Ref. Ares(2020)5998852 - 27/10/2020

MEETING OF THE EU INTERNET FORUM
16 JULY 2019
12:30-16:00

VENUE: ALBERT BORSCHETTE CONGRESS CENTER (CCAB), ROOM 3C,
RUE FROISSART 36, B-1049

ANNOTATED AGENDA

UNFORTUNATELY WE WILL NOT BE IN A POSITION TO OFFER INTERPRETATION

12:30-13:30 **Lunch**

13:30-15:00 ***EU Response protocol for Online Crisis***

The EU Response Protocol to Online Crisis (ERPOC) should be a mechanism to enable a coordinated response to a cross-border online crisis in the context of terrorism or violent extremism, between EU Member States law enforcement (LE) authorities, Europol, online service providers (OSPs) and possibly other organisations. The Protocol should aim to secure a rapid response to an ongoing or imminent online crisis, including secure and timely sharing of critical information and effective coordination and management of the crisis.

Following a brief presentation of the overall approach and key elements of a future potential crisis protocol, participants are invited to share their views and update on crisis response mechanisms developed by industry partners. We would aim to steer the discussion through examples, participants are also encouraged to present concrete cases to illustrate scope and potential functioning of the elements outlined below which would form part of the future crisis protocol.

1. **Discussion on what constitutes a crisis**

a. **Online crisis in the context of terrorism and violent extremism – what are the defining elements*?***

What type of event should trigger a crisis response? What should be the defining elements and what should be out of scope? The following aspects could be considered:

- *Depicting ongoing harm to life or physical integrity, or calling for imminent harm to life or physical integrity*
- *Context to terrorism or violent extremism (e.g. where the act has the effect of or aims at intimidating a population)*
- *Designed for virality, taking into account fast multiplication and virality across OSPs facilitated by a number of pointers.*

Are there other aspects that should or could be taken into account?

b. ***Case examples***

2. **Assessment and Classification of the online crisis**

What could or should be relevant indicators for assessing the occurrence of an online crisis? Do you consider the following indicators as relevant and useful: **g***eographical scope (affecting one or more countries, number of OSPs affected speed and longevity of the publicized content, resilience to takedown? What other aspects should be considered?*

Where is the threshold? Should there be gradation between low, medium or high risk (with a different response depending on the gradation) or rather a simple classification of crisis vs no crisis.

3. Crisis management

- ***Response:*** *Do we need different responses depending on the type or grade of crisis?*
- ***Key actors:*** *In addition to the EU IRU in Europol, OSPs and MS's law enforcement, which other actors should be involved in the Protocol? (Interpol, third countries and international bodies/organisations, traditional media companies, Tech Against Terrorism and other relevant organisations or researchers). Should they have different roles and responsibilities? Should all be able to trigger the crisis protocol?*
- ***Triggering the online crisis response:*** *Which actors can trigger the online crisis and what is the chain of notification (law enforcement/Europol vs GIFCT triggered)?*
- ***What type of communication channels should be defined?:*** *i) contact points, ii) secure communication channels, iii) relevant information (including hashes, urls etc)? What are possible legal or technical constraints to be taken into account (e.g. data protection regimes ?)*

4. De-escalation - Crisis closure and reporting

Debriefing between different actors*: How to assess the effectiveness of the crisis response and identify any lessons learnt to improve future actions (for instance through recommendations presented after the debriefing, evaluations of the procedures).*

15:30-16:00 Next steps and conclusions