COUNCIL OF THE EUROPEAN UNION

Brussels, 25 March 2010

5957/2/10 REV 2

LIMITE

CRIMORG 22
ENFOPOL 32

NOTE

from:	Presidency
to:	CATS
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 international cooperation and mutual assistance in law enforcement within Europe and between the EU and third countries needs to be substantially enhanced.

In recent years, several sets of 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 for specific action 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 for them to consider and discuss what to do next, 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.

Following the discussion held during the last MDG meeting and the written contributions received so far, delegations will find in the Annex 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 Cybercrime of 23 November 2001, that, inter alia, calls for international cooperation to protect society against this phenomenon;

2. The relevance given in the Stockholm Programme to the protection of the use of new technologies and the protection of citizens, and the modern challenges that have emerged in the form of cybercrime as criminal groups have taken effective advantage of new 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 the Stockholm Programme's provisions on 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's call on Member States, as laid down in the Stockholm Programme, to ratify the 2001 Council of Europe Cybercrime Convention as soon as possible, to give their full support to the national alert platforms in charge of the fight against cybercrime and the Council's emphasis on the need for cooperation with countries outside the European Union, and also its invitation 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 propose actions which would specify how the main points of the concerted strategy to combat cybercrime should be implemented, both in the short and medium term:

In the short term,

- finding out more about perpetrators and modus operandi, and sharing that knowledge in order to have a real idea of the scale of the problem and the way it is constantly evolving because of its heterogeneous nature, including crime related to the invasion of privacy, financial cybercrime, unauthorized access for the purpose of sabotage, crime against intellectual property, attacks on networks and against information systems, on-line fraud, child pornography and spam, and trafficking in illicit substances. Europol, in cooperation with the Member States and the Commission, is invited to facilitate this objective.

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

- 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 facilitate the collection, exchange and analysis of information. Europol, in cooperation with the Commission, is invited to facilitate this objective. The Member States are invited to set up their national cybercrime reporting systems or adapt their existing systems to be able to report to the ECCP.

- the implementation of priorities supported under the Safer Internet Programme 2009-2013 and the Prevention of and Fight against Crime (ISEC) Programme, to promote cross-border law enforcement cooperation and public-private partnership, particularly in the fight against child pornography. The Commission, in cooperation with the Member States, is invited to facilitate this objective.

- the continuity of existing activities and initiatives in this field, such as the CIRCAMP 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 distribution of child abuse images, facilitated by the European Financial Coalition (EFC), with active involvement by EUROJUST. The Commission and Europol are invited to facilitate this objective. The Member States, if they do not already do so, are invited to take an active part in the above activities.

- promotion of the use of joint investigation teams. The Member States, Europol and Eurojust, in cooperation with the Commission, are invited to facilitate this objective.

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

- To ratify the Council of Europe Cybercrime Convention. The Member States are invited to facilitate this objective.

- To consider raising the standards of specialization of the police, judges, prosecutors and forensic staff to an appropriate level to carry out cybercrime investigations. Europol and the Member States, in cooperation with the ECTEG (European Cybercrime Training and Education Group), Eurojust and the Commission are invited to facilitate this objective. The Member States are also invited, in cooperation with ECTEG and the Commission, to set up national centres of excellence in cybercrime training.

- To encourage information sharing between the Member States' law enforcement authorities; in particular, to facilitate the sharing of child pornography images with the International Child Sexual Exploitation Database at Interpol.

- To assess the situation regarding the fight against cybercrime in the European Union and the Member States, in order to achieve a better understanding of trends and developments in cybercrime. The Member States, in cooperation with Europol and the Commission, are invited to facilitate this goal through active participation at the European Union Strategic Group of the Heads of National High-Tech Crime Units at Europol.

- To adopt a common approach in the fight against cybercrime internationally, particularly in relation to the revocation of Domain Names and IP addresses. The Commission, in cooperation with the Member States and Europol, is invited to facilitate this objective.

- To promote harmonisation of the different networks 24/7, and of law enforcement contact points, eliminating possible duplication (G8 and INTERPOL). The Commission, in cooperation with the Member States, is invited to facilitate this objective.

- 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 reach a better understanding of the trends and modus operandi of this type of crime. The Commission is invited to facilitate this objective.

- To gather and update best practices on technological investigation techniques in the police, judicial and forensic authorities and to evaluate and boost the use of computer investigation tools by police officers, judicial authorities and forensic staff throughout Europe, in cooperation with entities established in this area such as ECTEG, INTERPOL, IACIS (International Association for Computer Information Systems) or other similar private and public organizations. The Member States, in cooperation with the Commission, are invited to facilitate this objective.

- To promote and boost activities to prevent cybercrime by promoting best practices in the use of networks, including cyber-patrols. The Member States, in cooperation with Europol and the Commission, are invited to facilitate this objective.

- To set up a documentation pool on cybercrime, to which all the actors involved have access, which could serve as a permanent liaison body with users' and victims' organizations and the private sector. The Commission, in cooperation with Europol, is invited to facilitate this objective.

Proposes that the Commission draw up a feasibility study on the possibility of creating a centre to carry out the aforementioned actions, where they have not already been achieved. The centre might also evaluate and monitor the preventive and investigative measures to be carried out. This feasibility study should consider, in particular, the aim, scope and possible financing of the centre and whether it should be located at Europol. The Centre could also fulfil the following tasks:

- help to meet the standards of specialization required by police, judges, prosecutors and forensic staff to carry out technological investigations as well as those needed by trainers in this field.
- serve as a permanent liaison body with user and victims' organizations and the private sector. The centre could design and update a model European contract for cooperation between the private and public sectors.

- gather and update standards on best practices on technological investigation techniques in the police, judicial and forensic authorities and evaluate and streamline the use of computer investigation tools by police officers, judicial authorities and forensic staff in Europe; make them available within the EU and possibly to third countries, and
- elaborate annual reports on cybercrime phenomena at European level and on other problems related to the use of new technologies, taking into account national statistics, and advise the Commission and the Council in the drafting of recommendations or rules designed to fight cybercrime globally.

INVITES the Commission to assess the progress made in preparing for the implementation of the actions provided for in the above short-term and medium-term points. Consequently, requests the Member States, Europol and Eurojust to inform it of the contributions they make.

CALLS for these measures to be included in the Action Plan accompanying the Stockholm Programme (2010-2014) and the future Internal Security Strategy mandated therein.

_____