to those currently in use, we would be willing to compromise on Article 5.

Comments from the Netherlands on the proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online
– 21 January 2020

These comments include the lines of the 4-columns table¹ which have not yet been provisionally agreed upon. References are made to the attachments included in the Presidency's e-mail of 17 January last, where:

- attachment 1 refers to the FIN wording proposals for Articles 1 and 2;
- attachment 2 refers to the EP proposals;
- attachment 3 refers to the Council proposals.

Article	Position
Art. 1(1) line 72	We support the Council compromise proposal (attachment 3), including the addition of 'public'.
Art. 1(1)(2a) line 76	We support the FIN building block for a possible compromise, included in attachment 1. As stated before, while we feel it to be important to adequately protect content of journalistic, artistic or educational nature or for awareness purposes. While we would not oppose this compromise, we would prefer not to have a blanket exception for such content, as suggested by the EP in amendment 45. This building block offers a good compromise.
Art. 1(2)(c) line 78	Support for the EP-proposal in AM 47 (line 78 in attachments 1 and 2). This regulation should be in accordance with other EU-instruments, and should thus not lead to a general monitoring obligation as stipulated in Article 15(1) of Directive 2000/31/EC. In addition, measures which lead to the proactive review and/or filtering of content prior to its publication, would be in violation of the Dutch constitution. For both reasons, this regulation should be without prejudice to Directive 2000/31/EC. This should also be reflected in Article 6 (proactive measures).
Art. 2(1) line 83	We can support the essence of the draft definitions circulated by e-mail of 16 January 2020, and would also support the addition of the word 'public'. However, it should be further clarified that e-mail, private messaging, B2B and other kinds of non-public forms of communication are excluded from scope, as it is generally technically not possible to gain access to such systems. This regulation should only cover information that has been made available to an indeterminate number of potential recipients, as included in the drafting proposal of recital 10, circulated by the Finnish presidency at 8 November 2019.
Art. 2(2) line 84	Support for the inclusion of the word 'public'. Only content available to the public should be within scope. Personal information, including B2B, should be out of scope.
Art. 2(3) lines 85-89	We support the Council compromise proposals, as the suggested wording offers additional clarity over the initial proposal (attachment 3).
Art. 2(4) line 90 and Art. 2(5)(a-d) lines 91-96	It is important that the definition of terrorist content is in line with the definitions of Directive 2017/541/EU. As such, the Netherlands was content with the definition of terrorist content in the general approach, in which the coherence between Directive 2017/541/EU and this regulation is ensured.

¹ Distributed on 15 January (WK 371/2020 INIT).

	<p>However, as most proposals of the EP (lines 90-96 of attachments 1 and 2) are also consistent with Directive 2017/541/EU, we take a positive attitude towards them.</p> <ul style="list-style-type: none"> - In particular, we can support the EP's proposals in lines 90 (terrorist offences) and lines 91, 93, 94 and 96 (definition of terrorist content). - Line 95 would be acceptable. However, it should be clarified what the objective is by the substitution of 'by' with 'in relation to'. The Netherlands feels it is important that the definition of terrorist offences remains in line with the CT-Directive. This change seems to deviate from that Directive, as 'in relation to' implies a wider scope. <p>We do not oppose the inclusion of 'promoting the activities of a terrorist group' in Article 2(5)(c), as we consider the wording of that paragraph to be very similar, albeit not equal, to Article 6 of Directive 2017/541/EU. However, we would not oppose a different wording.</p>
Art. 2(5)(d a) line 97	<p>We have previously expressed concerns about the proposed catch-all provision in Article 2(1)(5)(da) in AM57. These concerns remain with the compromise proposal of the EP in attachments 1 and 2. While the wording has changed compared to AM57, this change does not exclude the possibility that the mere depiction of a terrorist offence falls within the scope of the regulation: the wording 'constitution a threat' implies that all content which could lead to a terrorist offence being committed, is within scope. As much as NL empathizes with broadening the scope, if there is no element of inciting, advocating or promoting terrorist offences, the depiction of such an offense should not be within scope.</p> <p>After all, the depiction of a terrorist offence could have a very legitimate aim, such as journalistic articles or reports by NGO's. For example, the depiction of terrorist acts of ISIS by NGO's such as Amnesty International, which publicized 'stills' from videos, helped raise public awareness of the acts of ISIS.</p> <p>A possible compromise would be a recital, that clarifies that material which constitutes a threat that a terrorist offence is committed, falls within the scope of this regulation. That would give room for a case-by-case analysis, while ensuring that such material should still meet the criteria of Article 2(5)(a-d) and is thus not a category on its own. Alternatively the text of the GA, in line 92, would also be acceptable.</p>
Art. 2(6) line 98	Support for the position of the EP. This is in accordance with the definition of HSP's in line 72.
Art. 2(8) line 100	The wording of this definition depends on whether referrals are kept. Please refer to lines 137-144.
Art. 2(9a) line 102	<p>Legislation in this area should be effective, and with due respect to fundamental rights such as the freedom of speech and the right to an effective remedy. As such, this particular amendment should be assessed in relation to Articles 4 and 15, and in relation to other options to strengthen these fundamental rights, such as:</p> <ul style="list-style-type: none"> - a legal remedy in the Member State where the HSP has its main establishment or where its legal representative resides; - strengthening the position of the receiving MS in the consultation procedure in Article 4a, or

