EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A: Internal security
Unit A.1: Crisis management - Terrorism

Brussels, 14 October 2014

██████████

REPORT

Subject: **Ministerial dinner with the Internet industry to respond to the terrorist use of the Internet – Luxembourg, 8 October 2014**

Participants : See annex

Summary :

The ministerial dinner provided a sound basis for further cooperation between the Member states and the internet companies both on efforts to eliminate illegal content from the internet and to counter online terrorist propaganda and radicalisation. The consensus was that this successful first encounter should lead to further dialogue. While the discussions were rich, it is to be noted that only a handful of Member States of the twenty or so Member States present intervened in the discussion. They, and the industry representatives, welcomed this initiative to bringing together the real players in the efforts to identify the best tools to reduce terrorist use of the internet and social media.

Details

In her introductory remarks, the Commissioner explained the intention of the gathering to find a common ground to create a possible partnership between member states and private internet companies to address the challenges posed by the use of the internet and social media. She stressed that the Commission ████████████████████████████ ██████████████████████████████████ support the process of a dialogue and partnership between stakeholders. She highlighted that all shared the same democratic values. While effective mechanism to withdraw illegal content from the internet is essential, she underlined the necessity to give a bigger strategy push to the counter narratives space to win over hearts and minds, using the technology offered by the internet companies. On the response to the challenge, the Commissioner highlighted her readiness to support joint training and awareness raising initiatives, including offering financial support to Member States.

████████████████ welcomed the Commission's initiative to build a public-private dialogue around the current challenge. The respect of fundamental rights was highlighted (i.e. the court of Justice case on data retention). Responses should include both the promotion of

counter narratives and repressive measures removing illegal content. Minister Alfano insisted on the need to build dialogue and trust between law enforcement authorities and the private sector enabling the exchange of information and best practices. In that spirit, ███ welcomed the Commission's idea to support joint training sessions between the different stakeholders.

████████████████████████████████, recalled the level of professionalization and the speed of terrorist propaganda used by terrorist organizations such as ISIL and affiliates which master not only the internet content but also the strategic communication to recruit, to "scare the enemy", to promote the Caliphate or to threaten the West. The CTC recalled some of the responses initiated by the Commission (RAN, support to the SCATT – the European Syria Strategic Communications Advisory Team) or in Member States (particularly in NL and in the UK), and the efforts which are still to be made to challenge the extremism narratives. Movies such as the ████████ should be scaled up all the while measuring the impact of such measures. Industry can support actions by training moderate voices or to craft the message. On the repressive side, the CTC said that illegal content should be removed from the internet. Even if it is not always the most effective response, we need to continue to harass the extremists. Also, there is a need for a flagging system, and work with trusted flaggers in YouTube. Building public-private trust would ease the cooperation, especially via staff training session.

████████████████████ recalled the importance to keep a safe online environment (also for business reasons). The partnership with law enforcement has been essential notably in a programme ██ ████████████████████ mentioned a 96% accuracy rate which lead to take-down actions from ██████ On images, ██████ mentioned that although sometimes very painful to watch, images may enlighten on what motivates extremists. The challenge for ██████ is to provide ability to be informed. ██████ applies a 0% tolerance on video or images that make the promotion of terrorist training, violence or beheadings. However, shutting down does not apply to information on terrorist groups that may increase the understanding of the groups themselves. On counter narratives, ██████ highlighted the support given to the project ████████ and stressed the need to build strong and effective counter narratives that build on community as many vulnerable individuals seek a sense of belonging to a community. In the ██, ██████ has trained ████████ to work with large audiences. Finally, ██████ mentioned the importance of involving professional in communication to tailor messages.

████████████████████ stressed that addressing the use of internet by extremists requires a multi-prone approach. The tools of internet are powerful tools. ████████ policies doesn't allow extremist groups (i.e. ISIL) to have a ████████. But ████████ noted that sometimes ████████ is needed to recognize terrorist groups, which activities start offline and end online. Work is undertaken by a review team working 24/7. ████████ admitted that there are limits to the removal of internet content. ██ mentioned the area of child pornography as one area where ████████ has experienced good cooperation and dialogue with law enforcement authorities. ██ indicated that internet companies have developed collaborative working methods between themselves. On counter narratives, ████████ highlighted the need to educate groups to reach and moderate vulnerable populations. Finally, ████████ insisted on the importance of research, particularly in three areas : 1) identifying the best speakers to deliver counter narratives (public authorities are not the good ones); 2) defining the best counter violent content (photo, text, story, ..) and on works best for a specific group; and

3) understanding the broad landscape (what works in a country or community, doesn't necessarily work in another country/community). Finally, some assessment is possible through ███ or ████████████████. ████████ has indicated its willingness to share lessons learned with Member States.

