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	X (note bien! only in intellectual property right breaches)
Transparency rules	
Safeguards	

In Finland the E-Commerce Directive has been implemented in the provisions of Chapter 22 of the Act on Electronic Communications Services.

The Act on Electronic Communications Services does not have provisions mentioned in the recital 48 of the E-Commerce Directive on duty and care. There are no provisions on transparency of companies' actions in relation to the removal of terrorist content or provisions on safeguards. Notice and action procedure is in the national law, but only concerns breaches of intellectual property rights.

According to Finnish law, the service provider may face criminal liability as an accessory or an accomplice if he/she does not remove the illegal content. We have not enacted specific time limits, the time required is determined in accordance with general principles of criminal law. However, we have no general obligation to monitor and hosting service providers are not liable if they have no knowledge of the illegal content as stipulated in the Directive on electronic commerce.

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)?

National Bureau of Investigation and Finnish Security and Intelligence Service can notify the service providers about illegal terrorist content on their platforms.

[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

In Finland we have an act called ”Act on the Exercise of Freedom of Expression in Mass Media”:

https://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf

According to the provisions of the Act on the request of the public prosecutor, the head of a pre-trial investigation, or the injured party, a court may order that the publisher, broadcaster or keeper of a transmitter, server or other comparable device is to interrupt the distribution of a published network message, if it is evident on the basis of the contents of the message that providing it to the public is a criminal offence. In the same process the court may order on the request that such message shall be removed and destroyed. The court shall deal with these requests as a matter of urgency. There are safeguards related to this measure like the right to be heard in the court and appeal from the court decision. Relevant provisions are in Sections 18 and 22.3. These provisions cover all unlawful content, for example content constituting a public incitement to commit a terrorist offence, referred to in Article 5 of the Terrorism Directive. The punishable incitement has to cause a danger of the offence or a punishable attempt being committed.

We have same kind of a procedure for the blocking also covered by Article 21. Provisions related to that are in Section 185 of the Information Society Code:

https://www.finlex.fi/fi/laki/kaannokset/2014/en20140917.pdf

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

The current legislation and arrangements are deemed sufficient. Police can contact service providers and notify them on possible illegal content after which the service providers can make an independent decision whether to remove the content. When a crime is suspected and the illegal content is hosted in Finland, a court order to remove the content is a sufficient procedure.

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

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

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

There are no researches or statistics (confirmed data) to back this evaluation to one way or another, but it is estimated that the level of terrorist content online has stayed at the same level.

However, it should be noted that terrorist content online is more accessible nowadays as the content is user generated, in English, and it is aimed at the Western societies. Therefore it might seem that the level of terrorist content online has increased.

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?

This might pose some risks, as it could have an impact on ongoing information gathering etc. However, if service providers store content and publisher of the deleted data, this is risk significantly reduced.

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?

No such incidents have occurred in Finland.

A mitigating measure for erroneous removal would be a possibility for the producer of the content to ask the hosting service to return the (removed) content back online.

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?

At this stage the work of the EUIF complemented by the Recommendations are sufficient as long as the Recommendations' implementation is monitored regularly by the Commission and EU Internet Forum.

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)?

-

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)
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].
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)
4	More detailed requirements on transparency and reporting
4	More detailed requirements to companies on safeguards against over-removal
3	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.
3	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?

One possibility to reinforce voluntary approach would be commending openly those platforms doing well and in this way giving positive publicity the companies that work on voluntary basis to tackle terrorist content online.

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

Platforms that are used for dissemination of illegal and terrorist online content need to be recognised and approached with the companies already involved in this work in order to encourage them to cooperate on this phenomenon. Information on the work of EUIF should be distributed to the companies not yet involved.

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?

Small companies should be provided tools for automated content recognition. Access to these tools should be granted via cooperation with different stakeholders.

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
X	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?

<u>At this time Finland does not consider new specific legislation necessary.</u> Enough time should be given to the proper implementation of the Council Recommendations given in March 2018. Applicability and the level of implementation of the Recommendations should be examined during 2019 after which the necessity of new legislation could be properly evaluated. However, if the Recommendations were not provide the desired outcome, Finland would be willing to examine possibility for legislative proposals on terrorist content online.

RISKS

It should be noted, that not all material that is being monitored and in a need to be removed, relate to terrorist *crimes*, therefore legislative measures might cause further, counterproductive consequences in Member states.

Terrorist and illegal content online is a global phenomenon in which case legislation encompassing only EU might not have the desired effect as the service providers could locate to an area less restrictive.

BENEFIT

Having one set of legislation in the EU could make the situation clearer as the companies would have similar setting in all of the Member States. In a situation that each Member State end up drafting their own national legislation, service providers might relocate within the EU to countries that have more lenient legislation.

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:

[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

To what extent should material produced by UN/EU designated terrorist organisations 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)

5	Definition of terrorist content (*see question above*)
4	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)
	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
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
5	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)
5	Nomination of point of contact within Companies
5	Reporting obligations for companies[6]
4	Transparency requirements for companies vis a vis their users[7]
5	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?

-

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

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?

Should the suggested legislation be drafted, the scope ought to be extended to other service providers as well. The legislation should encompass also internet registrars and internet registries to tackle properly dissemination of the illegal content online. This is something to be negotiated with ICANN, which is in a position to make binding agreements with mentioned parties in order to include them to tackling dissemination of terrorist/illegal content online. **If the suggested legislation were to only consider social media platforms, would this mean that large portion of the internet publications wouldn't be covered by the legislation.**

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, with small amount of users, should be covered by the legislation, should this kind of legislation be drafted. However, the impact on the smaller companies should be assessed and the measures should be practicable and proportionate. Legislation and recommendations should be drafted so that all actors obligated by them are also able to act accordingly.

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?

Should the legislation be drafted, possible impact on fundamental rights need to be taken into careful consideration.

Legislative package on interoperability was discussed extensively in a high level group with participation from relevant agencies and stakeholders prior to Commission proposals for regulation - this kind of wide approach at the preparatory phase could be a good model, should the Commission decide to go ahead with new, specific legislation to tackle terrorist content online.