	<p>- additional ex-post checking by an independent or impartial authority to assess the appropriateness of removal orders.</p> <p>Please refer to our earlier comments, which we can.</p> <p>Pending further discussion in the JHA counsellors meeting on 31 January 2020, we would not oppose the suggestion made by the Presidency in its e-mail of 17 January ('competent authority' means a designated judicial authority or functionally independent administrative authority or an administrative authority subject to scrutiny by a functionally independent administrative authority in the Member State). This seems to imply that an administrative authority would be an independent decision-making authority. The exact interpretation should be clarified, f.e. in a recital.</p>
Art. 5 lines 137-144	While we would prefer including referrals in this regulation, we can be flexible on this, as we understand the reasoning of the EP which feels it is unnecessary to regulate something that is essentially voluntary.
Art. 13(4) Line 198	We would support the EP position where all terrorist content is reported to the authorities competent for the investigation (AM117). However, the obligation to report information would only occur where there is an 'imminent threat to life' and/or 'critical infrastructure', to prevent very large amounts of reports being made in situations of low impact.

Incitement and Public Glorification of Terrorist Activities**Article 110**

(1) Whoever incites commitment of criminal offences under Article 108 of this Penal Code and therefore propagates messages or makes them available to other persons in some other manner with the intention to promote terrorist criminal offences and thus causes danger that one or more such criminal offences would be committed, shall be sentenced to imprisonment between one and ten years.

(2) Whoever directly or indirectly publicly glorifies or advocates criminal offences under Article 108 or the criminal offence referred to in the preceding paragraph by, with the purpose under preceding paragraph, propagating messages or making them available to the public and therefore cause danger that one or more such criminal offences would be committed, shall be punished in the same manner.

(3) Persecution for criminal offences under preceding paragraphs shall be initiated with the permission by the Minister of Justice.

TCO REGULATION: UK RESPONSE TO PRESIDENCY PROPOSALS,
ARTICLES 1-2 (SCOPE AND DEFINITION)

Q1: Definition of 'public'

The UK is broadly content with the proposed text but would welcome the following changes and/or clarification to ensure the definition sufficiently addresses our concerns around the scope of access:

