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

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

[redacted], 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.

[redacted] 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.

[redacted] 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

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. 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

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, 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, 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

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. 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]*

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. 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. 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

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

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 *Director of ETNO* and *Mr 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 were 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

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.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

Directorate F : Security
Unit F1: Fight against terrorism
Unit F2: Fight against organised crime

Brussels, 4 June 2010

2nd CONFERENCE ON A PUBLIC PRIVATE DIALOGUE TO FIGHT ONLINE ILLEGAL ACTIVITIES

held in Brussels on 21 May 2010

SUMMARY

Meeting in a nutshell

The 2nd conference on public-private dialogue to fight online illegal activities, organised by the European Commission, Directorate-General Justice, Freedom and Security took place on 21 May 2010 and was attended by about 50 industry, law enforcement, justice and NGO representatives. The meeting saw presentations on practices in Member States and discussions on a previously circulated draft recommendation on notice and takedown procedures for illegal online content related to child pornography, terrorism and racism/xenophobia.

Details

1.

Considering some feedback received in advance of the conference, the Commission Unit F.2), in opening the meeting, reiterated the scope of the initiative which aims at a clarification of notice and take down procedures. It was pointed out that as such, the initiative aims at

- developing a voluntary agreement model (European agreement model) for cooperation between LE and private operators (c.f. Council Conclusions 27 Nov 2008)
- rendering notice and take down of illegal internet content more efficient
- setting up a list of contact points to facilitate contact between private and public stakeholders

Furthermore, the Commission clarified that the term "recommendations" was not to be understood as expressed in art. 288 TFEU and that any guidelines that would be the outcome of the process would be accepted on voluntary basis.

2.

The Spanish Presidency [redacted] (Policia Nacional) welcomed the dialogue, stating that dealing with all three content types was important.

3.

A series of presentations followed (from the International Association of Internet Hotlines/INHOPE / ECO, [redacted] Telefonica S.A., [redacted] and the Dutch National Counter Terrorism Coordinator [redacted], focussing on different ways of dealing with illegal online content. [redacted] explained that take-down of sites/material worked very fast (minutes/hours within the EU, non-EU 5-14 days) and that the hotline channel was much faster than the Interpol channel.

[redacted] rom Telefonica pointed out their strict notice & take down procedures applicable to child sexual abuse images. In Spain, established communication channels with the judiciary allow for response times between 30min and four hours. [redacted]

[redacted] from the Dutch National Counter Terrorism Coordinator's office spoke about a code of conduct for illegal content, elaborated in NL. Such code should be internationalised, and expanded to illegal use of the Internet, not only illegal content. NL, UK, DE, BE will submit project proposal to help this process.

A presentation on the need for a comprehensive public-private contact point list followed [redacted] The need for such a list has been raised since 2008, mainly by operational staff, as current formal assistance channels have proved too slow. Current contact point lists are too limited (for LE only) or too informal. The Commission [redacted] presented the CICILE system (Contact Initiative against Cybercrime for Industry and Law Enforcement - currently only as a 'test'), based on the SINAPSE web-platform and invited the participants to register and test the system.

4.

The remaining part of the meeting was given to a thorough discussion of the draft recommendations. Some industry representatives suggested that different recommendations should be adopted for online content relating to each crime area, i.e. child pornography, terrorism and hate crimes. The participants from German and Dutch ministries [redacted] stressed the need for industry to come forward with some voluntary steps as opposed to notification and action requirements that are exclusively coded in (criminal) law.

