This document has not been adopted or endorsed by the European Commission. Any possible measures indicated in this paper are the preliminary elements being considered by the Commission services, they do not preclude the measures to be finally considered in the Impact Assessment and may not in any circumstances be regarded as stating an official position of the Commission. The information transmitted is intended only for the Member State or entity to which it is addressed for discussions and for the preparation of the Impact assessment and may contain confidential and/or privileged material.

IMPACT ASSESSMENT ON ILLEGAL CONTENT ONLINE
STAKEHOLDER CONSULTATION:
MEMBER STATES

Introduction:

Following the initial discussion with Member States at the EU Internet Forum (EUIF), the Commission would like to get more detailed views on possible actions to more effectively tackle terrorist content online as part of the ongoing work on the Impact Assessment on Illegal Content Online. These views will complement the Open Public Consultation (OPC, available here), as well as the data collection exercise based on the table of indicators.

The Commission started work on an impact assessment outlining potential problems, objectives and options in the attached Inception Impact Assessment (IIA). As part of the options to be considered, the Commission will analyse the current situation (baseline scenario) as well as actions to reinforce the voluntary measures as well as possible sector-specific legislation (including in particular on terrorism content online) as well as horizontal legislation applicable to all types of illegal content.

The measures presented in the Inception Impact Assessment[1]are initial ideas, and additional actions and options could be considered. The actions to be undertaken would be mainly addressed to online platforms, but could also require further action by Member States.

Member States are kindly requested **to reply to the questions below and provide any additional considerations in writing by 13 June 2018**. The results of this questionnaire will be presented and discussed at the **forthcoming meeting on 15 June**. In parallel, the European Commission's Directorate-General for Communications Networks, Content and Technology convened its expert group under the eCommerce Directive also feeding into the work of the impact assessment.

[1] https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1183598_en

Questions

I. Problem and baseline scenario

1. What are the **provisions, arrangements etc under national law addressing the removal of terrorist content[2] for preventive purposes** (e.g. do you have duty of care provisions[3], specific notice and action procedures, provisions on transparency of companies' actions in relation to the removal of terrorist content, provisions on safeguards, etc.)? Please indicate below – where relevant – the applicable laws or other legal documents.

Notice and action procedures	The NL IRU only reports (Notice and Take Down) content if it thinks it is being recruited for the armed struggle (Article 205 of the Dutch Penal Code) or is incited to commit a (terrorist) crime (art. 132 Sr) (both crimes for which persons can be taken into custody). This working method is based on the regime for making data inaccessible. This regime is part of a new law on computer crime (Article 125p CCIII). This law is before The Senate (the upper house of the States General). This legislation provides a general framework for dealing with computer crimes. This includes not only terrorist crimes, but also crimes against child pornography. In addition there is a Notice and Take Down protocol for dealing with reports of illegal and punishable content on ('Dutch parts' of the) Internet
Transparency rules	
Safeguards	

Do you have **specialised entities that notify/refer terrorist content** to hosting service providers? What is the **legal basis and benchmark for notification/referral** (illegality of content, terms of service of hosting service provider)?

The NL IRU was set up within the Dutch national police force (based on the Action Program Integral Approach for Jihadism, Aug. 2014). It's tasks are: - Detection and interpretation of online terrorist and extremist content - Notice & Take Action (NTA); the non-committal reporting of punishable content (recruiting (Article 205 of the Dutch Penal Code) or incitement to commit a (terrorist) crime (art. 132 Sr)) to Internet companies,

[2] For the purpose of this questionnaire, "terrorist content" is defined as in the Commission Recommendation of 1.3.2018 on measures to effectively tackle illegal content online (C(2018) 1177 final). https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

[3] See recital 48 of the Directive on electronic commerce https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32000L0031

- Identification of producers and distributors of (criminal) content. The NL IRU has been operational since September 2017 and operates in close cooperation with Europol.

Do you consider them **sufficient** in terms of preventing accessibility of terrorist content? What are the limitations?

The NL IRU works within a very specific framework and focusses on making referrals to those platforms that are actively being used by relevant (within the Dutch context) terrorist and extremist ecosystems. This results primarily in referrals to 'novice platform' (i.e. platforms or companies that do not partake in the EU Internetforum).