- The recital provides helpful clarification which appears to bring into scope access to semi private channels: *"This can apply to natural persons which possess a registered user account for the respective service as well as to any natural person which does not possess such an account."* But this should be brought out more into the legal definition to clarify what is meant by *"special means"* alongside the levels of access, which would also address the concerns from cloud companies on naming types of service (particularly around B2B cloud) (proposed revised definition below).
- The UK agrees with the concerns raised by Ireland and Belgium during the Counsellors discussion on the use of the 'application layer'. Such language may be limiting, as it might be interpreted to only mean a very specific layer of services. For example, the different layers of the internet may merge, and thus some companies could say that we are not in that layer, therefore not in scope of the regulation.
- Both the Internet Protocol Suite (TCP/IP) and the OSI model - ways to describe the various layers/levels of the internet - use the term application layer but are slightly different in what scope they consider the term to refer to, so we risk being ambiguous by using this term. It is a useful technical model (e.g. <https://www.techopedia.com/definition/6006/application-layer>), but might not stand the test of legal requirements.
- The UK proposes the following revised text for the definition (removes 'application layer'):

Available to the public means available to be perceived directly by any natural person visually, in auditory form or by any other bodily form of perception. The perception through any natural person must be possible without special means of access to the backend infrastructure of the hosting service provider itself or to technical infrastructures of third companies which are necessary for the functioning of the service provided by the hosting service provider. For these purposes "special means of access" applies to natural persons which possess a registered user account for the respective service as well as to any natural person which does not possess such an account

Q2: Definition of terrorist content: alternatives to 'promoting' (line 95)

While the term 'promoting' is not included in UK legislation, existing domestic legislation, namely the Terrorism Act of 2006, goes beyond the proposed definitions under the draft TCO Regulation and covers **activities that have the effect of promoting terrorism** to support law enforcement activity.

- **Section 1:** provides an offence of **encouragement of acts of terrorism** or Convention offences. This covers publishing a statement which directly or indirectly **encourages the preparation, instigation of commission of an act of terrorism, or that is reckless as to whether it will have this effect**. This includes a statement that glorifies the commission or preparation of acts of terrorism, whether in general or specific acts in the past or future, and that could reasonably be inferred as suggesting that such acts should be emulated. It is not necessary for an act to have been carried out as a result.
- **Section 2:** It is an offence to provide/supply/sell/ transmit such a publication, with the intention that it will have the effect of **encouraging or assisting terrorism or being reckless as to whether it will encourage or assist terrorism**

The key gap under the proposed definition in A2 is that it does not, or does not necessarily, include reckless promotion. We suggest that specific provision be included in the definition.

At the operational level, the UK CT Internet Referral Unit (CTIRU) advise that EU Member states and the UK CTIRU mainly collaborate via the EUIRU. All the IRUs currently work from different legislation and remits. **It would be helpful to understand how the remit and work of EUIRU (including as a coordinating function) would be impacted by this definition.**

Q3: Definition of Competent Authority (A2(9a)): 'functionally independent'

It is important to understand whether Member States' existing Internet Referral Units (IRU), as law enforcement authorities, would fall under the proposed scope given the relevant expertise and implications this could have on cross-border investigations and prosecutions, as well as their existing work with companies to act against online terrorist content as the appropriate authorities. It is unlikely that there would be any other existing authority akin to IRUs that would be as competent to carry out this work. Therefore, it is in our collective and firm interest to ensure that the draft Regulation does not hinder or discourage this work going forward.

The UK's CT Internet Referral Unit (CTIRU) sits within the Counter Terrorism Policing Unit in the UK Metropolitan Police Service. The UK deems the police to be operationally, and therefore functionally, independent from the Government. This includes CTIRU which is also subject to legal oversight. **It would be helpful to have explicit clarity in either the text itself or through a recital that a police force/IRU is functionally independent and therefore in scope.**

Q4: Referring content for criminal investigation and prosecution (A13(4))

The UK's preferred approach on the requirement of HSPs to inform relevant authorities competent for investigation and prosecution of criminal offences is for HSPs to take reasonable steps to:

- Support law enforcement and other relevant government agencies for the investigations and prosecution of criminal offences.
- Inform law enforcement or other relevant government agencies of threats to life and imminent threats
- Preserve terrorist User Generated Content (UGC) that has been removed from their service, along with its related metadata, for a period of 12 months.

The key considerations informing this approach are the capacity of law enforcement, proportionality, and the balance on the right to privacy.