Conclusions

The meeting concluded on the usefulness of using CICILE/SINAPSE for the establishment of a contact point network. As for the draft recommendations, participants were invited to send in their written comments until 2 July 2010. A follow-up conference will take place in September / October 2010.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A : Internal Security
Unit A2 : **Fight against Organised Crime**

First meeting of the Sub-group on Cybercrime statistics
Brussels, 1 July 2010

AGENDA

	10:30 – 11:00	***Arrival and Registration***
	11:00 – 11:05	Adoption of the agenda
1	11:05 – 11:10	[redacted] Unit F2: Welcome
2	11:10 – 11:25	[redacted] Unit F2: Why do we need statistical data on cybercrime? - Introduction to the sub-group on data on cybercrime
3	11:25 – 11:40	EUROSTAT: Process for data collection (tbc)
4	11:40– 13:00	Discussion of mandate of sub-group on cybercrime statistics Tour de table – identification of needs for cybercrime statistics and overview on available statistics at national level
	13:00 – 14:30	***Lunch break***
5	14:30 – 15:30	Discussion of definitions and indicators for cybercrime
6	15:45 – 16:30	Summing-up of discussion
7	16:30 – 17:00	Follow-up action and future meetings / AOB

VENUE : DG HOME AFFAIRS – Salle Fortescue, ground floor
Rue du Luxembourg 46
B-1049 Brussels

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A : Internal Security
Unit A.2: Fight against organised crime

Brussels, 2 July 2010

MINUTES OF THE 1st SUB-GROUP MEETING ON CYBERCRIME STATISTICS

held in Brussels on 1 July 2010

Meeting in a nutshell

The meeting brought together representatives from the EU Member States' law enforcement (LE) / criminal justice authorities, Europol, the private sector (Microsoft and Symantec), the Council of Europe (CoE) and the Commission (COM). A thorough discussion of the undisputed need for public cybercrime statistics and the difficulties inherent in data collection for this crime area, such as, inter alia, diverse methods of statistical recording in the Member States or the difficulties of agreeing on an all-encompassing definition of cybercrime took place. It was agreed to start with the offences contained in the existing Council Framework Decision[1] (and future Directive) on attacks against information systems, to expand the list of offences to cover the complete list of the CoE Convention on cybercrime (ETS no. 185, so-called Budapest convention[2]) and finally explore possibilities to include also computer-assisted crimes such as online fraud and child pornography.

Details

Reasons for this meeting

The participants were welcomed by [redacted] Head of Unit "Fight against organised crime" (A.2) in COM DG HOME AFFAIRS (HOME). [redacted] COM DG HOME A.2, subsequently explained why this sub-group had been set up (cybercrime one of the fastest growing crime areas, no reliable data at EU level, EU action plan to measure crime and criminal justice 2006/2010). Furthermore, he presented the need for cybercrime statistics: to enable an evaluation of the real extent and magnitude of the problem at EU level, to detect gaps in existing legislation and to put LE and policy makers in a better position to take informed choices on resource allocation and policy options for the prevention and the fight against cybercrime.

The role of Eurostat

[redacted] DG ESTAT, presented the role of Eurostat in the process of data collection on crime, emphasising the importance of having legislation in place for collecting data on

[1] Council Framework Decision, 2005/222/JHA, OJ L 67/67, 16 March 2005, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:EN:PDF

[2] Council of Europe Convention on Cybercrime, signed in Budapest 23. November 2001, http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

specific crime types. Consistency between the indicators to be collected and the requirements identified in the legislation as well as the need for a concise list of indicators and full reporting of metadata were covered. In the next meeting of the working group on crime statistics, February 2011, COM will present for discussion the indicators identified by this sub-group of experts.

New directive against attacks on information systems

explained to participants the new requirements on statistical reporting foreseen in the Draft Directive against attacks on information systems. In the old Council Framework Decision there is no obligation for collecting statistics. The new proposal specifically mentions the information that is to be collected, such as the number of offences, the number of investigations, the number of offenders and the number of convictions. Problems inherent in crime reporting, such as dark field and discrepancy between initial police statistics and conviction statistics were covered. An option of how to arrive at national statistical figures was discussed, i.e. taking an offence included in valid EU legislation, identifying the corresponding article/statute in national penal law and analysing what statistics exist in relevance to a violation of the specific national law.

