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.

Duty of care provisions	The underlying law regulating general rules and duty of care based on eCD is the Information Society Services Act. In Estonian legislation the ISSA states: "The provision, in Estonia, of services belonging to the co-ordinated field through a place of business located in a Member State of the European Union or Member State of the European Economic Area are not subject to restriction, except in the case and to the extent justified for the protection of morality, public order, national security, public health and consumer rights." Accordingly, subsequent supervision of commission must be taken into account. Information Society Services Act: https://www.riigiteataja.ee/en/eli/513012015001/consolide
Notice and action procedures	Estonia does not have any special regulations on removal of terrorist content online. Mainly our responsible authorities are monitoring the situation and cooperate with different service providers on voluntary basis. But there are also law enforcement regulations (§ 29 and 29 of the Law Enforcement Act) that compel service providers to remove or restrict the access to illegal online content. The Law Enforcement Act: https://www.riigiteataja.ee/en/eli/507122016001/consolide There are also regulations under §19 of the Media Services Act (MSA), which make restrictions to media channels regarding the hatred on the basis of sex, racial or ethnic origin, beliefs or religion or the degrading of the lawful behavior or violation of law in any of the programs. Legal procedures regarding liability are mentioned in Chapter 9 of the MSA.

[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

	The Media Services Act: https://www.riigiteataja.ee/en/eli/511052015002/consolide
Transparency rules	Measures, implemented under the Law Enforcement Act need to be adequate and legitimate. Measures and restrictions might be disputed in Court.
Safeguards	Same or similar safeguards apply as provided in eCD. Internet service provider is responsible for the content of the information provided on the Internet, unless it is merely brokering of the information.

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)?

Estonian authorities do not have specialized entities for terrorist content only. But law enforcement authorities are monitoring the web to prevent and counteract to any illegal offences, incl. illegal contents. There is ongoing cooperation and exchange of information with local and international partners, including Europol. Estonian Police and Border Guard Board has the Web-constables unit, that responds to notifications and letters submitted by people via internet (incl. social networks) and train public audience at issues of internet security. The unit cooperates with different service providers (incl. social networks), internal and international partners and Europol.

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

Not applicable

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
	Increased substantially

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

No statistics or data available on that matter. Currently there is no terrorism related content found online in Estonian language. But we can report about the increased number of the hate speech and ethnically populistic content.

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 obstacles to investigation and proceeding may be caused by shutting down terrorism-related profiles online without any notification to the Security Authorities. Europol database of hashes is a useful tool that has to be in use by the service providers and law enforcement authorities. Therefore deceptive measures might be necessary for investigations or intelligence gathering as well; e.g. false availability for the uploader, but not for the public, etc.

The EU-wide common base standards for service providers specifically regarding the terms of use could potentially fulfil the purpose of tackling and restricting the access to illegal content online more effectively, but cooperation on voluntary basis (under the MOU) could also be influential.

Small service providers often have no capacity to automatically identify and remove illegal content, especially if it is published in uncommon language. Therefore it could be helpful to support them with the EU-wide IT solution, that would be developed in cooperation with Europol and supportive service providers.

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?

Definitely there are risks of over-removal. As explained above, due to our current legal procedure and views on that matter, we are not aware of any such incidents. But over-regulation is always a potential risk. It is doubtful, whether platforms are always up to terms with ability to make objective decisions and rather fall for “safe decision” (or “over-removal”) just to disclaim liability and thus hindering freedom of expression. One has to understand that the internet is a common public space where different jurisdictions intersect.

One mitigating measure would be an integrated definition - like “terrorist related content”, “violent extremism/violent radicalisation”, “hate speech” or “terrorism” overall. Another mitigating measure could be the establishment of **trusted flaggers**, i.e. panel of experts, including journalists and international relations experts. In some cases **redress mechanisms might be necessary**.

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?

Estonia acknowledges the work under the EUIF and admits the coordinative role of the Commission in strengthening policy measures. We support reinforcement of voluntary actions, but also express our willingness to discuss any analysis-based solutions.

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)?

