

# REPORT ON THE CONFERENCE ON PUBLIC PRIVATE DIALOGUE TO FIGHT ONLINE ILLEGAL ACTIVITIES

27 November 2009, Centre Borschette, Brussels

All PowerPoint presentations, and the conference programme are available on request from Carmen Guillén Sanz

## **1. Introduction- the context of the conference:**

### **1.1 Objectives**

The Conference was organised with the aim of setting up an informal platform for dialogue where different issues and topics related to the fight against online illegal activities could be discussed among private and public stakeholders as well as NGO-operated complaint hotlines. The creation of such platform for dialogue builds upon the Council Conclusions of 27 November 2008 on a concerted work strategy and practical measures against cyber-crime.

### **1.2 Background**

The Council Conclusions of 27 November 2008 invited Member States and the Commission, in particular, to draft, in consultation with private operators, a European agreement model for co-operation between law enforcement agencies and private operators.

The Framework Decisions listed below made punishable respectively the dissemination of child pornography; incitement to racist and xenophobic violence or hatred; provocation to commit terrorist attacks, terrorist recruitment and training legislation, also when it takes place online:

- the Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography (OJ L 13 of 20 January 2004, p. 44),
- the Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law (OJ L 328 of 6 December 2008, p. 55) and,
- the Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism (OJ L 330 of 9 December 2008, p. 21).

## **2. Participants**

- Representatives of the private sector, including European associations of telecom operators, internet service providers and mobile phones operators –ETNO, EuroISPA, GSMA- as well as companies such as Microsoft and e-Bay.
- Representatives of NGOs coordinating the action of complaint hotlines in Europe – INHOPE and INACH.
- Representatives of national authorities from France, Germany, Ireland, Portugal, Romania, Spain, Sweden, The Netherlands, United Kingdom.
- The EU Counter Terrorism Coordinator, representatives of the EU Council Secretariat, the Council of Europe, Europol and Interpol.
- Representatives of the Commission including DG JLS and DG INFSO

### **3. Detailed report**

*[Morning session]*

#### **3.1 Opening words**

Mr Martin Schieffer, Deputy Head of Unit, Fight against Terrorism, DG JLS, underlined, on the one hand, the seriousness of criminal activities online such as the dissemination of child pornography, incitement to racist and xenophobic violence or hatred, provocation to commit terrorist attacks, terrorist recruitment and training and, on the other hand, the need for smooth cooperation between public and private sector in order to fight such offences efficiently.

Mr Gilles de Kerchove, the EU Counter Terrorism Coordinator, stressed the importance of online criminal activities as a growing problem and gave an overview of what had been done so far to prevent criminal activities online, especially in the field of counter-terrorism, including the amendment of the Framework Decision on combating terrorism as well as to the project Check the Web. More importantly, the Counter Terrorism Coordinator focussed on what should still be done, in particular through public-private partnership. He advocated the need to take tough action on the web to prevent illegal activities and differentiated between negative actions, including notice and take down, de-registration and filtering, and positive actions, in particular the empowerment of the users and the promotion of media literacy.

Mr Michael Carlin, on behalf of the EU Presidency, supported the goal of the conference and underlined the importance of respecting freedom of speech in every action taken to fight illegal activities online.

### **3.2 Introduction: the reason and the aim of this dialogue**

*Mr Jakub Boratynski*, Head of Unit, Fight against Organised Crime, DG JLS, explained the background of the conference (referring to the recommendations on public-private cooperation annexed to the Council Conclusions of 27 November 2008) and its objectives. He stated that fighting illegal content was a priority for the Commission and stressed the high expectations of the Commission when setting up this platform for dialogue between public and private sector. Mr Jakub Boratynski advocated the setting up of a mechanism in order to facilitate notifications and cooperation dealing with illegal content. In addition he clarified that the focus of this dialogue should be illegal content strictly, thus excluding content that might be considered harmful or inappropriate. He added that the Commission was aware of the differences between child pornography, racism and xenophobia and terrorist-related content. Despite the synergies that could be found, the Commission did not assume that a uniform solution should necessarily apply for all.

### **3.3 Multi-stakeholder approach; best practices in the Netherlands:**

#### **3.3.1 Involving the private sector; Dutch policies**

*Mr Erik Planken*, Senior Policy Advisor, Dutch Ministry of Justice, presented an overview of illegal activities online the best practices developed in the Netherlands to fight against them. In particular, Mr Erik Planken made reference to the importance of reinforcing the capacity of police and prosecutors - good legislation, teaming up with the private sector – not only for prevention but also for enforcement and international cooperation.

