In 2015, the European Commission launched an EU Internet Forum – a platform for voluntary cooperation with Member States and online platforms to tackle terrorist content online. The work of the Forum has already brought some tangible results and has given rise to similar actions at the global level.

In the aftermath of the terror attack in Christchurch, New Zealand, government leaders and online platforms agreed on the Christchurch Call for Action. On this occasion, President Juncker announced the development of an EU Crisis Protocol in the context of the EU Internet Forum.

On 7 October, the participants of the Forum committed to this Crisis Protocol, providing a rapid response to contain the viral spread of terrorist and violent extremist content online. The EU Crisis Protocol will contribute to efforts undertaken at global level in the context of the Christchurch call, in particular the Crisis Response Protocol as announced in September at the margins of UNGA.

**What is the EU Crisis Protocol?**

The EU Crisis Protocol is a voluntary mechanism to help coordinate a rapid, collective and cross-border response to the viral spread of terrorist and violent extremist content online. The Protocol outlines the procedures, roles and responsibilities of key actors as well as the tools for monitoring and exchanging critical information. It ensures that any response safeguards fundamental rights and respects relevant legal frameworks, in particular the General Data Protection Regulation.

**Response mechanism: step by step**

**DETECTION**

Identification of an incident – where terrorist and violent extremist content spreads online rapidly – as a crisis. This includes an assessment of its geographical scope and the speed with which the online content spreads.
EU Member States should communicate with the public, media and other relevant stakeholders throughout the crisis related to the viral spread of terrorist and violent extremist content online. In particular, they should provide factual information to:

- Reassure the public the crisis is being managed
- Ensure any tensions are mitigated
- Prevent the spread of fake news

### NOTIFICATION

<table>
<thead>
<tr>
<th>MEMBER STATES</th>
<th>ONLINE SERVICE PROVIDERS</th>
<th>EUROPOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Member State and Europol alert online service providers via existing platforms and channels as well as any third country affected.</td>
<td>Online service provider alerts Member States affected, Europol and other service providers.</td>
<td>Europol can provide support as a Coordination Centre when several EU Member States affected.</td>
</tr>
</tbody>
</table>

### COORDINATION AND INFORMATION SHARING

Exchange of information between law enforcement and online service providers on a voluntary basis to effectively contain the crisis, as well as on measures taken to remove and disable access to the content in question.

Coordination of efforts between different actors, including preparation of operational plans by national law enforcement, real-time referrals to online platforms and sharing of hashes and URLs as well as crisis log.

### POST-CRISIS REPORT

A joint assessment of the response by all the actors involved to identify any gaps and lessons learnt for the future, while ensuring transparency towards the public on actions taken.

### CRISIS COMMUNICATION PRINCIPLES

EU Member States should communicate with the public, media and other relevant stakeholders throughout the crisis related to the viral spread of terrorist and violent extremist content online. In particular, they should provide factual information to:

- Reassure the public the crisis is being managed
- Ensure any tensions are mitigated
- Prevent the spread of fake news