There is a need to involve different service providers in cooperation against terrorist content online, but also countering any illegal activity online. It is important, that on-going measures and progress would not be harmed by further actions. Possible terms of agreement for private partners should be analysis-based and consider factors like size and capacity of the service providers, motivation for cooperation (incl. technical support), information exchange mechanism, survey, coordination, etc. As for the Member States, very concrete commitments have already been signed and there is a common challenge to implement them. The cooperation in the field of "Database of Hashes" is **extremely** important. This is a highly effective measure to proactively tackle terrorist content online. This tool should be accessible and affordable for all platforms, big or small, willing to participate.

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)
2	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)
4	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].
4	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)
2	More detailed requirements on transparency and reporting
2	More detailed requirements to companies on safeguards against over-removal
3	Establishment of an external audit/monitoring mechanism
3	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] See point 40 of the Recommendation.

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

No concrete suggestions.

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

EUIF could discuss possible additional motivational measures for the potential cooperation partners. One possible solution could be support of the small service providers with the EU-wide technical solution for automatic search and identification of terrorist-related content in different languages.

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?

We would support the solution, where service providers and different companies within themselves share information, best practice and support technical developments. One possible solution could also be support of the small service providers with the EU-wide technical solution for automatic search and identification of terrorist-related content in different languages.

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
	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 main concerns are: 1. As service providers also locate in third countries, it is useful to consider location-specific terms 2. Differences in security environment and threat levels in MS would not allow common obligations. 3. Any legislative measure will bring a need for oversight and dispute resolutions, which would be a remarkable additional burden for both parts. 4. Differences in terminology approach by the MS would bring additional disputes and litigations.

5. Additional legislative obligations and unavoidable over-removal, will bring additional burden to protection of fundamental rights.
6. Possible contradictions with e-commerce directive - even if companies reporting about the elimination of over 90% of illegal content themselves, it would be wrong to make this amount obligatory for them, as this would be in contradiction with art 15 of the eCD.

In other words, legislation is only necessary for regulating the intersection of jurisdictions in common (virtual) public space. Clarity is needed on the rules of engagement if one MS considers content illegal and others might not. Facilitation of tools and reporting mechanisms should be preferred over regulation.

Main **risks** are scope of application (especially towards third countries), limitation of freedom of expression and other basic rights, possible collision with currently rather effective eCD.

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:

	Recruitment for terrorism
	Providing training for terrorism
	Terrorist financing
	Other, please elaborate: **a call to action of terrorism, glorification/justification of terrorism, supporting of terrorism (incl logistic, housing, services, etc).**

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

No specific suggestions.

4. 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)

5	Definition of terrorist content (*see question above*)
4	Requirements regarding the companies' terms of service

[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

5	General requirement for companies to put the necessary measures in place to ensure that they do not host terrorist content (complemented by self regulation)
2	Specific requirements in terms of action upon referral (including time limit of one hour)
2	More explicit and detailed obligations to deploy specific proactive measures (including automatic detection)
4	Specific requirements to cooperate with other hosting service providers to avoid the dissemination across platforms
3	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)
3	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
4	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.

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

Considering our limited experience it is hard to predict the need for minimum regulative measures.

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

No concrete suggestions.

7. 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?

Only 'hosting' could be out-dated concept in contemporary world (i.e. who is accountable if a platform user streams illegal content which is not necessarily hosted or stored?). Principles of liability should be built on, but not in place of eCD.

[6] See point 41 of the Recommendation.

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

8. 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?

In case of minimum legislative obligations for the service providers, those should be minimal and suitable for all, regardless the size and capacity. Additional measures could be agreed on voluntary basis. Also, the size of the company (based on personnel and turnover) is irrelevant and misleading. More suitable threshold would be database of active users or net traffic generated by the company.

9. 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?

Additional legislative measures will bring a need for legal oversight and dispute resolutions. Unavoidable over-removal, will bring additional burden to protection of fundamental rights, disputes and litigations. In principle, similar safeguards as set out in Article 3 of eCD should be maintained along with relevant derogations to it.