Discussion

Constructive discussions on indicators for cybercrime and the approach to commence with data collection on some cybercrimes followed and took up the remaining time of the meeting. from Symantec mentioned the annual Symantec Global Internet Security Threat Report[3]. Data from this report often is cited also by public authorities in absence of reliable LE data. According to Symantec covers 200 million IT systems in roughly 200 countries, identifying 3000 new viruses in 2009. In the annual report they provide info only on the attacks they have stopped. No country breakdown is provided. According to their data circa 100 attacks are committed every second over the internet. However, the Symantec report only describes part of the picture as obviously not all victims of viruses or intrusion are their customers. Additionally, the rationale behind the collection and publishing of their data is different from LE considerations.

As Home Office, pointed out, the UK definition of cybercrime is different and it is considered to include computer-facilitated crimes. The German participants from the Bundeskriminalamt, explained that while the police crime statistics contain data on computer crime, a split-up according to specific offences might be difficult to achieve as the crime recording police officer uses key numbers (Schlüsselzahlen) to code crimes by crime area. The Estonian colleague, from the Ministry of Justice, stated that there is a distinction between crimes against computer systems (so-called CIA offences) and crimes committed via computer systems (computer-facilitated crimes). According to from the Italian Polizia postale it will be very difficult to come up with a common definition and it would be better to rely on a more descriptive approach focusing on offences. Europol, also made the case to focus on crime areas.

The types of cybercrime addressed in COM's proposed Directive on attacks against information systems is a subset of the crimes included in the CoE Budapest convention from the CoE indicated that the CoE (Budapest) convention on cybercrime had been ratified by 20-22 EU MSs and that the relevant articles have been introduced in the national criminal law.

The differences in the reporting systems were identified as a major problem, as existing statistical reporting does not exactly correspond to the articles of the criminal law (e.g. case

[3] Volume XI published April 2010, see http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

of UK). Changing national reporting systems could entail financial implications. COM clarified that it would not prescribe Member States how the national data collection plan should look like.

Two directions were discussed:

- To start with minimum requirements (starting with the indicators identified in the Directive and/or Budapest convention) and build gradually a more complete collection
- To take into consideration threat assessments, studies, other sources of information regarding victims, NGOs and perceptions and produce a general assessment of the situation.

The second approach, although useful, appears not feasible and would definitely not reflect the role of the COM. Threat assessments should be produced by Europol, as in the case of the OCTA. [redacted] from Microsoft underlined the importance of include the victim perspective in the process.

At the end of the meeting, the **following way forward** was agreed:

A phased approach to start the collection of statistical data on cybercrime will be taken. To begin with, the offences included in the new draft EU Directive which are a subset of CoE (Budapest) convention on cybercrime should be reported.

In a second step, further offences as listed in the CoE convention and computer-assisted crime, such as child pornography and online fraud, but possibly also cyber terrorism or terrorism propaganda, will be included.

Member States will have to nominate a single contact point in each MS for the collection and transmission of the relevant information. While it would be desirable to also obtain information on the damage caused by offences or the number of personnel resources dedicated to a specific investigation, the essential data on case numbers, offenders, convictions will be the initial focus.

Conclusions

1. COM will draft a document proposing a list of indicators and outlining the required information to start data collection on cybercrime for the members of this sub-group to check and revise (mid-October 2010).

2. Members of this group will verify, at national level, the availability and feasibility of such data, coordinating with all agencies that might hold relevant information. Members will also take care to identify a single contact point in their country dealing with all issues around cybercrime statistics.

3. A second meeting of this sub-group will take place in November 2010 in Brussels, a precise date will be communicated well in advance. At this meeting, a final decision on the indicators and the data to be collected will be taken.

4. COM will present the results to the expert group on policy needs that meets in December 2010.

5. Subject to agreement, COM will include cybercrime statistics in the new Action plan from crime statistics, covering the period from 2011 to 2015.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A : Internal Security
Unit A1 : Crisis management and fight against terrorism
Unit A2 : Fight against organised crime

Brussels, 2 February 2011

3RD CONFERENCE ON PUBLIC PRIVATE DIALOGUE TO FIGHT ONLINE ILLEGAL ACTIVITIES

held in Brussels on 15 December 2010

Summary Report

Chair: A.2 (a.m.) and A.1 (p.m.)
European Commission, DG Home Affairs

Meeting in a nutshell

The 3rd conference on public-private dialogue to fight online illegal activities, organised by the European Commission, Directorate General Home Affairs, gathered nearly 60 representatives of Internet service providers and industry (ISPs), law enforcement authorities (LEAs) and NGOs. The meeting focussed on discussing the revised Draft Recommendations to fight online illegal activities and possible ways forward.