████████████ from ████ pointed out that because of the nature ████████, which can be ████ or ████ not ████████, and on its amount, ████ does ████ ████. However, ████ applies a number of policies and rules which are reviewed regularly according to major incidents. On the removal of illegal content, ████ uses a number of mechanisms to be kept informed; a major difficulty encountered is that sometimes behavior considered illegal in a country is not in another (i.e. in the area of hate speech). On counter narratives, ████ works with civil society organizations to use the platform more effectively to suggest counter messages. A partnership with law enforcement authorities already exits to request information and deliver best responses.

████████████████████ explained the procedures and mechanisms put in place to keep the internet community safe through tools such as the community monitoring, review teams, waiting system, which operate particularly in the area of child abuse and pornography. ████ indicated that the interest from the public on how ████████ collaborates has increased recently ████ the ████████. ████ called for an international system of rules that would apply to all. ████ explained that ████████████ are located in different places; in Europe, the data center ████████████. In a veiled reference to the ████████████████████████ said that the rules applied in ████████ requiring ████████████████ ████████████ called for working to respect fundamental freedoms when accessing to data.

████████████████ welcomed the meeting with private internet companies and highlighted the need to cope with the speed and changes in tone of online extremists content, particularly considering that the threat represented by foreign fighters involve more and more youngsters. Many also exploit counter narratives to develop violent extremism behaviors. The threat calls for a robust response through a joint partnership involving public and private actors as well as civil society and community. ████ greeted the work undertaken so far by private companies. ████ explained the work done by the ████ ████████ which has allowed the take-down of ████████ so far. ████ is now willing to share lessons learned. ████ also indicated that while the work undertaken by big private companies has been key to keeping the internet environment safe, much is still to be done to support small internet companies. In this context, a public statement to encourage small industry to remove illegal content would be useful.
On the positive side (counter-narrative), ████████ praised the Commission' support to the SCATT project, as an important step to build cooperation between Member States. Civil society groups should be encouraged to occupy the online space. The Minister finally highlighted the importance to learn from what is done in other fields, i.e. on global child pornography.

████████████████ highlighted the need to build long term trust with private companies. The dialogue should inter alia include how to better use the flagging system, the involvement of civil society, and how to deliver the best messages which require understanding the broader landscape. Efforts should concentrate on the two aspects: facilitating counter-narratives and removing illegal content.

██████████████████████ indicated the need on one hand to find the right balance between fundamental rights/freedom of speech and, on the other hand, the protection of people, specifically young, from violence. ██ mentioned that in ██████, the police is present on social media, i.e. Facebook, as part of the preventive work. The Minister also praised the work of the RAN.

██████████████████████ referred to the Budapest international Convention on Cybercrime which 5 Member States did not yet ratified, indicating the need for more proactive attitude. Greater cooperation with the private sector is important. ██ welcomed the removal of content on child abuse and pornography. However ██ indicated that drawing the line on what is illegal or not is more difficult in areas as hate speech or the promotion of violence.

██████████████████████ highlighted the importance to complement the support to civil society to elaborate counter narratives with appropriate legal measures on the criminalization of passive incitement. A new framework is being adopted soon in ████, which will include inter alia the cooperation with internet companies. ██ also mentioned that other measures could draw inspiration from what is done in other sectors, such on pornography.

██████████████████████ confirmed that the process of radicalisation takes place more and more through the internet. Law enforcement efforts fall short in the face of the proliferation of extremist blogs; hence, the need for more public/private cooperation. The Minister summarised the package of proposed measures to remove online illegal content in ████ which allow administrative authorities to block the access to internet website. ██

In its answer, ████████ indicated that Member States are aware of notification procedures to remove illegal content. Problem arises with understaffed small internet companies. ████████ indicated that it helps already these companies, particularly in the area of child abuse.

In her concluding remarks, the <u>Commissioner</u> recalled the consensus on the need to collaborate. She welcomed this beginning of what she hopes to be a process leading to a public/public collaboration on research, training, counter-narratives and the sharing of best practices.

At the end of the meeting, an agreed press-release was issued by the Commission (see attached).

***

██