COUNCIL OF THE EUROPEAN UNION

Brussels, 8 March 2010

5957/1/10 REV 1

LIMITE

CRIMORG 22
ENFOPOL 32

NOTE

from:	Presidency
to:	Multidisciplinary Group on Organised Crime (MDG)
Subject:	Draft Council Conclusions on an Action Plan to implement the Concerted Strategy to combat cybercrime

Cybercrime is borderless by nature. For measures to combat cybercrime to be effective, adequate cross- border provisions are needed and the international cooperation and mutual assistance in law enforcement within Europe and between the EU and third countries needs to be substantially enhanced.

In the recent years, several Council Conclusions and initiatives have been agreed upon to define a concerted strategy to fight against cybercrime.

The purpose of this strategy is to cope with cybercrime effectively and in a way appropriate to the multiple crimes committed by means of electronic media: child pornography, sexual violence, terrorist activities, attacks on electronic networks, fraud, identity theft, etc.

As a follow-up to the Netherlands initiative to go forward with concrete actions to be taken to implement these Council Conclusions and the Commission Communication on cybercrime, the Presidency has submitted a discussion paper to Member States' delegations in order to consider and discuss the next steps to be taken, examining which of the alternatives proposed best defines the general guidelines which will serve as a basis for implementing the European Union anti-cybercrime strategy.

As a result of the discussion held during the last MDG meeting and the written contributions received so far, delegations will find in the Annex the draft Council Conclusions on an Action Plan to implement the Concerted Strategy to combat cybercrime.

ANNEX

COUNCIL CONCLUSIONS

of 2010

concerning an Action Plan to implement the Concerted Strategy to combat cybercrime

THE COUNCIL, TAKING INTO ACCOUNT:

1. The Council of Europe Convention on cyber crime, 2001.

2. The relevance given in the Stockholm Programme to the protection of the use of new technologies and the protection of vulnerable people , and the modern challenges that have emerged in the form of cybercrime as criminal groups have taken effectively advantage of technologies;

3. The need to ensure a very high level of network security and faster reaction in the event of cyber disruptions or cyber attacks by means of ad hoc European Union policies and legislation in accordance with Stockholm Programme's provisions for cybercrime;

4. The Council Conclusions on a working strategy and concrete measures against cybercrime adopted on 27 November 2008[1] inviting the Member States and the Commission to introduce measures based on case studies, taking particular account of technological developments, so as to make ready tools for operational use in the short and medium term;

5. The Council Conclusions adopted on 24 October 2008 on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet[2];

[1] 15569/08 ENFOPOL 224 CRIMORG 190.
[2] 14071/08 ENFOPOL 187 CRIMORG 162.

6. The Council Conclusions on the establishment of and contributions to the European Financial Coalition and national coalitions against child pornography on the Internet adopted on 23 October 2009[1];

7. The European Council calling on Member States, as laid down in the Stockholm Programme, to give their full support to the national alert platforms in charge of the fight against cybercrime and emphasizes the need for cooperation with countries outside the European Union, and also the invitation of the Council to:
   - the Commission to take measures for enhancing/improving public private partnerships,
   - and Europol to step up strategic analysis on cyber crime.

HEREBY

Considers that is of a paramount importance to develop an Action Plan against cybercrime which would specify how the main points of the Concerted Strategy to combat cyber crime should be implemented, including

in the short term,

- ☒ the acquisition of a better knowledge of perpetrators and modus operandi, in order to have real idea of the scale of the problem and the way it constantly evolves because of its heterogeneous nature, such as crime related to the invasion of privacy, financial crime, unauthorized access and sabotage, crime against intellectual property, attacks on networks and systems, usurpation of identity and deception, child pornography and spam and trafficking in illicit substances,
- ☒ the consolidation, and then, the revision and if necessary the updating of the functions assigned to Europol's European Cybercrime Platform (ECCP), in order to boost its training activity for investigators and to exchange information and analysis.

[1] 11456/2/09 REV 2 CRIMORG 106 EF 98.