Details

Opening

In the opening remarks the Commission provided a brief summary of the public-private dialogue, and emphasised the voluntary and bottom-up nature of the exercise, which is an opportunity to deal with illegal content online through a self-regulatory measure among the relevant actors. The Commission reiterated the mandate given by the Council Conclusions of 27 November 2008 and referred to the Internal Security Strategy, which aims at developing voluntary recommendations in 2011.

The representative of the Belgian EU Presidency (Federal Computer Crime Unit, FCCU) expressed its support to the initiative and stressed that the public-private dialogue is necessary in order to tackle the illegal content more efficiently. He acknowledged that although the text of Draft Recommendations is a good starting point, it is still limited to the worst cases while the spectrum of illegal content and activities online is wider.

Finally, the Commission briefed the participants on the main findings of the consultation process and outlined main changes introduced to the Draft Recommendations, and opened the floor for the discussion.

Discussion on the draft recommendations

During the discussion, EuroISPA (European Association of European Internet Service Providers), ETNO (European Telecommunications Network Operators' Association) and EDRi (European Digital Rights) voiced their criticism about the lack of a problem description underpinned by solid and quantifiable data. Other concerns referred to the need to tackle each and every type of illegal content separately since a single set of recommendations may not be the most suitable. The ISPs (KPN) asked also for clarifying the scope of the Draft Recommendations since some provisions could be interpreted as referring to filtering and blocking.

In addition, EuroISPA and EDRi questioned the operational capacities of LEAs to process and effectively deal with reports of illegal online content. Referring to the role and use of terms of service, the ISPs (Yahoo!) stressed that this is above all a tool to regulate relationships with consumers, and it should not be seen and used as a law enforcement mechanism. Yahoo! underlined also the need for clarifying the issue of jurisdiction.

Furthermore, KPN and Yahoo! pointed out at the need to explain the status of notifications especially in cases where the legality of a notified content is doubtful. In such cases, the ISPs would need an authoritative decision (legal order).

Finally, Microsoft/Signal Spam pointed out that the term "recommendations" may be misleading, and suggested to replace it with more neutral wording.

The Commission clarified that its position is not to impose a solution on the stakeholders but to facilitate the process and encouraged Member States' LEAs to take the floor and address the concerns expressed by the ISPs. The Commission underlined also that a number of problems (rationale for action) could already be identified, such as low awareness among citizens about possibilities to report illegal content, the lack of clarity in the relationship between stakeholders, and continuing availability of illegal content online. These items should be discussed and elaborated further.

In addition, INHOPE representatives stated that it would be possible to provide data on the nature and extend of the problems especially with regard to child-abuse material. The Commission (DG INFSO) highlighted a discrepancy in effectiveness of notice and take down procedures for child-abuse content ranging from 30 minutes to 3 months, which necessitates further analysis. Belgium (FCCU) played down the importance of statistical significance of different types of illegal content and stressed that any criminal incident, no matter how numerous, should be pursued.

Furthermore, the Commission admitted that while the terms of service should not be used as a law enforcement tool, the ISPs use discretionary, catch-all provisions, which enable them to take down very wide range of online content.

The Commission considered also the necessity to distinguish between hosting and access providers in order to clearly exclude blocking and filtering from the scope of the Draft Recommendations. Symantec and Belgium (FCCU) both referred to the need to take into account various means and technologies to distribute illegal content.

Germany (Ministry of Interior) pointed out that tackling all types of illegal content with one, general set of recommendations may not be the ideal solution.

Referring to the issue of jurisdiction, the Commission and Belgium (FCCU) clarified that both the ISPs and Hotlines should apply their national laws to process the reports and notifications.

