EU CRISIS PROTOCOL:
COLLECTIVE RESPONSE TO VIRAL SPREAD OF TERRORIST AND VIOLENT EXTREMIST CONTENT ONLINE

This is a working document drafted by the services of the European Commission and Europol to guide work under the EU Internet Forum.

I. Introduction

The terrorist attack in Christchurch on 15 March 2019 showed how an event in one country can have an immediate and significant impact across the globe: the attack was livestreamed on the Internet and the video was reproduced and shared at an unprecedented rate. The speed and volume at which the depictions of the terrorist attack were disseminated and the vast number of online service providers (OSPs) that were misused and exploited showed the limitations of the existing processes to address similar threats. This attack highlighted the need for a coordinated cross-border response across online service providers and law enforcement in relation to terrorist or violent extremist incidents with a significant online component.

The crisis response protocol should apply to extraordinary situations where the normal operating procedures are clearly insufficient. The overall aim is to disrupt the terrorists' aims while safeguarding dignity of victims and rights of users of online platforms. With the establishment of an EU crisis protocol the Commission will contribute to the Christchurch Call for Action. The adoption and implementation of the crisis protocol will be carried out in full transparency aiming at a large number of OSPs signing up to it. The protocol is a voluntary framework, and does not replace existing legal procedures or other regulatory action taken by Member States.

I. Aim

The EU Crisis Protocol on a collective response to viral spread of terrorist and violent extremist content online is a voluntary mechanism to enable a coordinated and rapid response to a cross-border crises in the online space stemming from a terrorist or a violent extremist act. The Protocol aims to facilitate rapid assessment of the online impact of terrorist attacks, secure and timely sharing of critical information between EU Member States law enforcement (LE) and other competent authorities, Union bodies (and in particular Europol), Online service providers (OSPs) and other relevant stakeholders in accordance with relevant legislation and within the relevant mandates, and to ensure effective coordination and management of the crisis.

The EU Crisis Protocol describes the voluntary procedures, roles and responsibilities of key actors, the tools used for monitoring and exchanging critical information, as well as the overall coordination and de-confliction mechanisms.

The response outlined in the protocol should be implemented with strong safeguards for protection of fundamental rights and in full respect of relevant legal frameworks, in particular the General Data Protection Regulation. The protocol is without prejudice to existing legal requirements and procedures (e.g. for evidence gathering, data retention) as well as future legislation to prevent the dissemination of terrorist content online or access to e-evidence. Finally, the protocol fully recognises national legal frameworks and the existing crisis management mechanisms applicable at national and international level and strives to complement them by streamlining the transnational activities and facilitating the collaboration with the relevant international players.

II. Definitions

For the purpose of this Protocol the following definitions will be used:

A **crisis** within the meaning of this Protocol constitutes a critical incident online where:

(1) the dissemination of content is linked to or suspected as being carried out in the **context of terrorism or violent extremism**, stemming from an on-going or recent real-world event which depicts harm to life or physical integrity, or calling for imminent harm to life or physical integrity and where the content aims at or has the effect of seriously intimidating a population; **and**
(2) where there is an anticipated potential for exponential multiplication and virality across multiple online service providers.

A strong indicator of terrorist or violent extremist context is where the content is produced by or its dissemination is attributable to listed terrorist organisations or other listed violent extremist groups. The Protocol pertains only to online content stemming from events of a suspected criminal nature.

'**Online Service Providers**' (OSPs) will refer to any platform or service that enables the public dissemination, storage or access to user-generated digital content.

III. Actors

The Protocol requires actions by several actors and entails different roles and responsibilities for the key stakeholders involved.