- the adoption of measures supported under the Safer Internet Programme 2009-2013, to promote partnerships with the private sector and the financial sector in order to disrupt the money transfers related to websites with child pornography[1],
- the continuity of the on-going activities and initiatives in this field such as CIRCAMP[2] project to develop a filtering system against child sexual abuse contents; the Europol Working Group on Monitoring of Internet Communication and the inventory of good practices to investigate commercial websites containing child abuse images made by European Financial Coalition (EFC) in connection with the active involvement of EUROJUST.
- To promote the use of joint investigation and enquiry teams

In the medium term, to make progress with the following actions:

- To set up and raise the standards of specialization of the police, judges, prosecutors and forensic staff to an appropriate level to carry out the technological investigations, especially as regards the establishment of a permanent cyber training platform,
- To assess the situation regarding the fight against the cybercrime in the European Union and the Member States, in order to improve a better understanding of the trends and developments in cybercrime, to make the relevant proposals for improvement and assisting the Commission and the Council in the elaboration of recommendations or rules to fight cybercrime,
- (...)
- To homogenize the different networks 24/7, eliminating possible duplications (G8 and INTERPOL),

[1] The term "child pornography" was used during the Swedish Presidency.

[2] The overall aim of this network is to promote an organized and extensive cross-border exchange of best practice between law enforcement agencies in the fight against production, online distribution and access to child sexual abuse material.

- To promote relationships with European Agencies (EMSI, CEPOL, EUROJUST, EUROPOL, ENISA, etc.), international bodies (INTERPOL, ONU, etc.) or third countries on new technology subjects, in order to improve a better understanding of the trends and modus operandi of this crime,
- To gather and update the best practices on technological investigation techniques in the police, judicial and forensic authorities and to evaluate and strengthen the use of computer investigation tools to be used by police officers, judicial authorities and forensic staff throughout Europe; in cooperation with the agencies established in this area such as INTERPOL, IACIS[1], or other similar private and public organizations,
- To promote and boost activities to prevent cybercrime by promoting best practices in the use of the networks, using cyber-patrols, integrating the volunteers, setting up black lists of toxic products and their producers and publicising assistance points to victims or consumers (minors), taking into account the relevant parts of the Conclusions from the 2009 European Crime Prevention Network Best Practice Conference and other forums related, and
- To set up a documentation pool related to cybercrime, to which all the actors involved have access, which could serve as a permanent relationship body with users' and victims' organizations and the private sector[2],

[1] The International Association for Computer Information Systems is a non-profit organization providing a forum for interpersonal networking and the sharing of research, teaching, and technical information through an annual International Conference, occasional special conferences.

[2] The fight against the cybercrime carried out in the Member States is different and there is no common storage of knowledge at European level or a common point of view in this respect. MS cannot benefit from the positive elements applied elsewhere nor learn from the mistakes and the possible solutions discovered. In fact, even thought CEPOL is carrying out a task in training, there isn't a common list of the "…courses run by..." and "…courses accepted by…" all the different stakeholders.

Proposes to draw up a feasibility study of the possibilities to create a Centre to carry out the aforementioned actions, if not already achieved and to serve as a reference body to third developing countries and relevant organizations in the fight against cybercrime. The Centre might also evaluate and monitor the preventive and investigative measures to be carried out in, taking into account the different point of views (law enforcement, judicial and administrative) in order to define common parameters. This feasibility study should consider notably the aim, scope, possible financing, and best location of this Centre. The Centre should fulfil the following tasks:

- To set up and update the standards of specialization to the police, judges, prosecutors and forensic staff with the appropriate levels to carry out the technological investigations. Likewise, to set up and update the minimal standards for the future trainers within the technological crime scope,
- To encourage and advise the Commission and the Council in the drafting of recommendations or rules designed to fight cybercrime from a global perspective,
- To serve as a permanent liaison body with user and victims organizations and the private sector. The Centre could design an European contract model of cooperation between the private and public sectors,
- To gather and update standards on the best practices on technological investigation techniques in the police, judicial and forensic scope and to evaluate and straighten the use of computer investigation tools to be used by police officers, judicial authorities and forensic staff in the European scope; to make them available within the EU and possibly to third countries, and
- To elaborate an annual (periodical) global report at a European level on the monitoring of the cybercrime phenomena and other problems related to the use of new technologies by the cybercrime, taking into account the national statistics.

Recognises the need to include the priorities identified in the Justice and Home Affairs external dimension strategy in an Action Plan in order to take further steps in cooperation with third countries whose involvement in the fight against cybercrime is essential.

Stresses that it is necessary to find out the best way to ensure an adequate financial support, a regular evaluation and an effective follow-up mechanism for this Action Plan in order to pinpoint any obstacles that may reduce the effectiveness and consistency of the actions to be carried out.

Calls upon the Commission to propose an Action Plan in order to improve the response against the problem of the cybercrime by way of short and medium-term actions to be launched no later than 2012.