At the request of the UK (Office of Fair Trading), the Commission clarified that involvement of the Domain Names Providers in the public-private dialogue is to be considered.

The Netherlands (National Counter Terrorism Coordinator's Office) offered to share the Dutch experience and proposed to form a smaller working group, which would identify main problems and propose appropriate solutions. This idea was echoed by Microsoft.

Safer Internet program – information point

The Commission (DG INFSO) provided a brief update on the Safer Internet program and underlined that the Hotlines should be the first step for receiving the reporting from citizens. Apart from the varying response times to take illegal content down, the Commission reported that the resources allocated to fight child-abuse content differ to a large extent across the Member States.

Representatives of INHOPE echoed the Commission and underlined the need for closer cooperation between the Hotlines and LEAs.

Examples of public-private models – Signal Spam

The Signal Spam initiative was presented by various stakeholders representing public and private sector (Microsoft, SFR, Orange, Return Path - EMEA, Association des Fournisseurs d'accès et de Services Internet, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication, Commission Nationale Informatique et Libertés, L'Agence nationale de la sécurité des systèmes d'information).

The presenters pointed out the importance of awareness raising campaigns since the initiative is based on the users' reports. A number of advantages were highlighted such as the automation of the reports' processing and the added value the initiative brings to the public and private stakeholders e.g. increased efficiency of LEAs and data protection agencies' proceedings against the spammers, increased client protection and faster identification and analysis of botnets.

Finally, Signal Spam gradually expands abroad as a role model initiative in cooperation with partners from the US, Canada, United Kingdom, the Netherlands, Switzerland and Japan.

General discussion

During the discussion Microsoft underlined that the public-private cooperation model of Signal Spam is transferable to other areas and could be used to address the issue of illegal

online content. Microsoft stressed however that the ISP industry's commitment depends on the identification of their commercial interest and the added value.

Conclusions

The Commission concluded the conference and proposed to further investigate of the following issues:

- the main problems;
- scope of the exercise and
- interests and added value for the ISPs.

The next conference on public-private dialogue to fight online illegal activities is to take place during the course of 2011.

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A : Internal Security
Unit A.2: Fight against organised crime

Brussels, 14 February 2011

MINUTES OF THE 2nd SUB-GROUP MEETING ON CYBERCRIME STATISTICS

held in Brussels on 25 January 2011

Meeting in a nutshell

Follow-up to the first meeting in July 2010, attended by law enforcement representatives from EE, SE, BE, DE, FR and MT. Symantec and Microsoft, Europol, ESTAT and Council of Europe were also represented.

Conclusions on four indicators to start the collection of basic statistical data on cybercrime were reached on the basis of a draft list of indicators prepared and circulated by the Commission (COM) ahead of the meeting.

COM will write the exact guidelines for the data collection for the years 2007, 2008 and 2009 by March 2011 and distribute them to the participants. Afterwards, distribution to Member State contact points is foreseen. The Eurostat Working Group on Statistics will discuss the proposal in May 2011. First data collection could start in 2012.

Details

The participants were welcomed by [redacted] Head of Unit "Fight against organised crime" (A.2) in COM DG HOME. [redacted] COM DG HOME A.2, subsequently recapitulated the outcome of the first meeting, i.e. agreement that COM had agreed to draft a document proposing a list of indicators and that Member States were to verify at national level the availability of data. A draft list of indicators – based on art. 3 to 8 of the Draft Directive (COM(2010)517 final) on attacks against information systems - itself largely based on the Council of Europe Budapest Convention against cybercrime – had been circulated before the meeting. According to this list, the following data should be collected for each article (3 to 8):

number of offences – number of investigations – number of persons prosecuted – number of persons convicted.

If possible, the ***actual damage caused***, should be recorded and transmitted by each Member States for a given reporting period.

Should a Member State have problems providing such a detailed view on cybercrime data, at least a breakdown for aggregated confidentiality, integrity and availability offenses (CIA crimes) on the one hand and computer-related crimes (such as online fraud etc.) on the other hand should be provided, thus classifying all possible cybercrimes in those two data "containers". A round-table discussion followed.