As regards public private partnerships, Mr Erik Planken referred to information sharing, filtering and blocking of websites, financial barriers and clearing the internet from violent radical content. In particular, he stressed favouring prevention instead of repression, promoting information sharing between public and private sector and extending best practices from national to international level.

#### **3.3.2 General Principles on Effective Self Regulation on the Internet based on Public-Private Partnerships**

*Mr Jeroen van Vugt*, Programme Manager, Dutch National Coordinator on Counter Terrorism

- The project "Exploring the Islamist Extremist Web of Europe" identified preventive measures to fight against this type of content. The measures included cross-border cooperation, cooperation with the private sector and promotion of public private dialogue at EU level. There should be a follow-up of the project.
- Non legislative means should bridge the gap between the legal framework and efficient fight against terrorist-related content. This should include the clarification of responsibilities, the

establishment of clear procedures to deal with illegal content and reaching out to third countries.

- A general framework for ISPs and Member States with regard to the illegal use of the Internet should be created. Such framework should be based on general principles to be adopted by public and private partners. Best practices to be implemented voluntarily should follow. The framework should clarify how to act in case of illegal content and prevent illegal content as much as possible, explaining how public and private partners should work together.

*[Q&A]*

- Reaction from the representative of INHOPE, stressing the importance of the role played by hotlines in the fight against online illegal content.
- Reaction from the Interpol representative on the role of law enforcement authorities to fight against online illegal activities and explanation of practical cross-border cooperation facilitated by Interpol.
- Remark from INACH representative: It should be clear that certain types of content are illegal and therefore the discussion of general principles concerning the removal of such content is not appropriate. The Chair clarified that the speaker did not intend to challenge our common legal framework which makes the dissemination of certain content punishable. Mr van Vugt had referred as how best to prevent the dissemination of such content in practice by ensuring a smooth cooperation between law enforcement and the private sector.

**3.4 Examples for standard business conditions concerning illicit content** *[general conditions of contract]*

*Dr Oliver Maor*, Deputy Head of Division, Legal and general affairs of counter-terrorism, Federal Ministry of Interior, Germany

- The project "Exploring the Islamist Extremist Web of Europe" identified preventive measures to fight against this type of content. In particular, Germany developed a model of general conditions that might be introduced in the contracts between ISPs and their customers.
- Mainly, these conditions would protect ISPs from eventual liabilities before their clients following the removal of certain content as a consequence of a request to remove illegal or harmful content. Such protection would apply even if the content was declared legal at a later stage by a court.

- ISPs would obviously remain free to introduce conditions of this kind in their contracts. Germany offers this model/idea as possible help for ISPs that find themselves in the difficult situation of deciding whether to follow the request of removing illegal or harmful content or not, when removing such content might result in the ISP's liability before the customer.

*[Q &A]*

- Clarification from the Chair: the Commission does not target harmful content, and intends to develop public-private cooperation only against illegal activities online. In particular, controversial and extremist opinions remained covered by the right of freedom of expression, without prejudice to the editorial freedom of ISPs.
- Intervention from DG INFSO representative: The representative referred to the example of a network of hotlines against child pornography and paedophiles, which covers the whole EU. Content of suspicious websites is assessed in close cooperation between hotlines and police authorities. He underlined that a swift removal of the content avoided double victimisation and pointed out the example of Germany. He suggested that the challenge posed by hosting the content abroad (i.e. non-EU countries) could be overcome by a closer cooperation between the EU and non-EU hotlines.
- Question from the IIEA representative on how these general conditions have been received by ISPs. Mr Olivier Maor clarifies that the elaboration of the conditions is very recent and there is not enough feedback yet.
- Question from Microsoft representative on the possibility of a request from a third country or international organisation to remove certain content. Mr Olivier Maor explains that the conditions could still apply when the content is illegal under national legislation and agrees with the Chair that the content might be removed as a case of "probably illegal content".
- Remarks from the representative of the Council of Europe: Public authorities must act as guardians of the right of the freedom of expression and therefore favour public private cooperation that fights strictly illegal content. The representative of the Council of Europe referred to the Council of Europe 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime' issued in April 2008.

