European Commission

STATE OF THE UNION 2018

A Europe that protects: Countering terrorist content online

#SOTEU

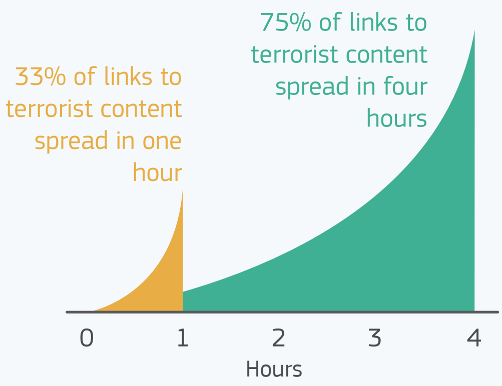
12 September 2018

'My Commission has prioritised security from day one — we criminalised terrorism and foreign fighters across the EU, we cracked down on the use of firearms and on terrorist financing, we worked with internet companies to get terrorist propaganda offline and we fought radicalisation in Europe's schools and prisons. But there is more to be done.'

Jean-Claude Juncker, State of the Union Address, Strasbourg, 14 September 2016

The continued presence of terrorist content on the web is a grave risk to citizens and to society at large. Its potential for causing harm is made worse by the speed with which it spreads across platforms. Several of the recent terrorist attacks in the EU have shown how terrorists misuse the internet to spread their messages. So far, the approach to cracking down on the proliferation of terrorist content online was based on voluntary cooperation. Whilst significant progress has been made under the EU Internet Forum established in 2015, it is clear that more needs to be done to ensure the engagement of all internet platforms and national authorities to protect Europeans online and deny terrorists the ability to spread their propaganda online.

SPEED OF DISSEMINATION



The Commission is proposing a new approach with clear and transparent rules to ensure that when terrorist content is identified:

- it is taken down as early and as quickly as possible;
- online platforms take measures to ensure that their services cannot be misused and that removed content is not re-uploaded elsewhere;
- citizens' fundamental rights to freedom of expression and information are fully protected.

What is the Commission proposing?

ONE-HOUR RULE

Terrorist content is most harmful in the first hours of its presence online because of the speed at which it spreads. The Commission is therefore setting a legally binding one-hour deadline for content to be removed following receipt of a removal order issued by national authorities.

BETTER PROTECTED ONLINE PLATFORMS

Hosting services exposed to terrorist content will be required to better protect their service and their users from terrorist abuse by taking proactive measures, for example to prevent the re-uploading of terrorist content once removed, including through automated means. To avoid an excessive burden on companies, these proactive measures must be proportionate to the risk and level of exposure of internet platforms to terrorist content.

INCREASED COOPERATION

Service providers and Member States will be required to designate points of contact reachable 24/7 to facilitate the follow up to the removal orders and referrals. The new rules set up a framework for strengthened co-operation between hosting service providers, Member States and Europol.

STRONG SAFEGUARDS

To mitigate possibly erroneous removal of legal content, hosting service providers will be required to have effective complaint mechanisms in place and to inform users when their content is taken down – unless there are significant security reasons not to do so. When making use of automated detection tools, human oversight and verification are to be in place to prevent erroneous removals. Member States will need to guarantee effective judicial remedies as well as the right to challenge a removal order.

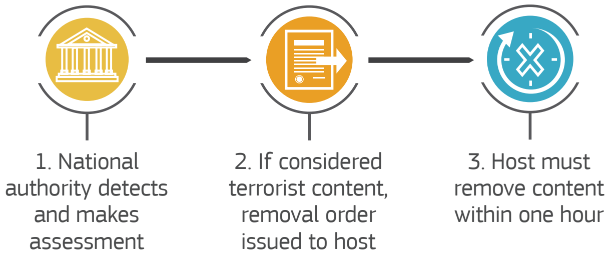
INCREASED TRANSPARENCY AND ACCOUNTABILITY

Hosting service providers will have to publish annual transparency reports and Member States will be required to submit an annual account of their actions to help reduce access to terrorist content online to the Commission, who will establish a programme for monitoring the results and impact of the new rules.

STRONG PENALTIES

Effective, proportionate and dissuasive penalties for not complying with orders to remove online terrorist content will be put in place. In the event of systematic failures to remove terrorist content, a service provider could face financial penalties of up to 4% of its global turnover for the last business year.

How does the new procedure for removing terrorist content work?


1. National authority detects and makes assessment

2. If considered terrorist content, removal order issued to host

3. Host must remove content within one hour

- **Right to challenge**: Hosting service or content provider may appeal the removal order. If the appeal is successful, the content is restored; if the appeal is rejected or the deadline lapses, the removal order stands and the content must be permanently removed.
- **Obligation to report**: If issued with a removal order, the host must report on proactive measures taken to address terrorist content online three months after receiving the removal order.

Why step up work now?

Terrorist content continues to circulate online, representing a real risk to European citizens. For instance, almost 700 new pieces of official Da'esh propaganda were disseminated in January 2018 alone. The fact that this type of propaganda can be spread rapidly across platforms demands an equally rapid response. Any propaganda that prepares, incites or glorifies acts of terrorism is illegal and must be taken offline.

The 'Database of Hashes' launched by companies within the EU Internet Forum in 2016 contains over 80,000 hashes of known terrorist videos or images.

Over 60,000 examples of terrorist content online flagged since 2015 by the EU Internet Referral Unit at Europol.

Over 150 companies identified as hosting terrorist content according to Europol.

To whom will the rules apply?

Once adopted by the European Parliament and the Council, the new rules will apply to all internet companies offering services in the EU, wherever their headquarters are based in the world and irrespective of their size.

Who does what?

Hosting service providers should:

- put in place **robust procedures** to be able to deal with removal orders and referrals;
- have a **designated point of contact** reachable 24/7 and responsible for the swift removal of content (within one hour of receiving a removal order) and for communication with national authorities;
- ensure that **safeguards** are in place — including human oversight — to avoid content being erroneously removed when automated tools are used;
- put in place effective **complaints procedures** so users can appeal against content that they consider has been removed in error;
- **cooperate with national authorities** on measures taken to remove terrorist content and prevent it from being hosted, uploaded, and re-uploaded — in the case of content involving a threat to public safety, law enforcement authorities should immediately be informed;
- set out in their **terms and conditions** their policy to prevent the dissemination of terrorist content and publish annual **transparency reports** on action taken to tackle this issue. Those affected by terrorist content should also provide reporting to the relevant Member State on their actions.

Member States should:

- ensure the responsible authorities have the **capacity** to identify terrorist propaganda online and swiftly issue removal orders or referrals where necessary;
- **coordinate** with other Member States and Europol to ensure that evidence of online terrorist content is flagged, and that duplication and interference in national investigations is avoided;
- put in place adequate **appeals procedures** for platforms and content providers to be able to complain if they consider a removal order to be unjustified;
- determine the **financial penalties** for online platforms found in breach of removal orders, taking into account all the relevant factors set out in the Commission's proposal.

Europol should:

- **refer** terrorist content to online platforms;
- **facilitate and coordinate** referrals and removal orders, to ensure that duplication is avoided;
- act as a **point of contact** for platforms who are unsure which Member State they should alert in relation to evidence of terrorist offences;
- provide expert **support and advice** to both Member States and hosting service providers.