During the meeting, participants were asked to indicate if their country was able to provide the required data dimensions.

FR, BE, EE, MT and DE indicated that a detailed split-up of data would be feasible. SE stated that there was one "container" for all computer intrusion offences. MT remarked that possible difficulties as to the data on convictions existed, similarly to DE, where data concerning the number of prosecuted and convicted persons would have to be delivered by the Ministry of Justice.

The Europol delegate gave a short presentation on the Europol Internet Crime Reporting Online System (ICROS), indicating how this system is related to the Europol Information System (EIS) and relevant Analytical Workfiles.

The delegate from the Council of Europe invited the COM to map all existing cybercrime data in the EU.

Conclusions

1.

COM will finalise a document detailing the required information to start statistic data collection on cybercrime for the members of this sub-group. This document will contain exact guidelines such as reference periods (time of recording) and will be circulated in March 2011.

2.

Subsequently, the document will be send out to all EU Member States.

3.

The indicators will be introduced at the Eurostat Working Group meeting in May 2011.

4.

Subject to agreement, COM will include cybercrime statistics in the new Action plan for crime statistics, covering the period from 2011 until 2015.

5.

First data collection could start in 2012 for the reporting periods 2007, 2008 and 2009.

The Hague, 22nd March 2012

EDOC # 594857-v8

DRAFT AGENDA
5th Meeting of the European Union Cybercrime Task Force (EUCTF)

Date(s)	**27.03.2012** **28.03.2012**	**Start: 08:30** **09:00**	**End: 18:00** **17:30**
Place	**European Commission**		
Board Members	[redacted] Belgium – Chairman (Vacant) – Vice Chairman [redacted] Ireland – Member European Commission and Europol - Members		
Participants	**EU MS Cybercrime Units, European Commission, Eurojust, non EU law enforcement MS, CEPOL**		

Item/ Topic or time	Subject	Responsible/ Announced by	Document Reference or Place
	27th March – Closed Session **[only for EU Member States (Law Enforcement), European Commission, CEPOL and Eurojust]**		Hotel Leopold, Meeting Room 'Elisabeth' Rue Luxembourg 35, Brussels
08:30 – 09:00	Arrival and Registration		
09:00 – 09:45	Welcome Mutual Introduction	[redacted] Head of Unit, A2 DG Home Affairs, European Commission [redacted] Chairman	

	Presentation EUCTF Adoption of the Agenda and minutes of the last meeting	EUCTF All Head of Cybercrime Unit Ireland Chairman EUCTF	
09:45 – 11:15	European Cybercrime Centre: Update on the latest developments Discussion: • How can European Cybercrime Centre help to coordinate our actions in fighting cyber attacks in the EU(strategic goal 4 EMPACT) • Round table discussion	European Commission Head Cybercrime Unit Ireland All	
	Coffee Break		
11:30 – 12:15	Strategic Goals to combat cybercrime outside EU	European External Action Service	
12:15 – 13:00	Implementation EU Policy cycle for organised and serious international crime Operational Action Points related to EU Cyber Crime priority: • Update on the latest developments • Joint Investigation teams	– Head of Cybercrime Unit Romania (Driver) – Europol and – Liaison Officer at Europol	Reference texts - Council document 14452/2/11 17.10.2011 - Council document 17809/11 30.11.2011

	• Round table – update from EU MS • Discussion and way forward	All	
13:00 – 14:00	**Lunch Break**		
14:00 – 16:00	SUBGROUPS: Implementation of Operational Action Plan and feedback (the subgroups are expected to report to plenary)	All	Rooms to be announced
	Coffee Break (during subgroups activities)		
16:00 – 16:30	Reports from the Subgroups Way Forward	All	
16:30 – 17:15	Relationship with Non – EU Member States Overview and National Strategy Round Table discussion	– HTCU Switzerland All	
17:15 – 17:45	Election of Board offices: Vice-Chairman and Europol Permanent Member	All	
17:45	Wrap Up – Closing of day one	All	
19:00	*Dinner*		

