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 rule that allow the removal of terrorist content is Act 13/2015. Criminal Procedure Code. Also Law 34/2002 on information systems and electronic commerce stablishes a framework or collaboration among authorities and providers*
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 specialized entities that deal with terrorism are the Investigations Units. They evaluate the content and, if necessary, request the removal or the court safeguards in order to send court warrants to ISPs. Furthermore, the request for terrorist content removal is also carried out through the Europol IRU using the relevant mechanisms.

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

There would have to be more obligations and commitments from ISPs which are located outside the EU, so as to deal with requests more quickly. It would also be necessary to enhance the IRUs as well as the information exchange among them. Likewise, the information flows between IRUs and ISPs should also be reinforced.

[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

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

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

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

The extended use of instant messaging apps which allow to disseminate terrorist.
The ongoing investigations have revealed an increase in the content related to terrorism. Online communications are affordable for everyone, so anyone with the proper technology is able to generate and share content online. However, as regards DAESH, the quality of its media production has declined, especially in terms of video edition. This is probably due to their loss of territory and human resources and their current weak structure.

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?

The removal of content by companies is a risk since it can interfere with current investigations. In order to mitigate that behavior they should notify the likely removal to LEAs in order to open a period of answer in case there is a current investigation related to that content. It is also necessary to establish a flagging system for the content that should not be removed.

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?

A significant risk can be observed in these cases. However, the analysts responsible for monitoring said content have a notorious expertise to assess which content should

be proposed for removal. Furthermore, they work with profiles and channels where this propaganda content is usually published.

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 work under EUIF is necessary. Nevertheless, LEAs in general should be taken into account in a more effective way.
Also, It would be convenient to create similar fora in every MS where all relevant stakeholders are represented.

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)?

We do consider that the EUIF's work should be further developed.

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)

3	More specific objectives for companies' actions (e.g. request a certain percentage of content taken down within a certain time limit)
5	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
5	More detailed requirements to companies on safeguards against over-removal

[4] See point 40 of the Recommendation.

2	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.
5	Additional support (e.g. by Europol) to referral capacities in Member States

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

It would be useful to create a database with all the content proposed for removal in order to carry out analyses and statistics, which could also be used as evidence in potential judiciary proceedings. Likewise, companies should classify the removed content based on the type of file, content, etc.

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

The companies which are not engaged yet need to understand that the work of EUIF is necessary in order to reinforce the capabilities to access terrorist content for investigations, whether it is for removal or other purposes.

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?

It could be effective to provide these small companies with best practices guides and other support actions. These actions should be taken by public authorities.

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

II. Legislative options

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

Legislation about this matter is necessary in order to assure that all companies act in the same way in the same cases. *It is the proper procedure to establish obligations for ISPs in order to accomplish request from LEAs. The significant impact that content dissemination has on society forces authorities to regulate the ways in which said content should be removed.*

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
X	Other, please elaborate:

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

Glorification of terrorism.

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)

4	Definition of terrorist content (*see question above*)
4	Requirements regarding the companies' terms of service
5	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self

[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

	regulation)
4	Specific requirements in terms of action upon referral (including time limit of one hour)
5	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
5	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
4	Clarify that companies engaged in proactive measures benefit from the liability exemption (Good Samaritan clause)
4	Requirement to Member States to increase referral capabilities, quality criteria for referrals and for referral entities in Member States to provide relevant 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]
3	Transparency requirements for companies vis a vis their users[7]
4	Compulsory safeguards, such as the ones in the general chapter of the Recommendation
3	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?

Creating a database with all the content proposed for removal in order to carry out analyses and statistics, also used to collect evidence for legal proceedings Moreover, companies should classify the removed content depending on the type of content, etc.

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

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?

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

Of course, not only hosting service providers, but also the rest of companies offering any services. Legislation would apply to all terrorist online propaganda activities.

6. 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 should be covered by the same obligations.

7. 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?

The regulation itself fully respects fundamental rights. Similarly, judiciary authorities also safeguard compliance with this regulation.
It should be necessary to balance the rights to security and freedom.