### **3.5 Presentation by Europol**

*Mr Nicola Dileone*, High Technology Crime Centre, Europol

- Cyber-crime perspective of Europol: information of the different types of online criminal activities, the difficulty to identify the offenders because of the borderless nature of the Internet and the anonymity it provides, and the difficulty of preventing the offences.
- Europol's response: information on the European Alert Platform which includes:

1) An Internet Crime Reporting Online System (ICROS)

2) An Analytical Work File (AWF Cyborg)

3) An Internet Forensic Expertise Forum (IFOREX)

- Relations between law enforcement and private sector: the success of an investigation is not only the success of the law enforcement. There is a social interest in preventing online illegal activities that concerns both law enforcement and private sector. This is a common interest; therefore the success of the fight against cyber-crime is the success of many partners. Therefore, there should be a common understanding about the area to work together, finding a common way to help both parties.

*[Q&A]*

- Comments from INHOPE, referring to the need for a public private partnership platform and offered its help to provide information about stakeholders in third countries.
- Europol stressed the importance of the identification of the child in cases of child pornography.

*[Afternoon session]*

### **3.6 Presentation of the study on non legislative measures to tackle terrorist related content**

*Mr Johnny Ryan, Senior Researcher, IIEA* informed about the study that the Institute of International and European Affairs will elaborate for the Commission on "Non-legislative measures to fight violent radical content". He drew the attention of the participants to the need of input in the study and therefore, asked for their cooperation.

### **3.7 Cyber criminality: the private sector perspective**

A common and exhaustive presentation of *Mr Michael Bartholomew, Director of ETNO* and *Mr Michael Rotert, President of the German ISPA and Vice-President of EuroISPA*:

- Welcomed the initiative of the Commission of promoting public-private dialogue to fight illegal activities on the Internet.
- Drew attention to the need of precaution against spam, software from unknown sources etc. Raising awareness and promoting media literacy was identified as a priority.
- Drew attention to the lack of specialised of judges and prosecutors in many cases, the lack of enough investment in training of law enforcement in cyber-criminality and the difficulties resulting from this.

- Referred to the confusion caused by different guidelines, recommendations and regulations applying to cyber-crime.
- Listed different initiatives where the private sector was involved to help law enforcement in the fight against online illegal activities i.e. the advance fee fraud coalition, the European financial coalition, the Lisbon centre for studies on cyber-crime, the 2CENTRE project.
- Clarified that, although cooperation could still improve, the main activity of the private sector was not fighting criminality.

*[Q&A]*

- The Chair clarified that:
  1. The equivalence between the Council of Europe 'Guidelines for the cooperation between law enforcement and internet service providers against cybercrime' and the EU recommendations on public-private cooperation annexed to the Council Conclusions.
  2. The project 2CENTRE was still in the process of evaluation within the Commission.
- Question from the UK representative
- The representative from Europol recognised that older generations of law enforcement were more easily affected by the problem of insufficient knowledge on cyber-crime and explained all efforts deployed to improve the training of law enforcement, in particular, by means of recognition (degree) of the specialised knowledge following the training.

**4. Conclusions: the way forward**

*Mr Martin Schieffer* presented the Commission's view on the follow-up of the conference. The approach was supported by all participants. In particular, participants fully supported the continuation of this public private dialogue and the role of the Commission to facilitate it. See below the "way forward" as presented by the Commission at the conference, complemented with the suggestions of participants:

WAY FORWARD

- Meet regularly in this public private platform to reinforce dialogue in the fight against illegal content between law enforcement authorities and private operators at EU level. Future meetings should include thematic conferences in addition to general ones.
- More specifically, the objectives of the PPP platform are:
  - (1) raise awareness and sharing information about ongoing projects and initiatives related to the fight against online illegal activities at national and European level.

(2) promote an open and constructive discussion on questions related to the fight against online illegal activities in order to develop a voluntary agreement model for co-operation between law enforcement agencies and private operators (as mandated by the Council Conclusions of 27 November 2008 on a concerted work strategy and practical measures against cyber-crime)..In particular, the Commission should present a first draft of the "European agreement model" for the next conference.

- Further involvement of the private sector in this public private platform – especially private companies.

### **5. Next steps**

The strong support for the continuation of the public private dialogue to fight online illegal activities has encouraged the Commission to envisage a follow-up conference in spring 2010, where a first draft of a set of principles on public private cooperation to fight online illegal activities could be presented.