There are actors who will have a central role, especially the Member States law enforcement and other competent authorities of the Member State where the attack occurs, Europol, online service providers including dedicated industry forums such as the Global Internet Forum to Counter Terrorism (GIFCT) and specialised partnerships such as Tech against Terrorism. The following actors have a central role in monitoring, analysing and notifying a crisis as well as putting in place appropriate response mechanisms:

- EU Member States' Law Enforcement (Internet Referral Units and other competent authorities)
- Europol (and within it the ECTC, including the EU IRU and the Operational Centre)
- Online Service Providers (OSPs)
- Global Internet Forum to Counter Terrorism (GIFCT) and Tech against Terrorism

In addition, a number of other actors are key in ensuring a coherent response, depending on the specific crisis situation. These include third countries which could be affected by the crisis incident online, non-governmental organizations and academia who also have capacity to monitor and analyse both the situation and response. In addition, media organisations whose reporting of the events can have a significant impact on the course of the crisis may also be alerted to the events by the Member States where they are located, in full respect of freedom of the press and national safeguards.

IV. Process description

Stage 1 - Detection and classification

Europol, EU Member States' Law Enforcement, OSPs and third parties or entities with a monitoring system in place, should assess the occurrence of a potential crisis online. The monitoring and reporting mechanisms are under each actor's responsibility in accordance with the legal framework under which they operate

Based on the information available and having evaluated it for accuracy and reliability, any of the relevant actors should assess if any online content has the potential to evolve into a crisis which warrants the triggering of the operational stages of the Protocol or whether it should be handled within the applicable normal operating procedures of each actor.

***RED** = Crisis; **YELLOW** = normal operating procedures, increased monitoring; **GREEN** = normal operating procedures*

Indicators

Target	*Explanation of the indicator*	**Impact**	*Explanation of the indicator*
Geographical scope	Number of jurisdictions/ countries potentially affected	***Virality***	Reach and speed by which the content is publicised and reproduced
Online service providers	Number or type of OSPs affected (e.g. size of global audience) Diversity in the type of OSPs affected (e.g. social media, file sharing, websites);	***Reproducibility***	Level of expertise required to ensure virality (how easy is it to replicate the content)
Type of attack/ Victims affected	Terrorism or extremist context of the attack, soft or hard targets, number of victims, past, ongoing or imminent attack.	***Resilience***	Resilience of the content to takedown

Case example 1:
Christchurch attack

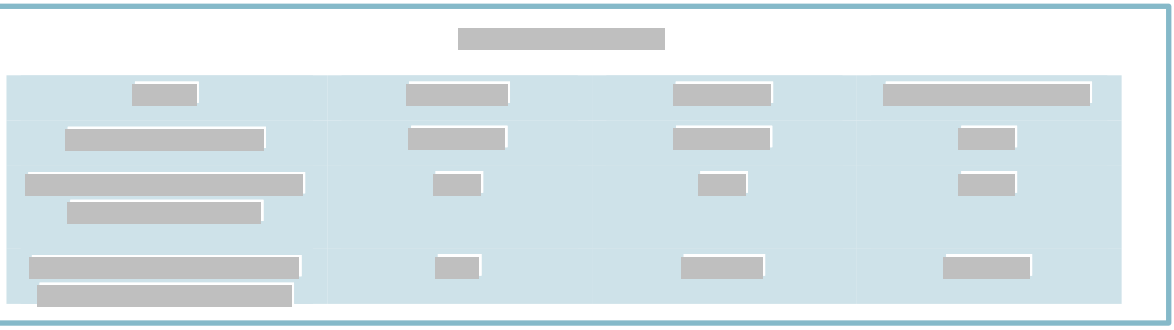
On 15 March 2019, a user of an online forum announced his intention to carry out an imminent gun attack and to livestream it on his social media account. He shared beforehand a publication (manifesto) providing information on the motive behind the attack. The video of the attack on two mosques in Christchurch, New Zealand, was subsequently livestreamed as announced. The attack resulted in the killing of more than 50 and 41 injured. The content of the video, manifesto, and forum post clearly suggested a right wing extremism motivated attack. The video of the attack and the manifesto were shared online by a large variety of Internet communities, and news organisations intensively reported on the attack and featured related propaganda material (video of the attack and manifesto) in news reports.