2. Do you consider that the **amount of terrorist content online** in the last [two] years has overall

	Decreased substantially
x	Decreased
	Continued at the same level
	Increased
	Increased substantially

Please indicate the basis for your assessment. What do you think has contributed to this trend?

The Netherlands believes that the measures taken by the private sector in combination with the founding of Internet Referral Units and the geo-political developments contributed to a decrease in the amount of publicly visible terrorist content online. We do however assess that plenty of non-visible materials remain.

3. Do you see a **risk that removal by companies** on their own initiative could **interfere with investigations or intelligence gathering**? What would be the **mitigating measures** necessary to address any such risks?

To mitigate risks of interference with investigations or intelligence gathering, we underline the importance of referral units, support to companies in case of doubt about qualification as terrorist content and arbitration or independent oversight. In addition transparency or oversight specifically concerning the assignments given to automated means of detection could mitigate such risks.

4. Do you see a risk of **erroneous removal** by platforms of legal content (e.g. removal of content misidentified as illegal, removal of content disseminated for research, educational or journalistic purposes, "over-removal")? Are you aware of **any cases** of over-removal? What would be the **mitigating measures** necessary to address any such risks?

The Netherlands does recognise the risk of erroneous removal by platforms of legal content. That is why we are in favour of independent oversight and/or an arbitration mechanism. In addition, this arbitration should also include the possibility to appeal against a decision to remove online content.

II. Non regulatory options: reinforcing voluntary action

1. Do you think that the work under the **EUIF** as reinforced and complemented by the **Recommendation** is **sufficient** action at EU level to effectively tackle terrorist content online?

The Netherlands recognises the success of the current voluntary approach and would like to continue the constructive and innovative collaboration in the EUIF. The Netherlands questions whether the current interest in companies to tackle illegal content is sustainable and whether we can continue without one European uniform mechanism against illegal terrorist content and without independent review.

2. Do you consider that the **EUIF's work should be further developed** in order to reinforce action at EU level to tackle terrorist content online e.g. through a Memorandum of Understanding in which companies and possibly Member States would sign up to concrete commitments (see possible measures below)?

The Netherlands believes that the EUIF's work should be continued and further developed. The current dynamics between the MS and the partaking companies has yielded much progress and positive results. Yet the legal safeguards are limited and the likelihood of all relevant companies actively taking part in the EUIF is limited.

3. Which of the following **possible elements** should in your view be addressed and further developed within a voluntary approach? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

2	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit)
3	Stronger commitments in terms of internal processes and resource allocation (e.g. to have certain procedures in place, conduct risk assessments and establish mitigating procedures, content of Terms of Service, training, capacity to detect content in different languages)
5	Standardised working arrangements between companies, law enforcement and Europol to enhance understanding of how platforms are abused, to improve referral mechanism, avoiding unnecessary duplication of efforts, facilitating requests from law enforcement agencies in relation to criminal investigations[4].
5	Stronger commitment on specific proactive and preventive measures (i.e. further development and participation in industry-led schemes, such as the database of hashes developed in the context of the EUIF)
5	More detailed requirements on transparency and reporting
4	More detailed requirements to companies on safeguards against over-removal
5	Establishment of an external audit/monitoring mechanism
5	Establishment of contact points, both in companies and Member States, to facilitate referrals (and feedback) and requests from law enforcement authorities in relation to criminal investigations.
4	Additional support (e.g. by Europol) to referral capacities in Member States

[4] See point 40 of the Recommendation.

4. What other additional measures could be developed within a reinforced voluntary approach?

We underline the importance of facilitating an open and transparent dialogue concerning the role of automated means of detection in the removal of illegal content.

5. Which further actions could be taken to secure participation from those **companies** who have **not engaged**?

The possibility of a public/private fund to promote making content monitoring in integral part of new designs in new applications could be further explored.

6. Which further actions could be taken to **support small companies** and start-ups in tackling terrorist content online effectively? Should these be taken by larger companies, public authorities or both?

See answer 5 above.