Item/ Topic or time	Subject	Responsible/ Announced by	Document Reference or Place
	28th March – Open Session		
09:00 – 09:15	Welcome	Director, Internal Security DG Home Affairs European Commission	Hotel Renaissance, Meeting room 'Copenhagen', Rue du Parnasse 19, Brussels
09:15 – 10:45	Legal Aspects - updates on: • Europol's data protection rules for the fight against cyber crime	– Head of Data Protection Office Europol	

	• Data Retention – Latest Developments	European Commission	
	Coffee Break		
11:00 – 12:00	Legal Aspects (cont.) - updates on: • Directive on Attacks against Network Systems • ICT Policy Support Programme	Member of European Parliament To be announced	
12:00 – 12:45	Cybercrime Centre in Singapore	– Acting Assistant Director, R&D IGCI, Interpol	
	Lunch		
14:00 – 15:00	EU Computer Emergency Response Team	Head of CERT EU Pre-Configuration Team	
15:00 – 16:00	Commission Communication on the European Cybercrime Centre - Ways toward its implementation - the role of Europol	Cecilia Malmstroem - Commissioner Rob Wainwright - Director of Europol Chairman EUCTF	
16:00 – 16:30	Q & A with the Commissioner / the Director of Europol	All	
	Coffee Break		
16:45 – 17:15	The European Cybercrime Centre - Implications for EUCTF	Chair/ Commission	
17:15	Wrap up, date of next meeting and close of meeting	Chair All	

EUROPEAN COMMISSION
DIRECTORATE-GENERAL HOME AFFAIRS

Directorate A : Internal Security
Unit A.2: Fight against organised crime

Brussels, 29 March 2012

Meeting report
Fifth meeting of the European Union Cybercrime Task Force
Brussels, 27 / 28 March 2012

Purpose of the meeting

The **Fifth** meeting of the **European Union Cybercrime Task Force** (EUCTF) was divided in a closed law-enforcement session on 27 March and an open session on 28 March which also included representatives from industry, other institutions and agencies.

Total attendance 27 March: 47 participants, 28 March: 67 participants.

Main points covered

The EUCTF brings together the Heads of the Member States' National Cybercrime / High Tech Crime Units and was founded in 2010. For the first time – on the occasion of the adoption of the Commission Communication on a European Cybercrime Centre (COM (2012) 140 final) on 28 March 2012 – the meeting was organised in Brussels and paid for by the Commission.

While the Communication and planning of the European Cybercrime Centre played a prominent role in the meeting, especially with speeches by Commissioner Malmström and Europol Director Wainwright on the second day, other important points were covered.

Those included further discussion on the operational action points as agreed in November 2011 for implementation under the EU policy cycle for organised and serious international crime. Here, RO as driver country was introduced and subgroups worked to advance on the fight against botnets (lead BE), a definition on serious cybercrime (lead NL) and cybercrime reporting, including ICROS (Internet Crime Reporting Online System-lead Europol).

The second day saw presentations on Europol's data protection regime (Europol) and on the state-of-play of data retention (Commission). Improvements to art. 25 Europol Council Decision to facilitate exchanges of information with the private sector (but also third country partners) should be earmarked under the general revision of Europol's current legal framework. MS and Europol should already now identify examples to argue for a more permissive wording. Examples illustrating the need for longer data retention periods are also urgently needed to make the case of justified law enforcement needs.

MEP [redacted] informed on the state-of-play of discussion on the Directive on attacks against information systems (COM(2010)517 final) in the Parliament. An orientation vote took place in EP's LIBE committee on 27 March with 50:1 in favour of the negotiated text. MEP [redacted] argued also positively for the ECC (budget) and underlined the need for a comprehensive cyber strategy of the Union as an overarching product of EEAS and all relevant Commission services.

Interpol presented an outlined of its envisaged cybercrime centre (global complex), scheduled to commence operations in Singapore in 2014. A close cooperation with the European Cybercrime Centre is desirable.