Case example 2:
Killing of two Scandinavian tourists in Morocco

On 17 December 2018, two tourists from Denmark and Norway were stabbed and beheaded in Morocco. On 19 December 2018, a video recording of the killing started circulating on multiple OSPs. The video was shared by varied Internet communities and news organisations. A second video showing the alleged perpetrators pledging allegiance to IS leader Abu Bakr al-Baghdadi was shared online on 20 December 2018.

Case example 3:
Release of the video "In the hospitality of the Emir of the believers"

The so-called Islamic State (IS) terrorist organisation released on 29 April 2019 a video entitled "In the hospitality of the Emir of the believers", featuring for the first time in nearly five years IS leader Abu Bakr al-Baghdadi. The video was extensively shared online among IS sympathisers and reported by news organisations.



Stage 2 - Response

2.1 Notice of a crisis

Where an actor assessed an incident to constitute a crisis in the online space it should communicate the assessment and any other appropriate information to the relevant stakeholders, using the pre-agreed communication channels and Points of Contact (PoC).

Europol will act as a Coordination Centre for Member State response,

- [redacted]

2.2 Crisis Coordination and information sharing

Following the notification each actor will take the necessary steps to contain the crisis. These steps include information sharing as well as measures to remove and disable access to the content in question.

Information exchange between law enforcement and online service providers

During the crisis, law enforcement authorities and Online Service Providers should endeavour to share information on the nature and spread of the content at issue [redacted].

The information exchange will be done on a voluntary basis and should comply with the respective legal framework and data protection regimes of each actor as well as any existing legal requirements and procedures (e.g. for evidence gathering) as well as future legislation to prevent the dissemination of terrorist content online or access to e-evidence.

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted].

[redacted]

[redacted]

2.3 Safeguards against undue removal of content

Online services providers should provide appropriate and effective complaint mechanisms challenging the removal of content or the prevention of its upload, including the possible reinstatement of content or user accounts that may have been removed or closed in error[2].

2.4 Communication with other stakeholders during and in response to a crisis

EU Member States should communicate with the public, media (e.g. where they disseminate the relevant online content) or other relevant stakeholders and communities during and in response to a crisis, including by ensuring the availability of relevant information to help preserve public safety. During a crisis, communication is best used to reassure the public that the crisis is being handled, mitigate against, de-escalate tensions and hinder the spread of misinformation and disinformation. [redacted]

[2] Content should be considered as being removed "in error" where the content in question is either not illegal under the applicable legal framework or not in contravention of the companies' own terms of service.

Crisis Communication Principles

Decide if to communicate. Unless there is a credible threat to an EU Member State which would constitute a crisis, communication may further legitimise and give visibility to the propaganda efforts of terrorist and violent extremist groups.

Be first, be fast, be accurate. Governments and law enforcement authorities should, as soon as a crisis warrants a communication response, communicate on the events and the actions being taken to hinder the spread of fake news.

Be transparent. If there are things you do not yet know, communicate the processes, procedures and timescales that are being implemented to ascertain this information.

Show leadership and be reassuring. It is important that governments and law enforcement authorities demonstrate that the crisis is being dealt with, while appealing for calm to seek to allay public fears and concerns for safety. Showing solidarity and empathy towards the affected communities is crucial.

Language. Choose terminology carefully to describe the nature of the crisis, the perpetrators and the affected communities so as not to stigmatise.

Stage 3 - Crisis closure and reporting

Once the crisis has been contained, a closure notice is sent by the entity having activated the crisis protocol mechanism to all actors who received the initial notice. A multi-stakeholder assessment of the response including its effectiveness in disrupting the terrorist narrative and minimising harm to users will be carried out.

a set of recommendations with the aim improving or adjusting the protocol. This report should be shared with and endorsed by all participants.

The closure of the crisis protocol should also include **transparency** towards a wider set of stakeholders, as to the actions taken during the crisis by both the online service providers and the involved law enforcement authorities, which should to the extent possible include public reporting on the nature and volume of any content removed.

[3] It is important that the reports provided by companies contain sufficiently detailed information. Companies should indicate the level of sensitivity/confidentiality.