7. Do you think that the voluntary approach is **effective** and flexible enough to ensure that companies continue their efforts in the **long term**? Please indicate with which statement you would agree with:

	Yes
	No, it should be reinforced as presented above to obtain sufficient guarantees
x	No, it should be reinforced via legislation

III. Legislative options

1. Why would you consider **legislation necessary at this time**? What would be the concrete benefits? What **risks** could legislation entail?

The Netherlands sees the success of the current voluntary approach and would like to continue the constructive and innovative collaboration in the EUIF. The Netherlands questions however whether the current interest in companies to tackle illegal content is sustainable and whether we can continue without one European uniform mechanism against illegal terrorist content and without independent oversight. Creating a European level playing field by implementing a uniform mechanism to deal with illegal terrorist content could be beneficial to consolidate the current success of the EU IF.

2. What should be the **material scope of legislation** (i.e. how should terrorist content be defined)? Do you consider that covering material inciting to commit terrorist acts

(Article 21/Article 5 of the Terrorism Directive[5]) is sufficient or should the dissemination of material pursuing other terrorist purposes be included as well?

Material the dissemination of which pursues the following objectives should be included in legislative measures:

x	Recruitment for terrorism
x	Providing training for terrorism
x	Terrorist financing
	Other, please elaborate:

To what extent should material produced by UN/EU designated terrorist organisations be included?

All material or information of which the dissemination amounts to offences specified in Directive (EU) 2017/541 or terrorist offences specified in the law of a Member State concerned, including the dissemination of relevant information produced by or attributable to terrorist groups or entities included in the relevant lists established by the Union or by the United Nations should be included.

3. Which **measures** (based in particular on the elements mentioned in the Inception Impact Assessment) do you consider as **necessary elements of legislation** to be impactful? Please indicate the need from a scale from 1 (unnecessary) to 5 (very necessary)

3	Definition of terrorist content (*see question above*)
2	Requirements regarding the companies' terms of service
4	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
3	Specific requirements in terms of action upon referral (including time limit of one hour)
4	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
5	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
4	Sanctions in case of non-compliance
5	Exchanges of information with law enforcement to limit any interference with investigations and to feed into the analysis of terrorist material
1	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
5	Requirement to Member States to increase referral capabilities, quality criteria for referrals and for referral entities in Member States to provide relevant

[5] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017L0541

	support to companies in case of doubt about qualification as terrorist content (e.g. through points of contact)
4	Nomination of point of contact within Companies
5	Reporting obligations for companies[6]
5	Transparency requirements for companies vis a vis their users[7]
5	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
5	The establishment of an external audit/monitoring mechanism for assessing compliance of companies.

Do you consider that minimum requirements could usefully be complemented by self-regulatory measures? And if so, which ones?

An European uniform mechanism against illegal terrorist content under independent review could very well be complemented by self-regulatory measures such as best practice sharing concerning specific proactive and preventive measures and further development and participation in industry-led schemes, such as the database of hashes or a database for url sharing as currently being developed in the context of the EUIF

4. What **other additional measures** could be developed within legislation?

The Netherland would also be interested in exploring option concerning transparency or oversight concerning the assignments given to automated means of detection.

5. What should be the **personal scope of the legislation**? Only hosting service providers within the meaning of the Directive on electronic commerce or other service providers?

To be determined.

[6] See point 41 of the Recommendation.
[7] See points 16 and 17 of the Recommendation.

Do you think **smaller companies** should be covered by all obligations or should they be exempted from some of the obligations (e.g. proactive measures) but obliged by others (e.g. time-limits after referral)? Which companies could be partially exempted and from which obligations?

Smaller companies mostly make use of hosting providers. Measures should therefore take into account the market position and the extent of control that companies have on online content.

6. How do you see the **impact on fundamental rights** of the above-mentioned measures and which safeguards would be necessary to avoid undue interference with fundamental rights?

We anticipate that respect for fundamental rights form an integral part in all propositions made by the European Commission and/or Member States. In addition, we are fully aware that the use of automated means of detection could potentially lead to fundamental rights violations. It is therefore of great importance that the European approach includes checks and balances (f. ex. arbitration, independent oversight and transparency or oversight regarding tasks given to automated means of detection) to protect fundamental rights.