The Head of the EU-CERT pre-configuration team explained the mandate and concrete examples of the work of his team. He pointed especially to the fact that in many cases of cyber attacks, of malware infections or cyber "extortion" cases no reporting to law enforcement authorities occurs, pledging the audience to reflect on remedies.

EUCTF Board composition

The respective Heads of the National Cybercrime Units from Ireland and Latvia were elected to the positions of EUCTF vice-chair (IE) and Board Member (LV). For Europol, Assistant Director [redacted] will from now on represent the agency on the EUCTF board.

Next meeting

Next meeting of the EUCTF will be held in October 2012 at Europol (exact dates to be confirmed).

(signed)

Distribution (via email)

- DG HOME: [redacted]
- EU-CERT pre-configuration team: [redacted]
- EEAS: [redacted]
- Council: [redacted]
- European Parliament: [redacted]

► **To be distributed at the next meeting of the ISG on cyber-security and cybercrime**

All relevant presentations, attendance lists etc. available from DG HOME A.2

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

Directorate F : Security
Unit F3 : Police co-operation and access to information

Brussels,

MEETING REPORT

Subject: Meeting between EU Commission/ CAB BARROT – DG JLS and Microsoft
Date: Tuesday 16 June 2009

Microsoft representatives called on Cabinet Barrot to exchange view on common issues and interests. Among the issues mentioned, the most salient were the following:

- **Putting the citizen in the centre**. Microsoft, as platform provider, is developing alone, with governments, NGOs and other private actors applications to empower individuals, giving them control over their own data, e.g. ability to selectively release information from their health file to certain doctors), to enhance trust in the private market (banking, e-commerce), or protect children (when participating in social website, protection against predators); this calls for the development of a comprehensive cyber security policy. Microsoft is also in favour of individuals being able to access data that industry gathers about them (e.g. energy companies are establishing individuals' consumption profiles that are hitherto not available to consumers, but could help them to make better choices).
- Huge need for **awareness raising** endeavours: to empower individuals, but also to make them aware of the risks of their online behaviour. This calls for development of education skills. The development of "trustworthy computing" does require knowledge, a security policy, and guidelines on jurisdiction issues.
- **Cloud computing** (the web = the computer) creates new issues and opportunities. Microsoft's interest is in offering software to access the cloud and use the potential. Developments should lead to an enabling environment, "individuals' choice" being the guiding concept. Microsoft stated that developments take place at such speed it is ineffective to legislate. Governments have to make an effort to "keep up" with developments in dialogue with industry.
- **Required regulatory environment for online economy**. A global approach is required that combines government-to-government action and private sector self-regulation, inter alia to address the challenges posed by cyber crime (money laundering, child pornography,

Intellectual property infringements), to offer security of online activity, of freedom of expression, and monitored social websites.
KJ mentioned the "loi Hadopi", which poses the question of enforceability and need for transnational cooperation between governments: an growing number of data will be available outside of the jurisdiction. Cloud computing exacerbates this trend.

US industry and government relations. This block should entail strong personal data protection, which is entirely supported by Microsoft. US government is expected to present in 2010 federal data protection legislation in the private sector. Cyber security is part of the package.
Asked why this legislation is now possible, Microsoft said that new administration puts focus on people's issues, and civil rights groups are increasingly concerned about the enormous quantities of data that have been gathered. Also the explosion of social websites calls for a horizontally structured protection as opposed to the US sectoral approach that existed before. Microsoft acknowledged that the constant focus by EU on data protection has contributed to the change of opinion.

- **Unification of breach notifications.** Microsoft reports that industry is affected by diverging interpretation of the regulatory environment in Member States (intellectual property laws, Data Retention, e-Privacy and E-Commerce); guidelines for software developers would be welcomed. Issues regarding jurisdictions should be addressed in a government to government dialogue.
- **Industry is calling for roles**: it wants to joint forces with governments to provide new services. A large part of the Obama economic stimulus package is about rolling out those new services (e.g. smart grid: electricity companies adjusting parameters of their grid according to needs, patient controlled health records, learning and school services).

[signed]