COUNCIL OF THE EUROPEAN UNION

Brussels, 11 November 2008

15569/08

ENFOPOL 224
CRIMORG 190

NOTE

from :	Presidency
to :	COREPER/Council
No. prev. doc. :	15236/08 CRIMORG 181 ENFOPOL 214
Subject :	Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime

The Justice and Home Affairs Council, held on 24 and 25 July 2008, welcomed the Presidency's idea of drawing up a plan to combat cyber crime in the EU, consisting of both the setting up of national alert platforms as well as a European alert platform and the elaboration of a concerted work strategy and practical measures to combat cybercrime. On 24 October 2008 the Council adopted conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet.

The Presidency submitted a proposal for draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime. These draft Council Conclusions were recently discussed at the Police Cooperation Working Party meeting on 5 November 2008 and agreed by the Article 36 Committee at its meeting on 10 November 2008. The draft conclusions as they result from these discussions are set out in annex.

The Permanent Representatives Committee is invited to agree to the draft conclusions contained in the annex and to submit them to Council for approval.

Draft Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime

NOTING THAT:

- one of the objectives of the European Union is to gradually set up an area for Justice, Liberty and Security by establishing joint actions by the Member States in the sphere of police and judicial co-operation;

- protecting Europeans is one of Europe's basic tasks. Accordingly, the Union must be in a position to detect emerging forms of crime and to adapt its action so that responses are set up rapidly;

- in recent years, there has been a continual increase in offences observed on the Internet which are increasingly transnational, as the Internet removes all borders;

- the priority given to a strategy aiming at combating organised crime and computer crime was set at the European Council meeting in Tampere in October 1999. Since then, it has been confirmed by the considerable amount of work carried out by European institutions, particularly with the Commission's communication of 22 May 2007 to the European Parliament, the Council and the Committee of the Regions: "Towards An Overall Policy Against Cybercrime" and the 2005/222/JHA Framework Decision of 24 February 2005 on attacks against information systems[1], which the Commission intends to update in 2009;

- by 15 September 2010 at the latest, the Commission will carry out an assessment on the implementation of Directive 2006/24/CE of the European Parliament and the Council of 15 March 2006, regarding data retention;

[1] OJ L 69, 16.3.2005, p. 67.

- the Commission and the Council of Europe have already achieved work in order to strengthen the partnership between public authorities and the private sector to combat cybercrime;

- the Commission will present a communication on future priorities in the fields of Liberty, Security and Justice in Europe which will prefigure the next long-term programme (2010-2014) and which should deal with the fight against cybercrime;

- the Council's adoption of the conclusions on the establishment of national mechanisms enabling a European platform for reporting offences noted on the Internet[1] expresses this intention to reinforce law enforcement co-operation by providing law enforcement agencies with significant and effective resources;

- finally, the development of a comprehensive programme against cybercrime appears to be the most appropriate working method at Union level if we are to find solutions to all the issues which arise on the subject, or which are likely to arise in the near future, and to monitor their implementation.

THE COUNCIL:

1) CONSIDERS that it is important to combat the various elements of cybercrime and to invite the Member States and the Commission to determine a joint working strategy, taking into account the content of the Council of Europe Convention on cybercrime.

   The purpose of this strategy should be to make it possible to cope even more effectively with the multiple crimes committed by means of electronic networks. These take forms as worrying as child pornography, any form of sexual violence, and any act of terrorism – as defined by the Framework Decision 2002/475/JAI of 13 June 2002.
   It should also contribute to responding to the specific threats weighing on electronic networks (large-scale attacks against information systems).

[1] Doc. 13243/08 ENFOPOL 162 CRIMORG 140.

Finally, this strategy should tackle the means of combating the traditional forms of crime committed via the Internet, such as identity fraud, identity theft, fraudulent sales, financial offences, illicit trading on the Internet, particularly narcotics and arms dealing.

2) CONSIDERS that the search for an effective response to these various threats in relation to electronic networks must be met by such horizontal measures as:

a) strengthening the partnership between public authorities and the private sector so as to jointly design methods for detecting and preventing damage caused by criminal activities and for victimised companies to transmit relevant information concerning the frequency of offences suffered to the law enforcement agencies. In particular, it is recommended that the Commission work on the details of the guidelines adopted by the Conference on Global Co-operation Against Cybercrime, which met under the auspices of the Council of Europe on 1 and 2 April 2008, and which aimed at improving the partnership between public authorities and the private sector in the fight against cybercrime. In this context, the Council notes the recommendations made after the meeting of experts organised by the Commission on 25 and 26 September this year, attached in appendix;

b) improving knowledge and training among stakeholders involved in the fight against cybercrime in Europe. In particular, setting up a network of Heads of police against cybercrime would be appropriate. This initiative would indeed supplement the work undertaken by active expert groups in this field, which will not only take into account the future risks, but also the procedures for urgent actions with regard to severe incidents, similarly to the group set up under the auspices of Europol, or by the Joint Research Centres, set up by the Commission;

c) reinforcing technical and international co-operation with third countries, which must increasingly cope with this criminal scourge, as well as technical assistance;

3) INVITES, from this viewpoint, the Member States and the Commission to introduce measures based on case studies, particularly taking into account technological developments, so as to prepare tools for operational use, in the short and medium term, such as:

a) in the short term

- setting up a European platform aimed at reporting criminal acts committed on Internet;
- drafting, in consultation with private operators, of a European agreement model for co-operation between law enforcement agencies and private operators;
- finding a description of what is meant by identity fraud on the Internet, in compliance with domestic laws;
- setting up national frameworks and exchanging best practice regarding cyberpatrols, which is a modern tool against crime on Internet, enabling information on nicknames to be shared on a European scale in accordance with domestic laws on the data exchange;
- resorting to joint investigation and enquiry teams;
- finding a solution to the problems caused by electronic networks roaming and by the anonymous character of prepaid telecommunication products;

b) in the medium term

- exchanging on the mechanisms for blocking and/or closing down child pornography sites in Member States. Service providers should be encouraged to adopt these measures. If necessary, the European platform could be a tool for establishing a common blacklist;
- facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country;
- developing temporary definitions of categories of offences and statistical indicators to encourage the collection of comparable statistics on the various forms of cybercrime, taking into account the work that the European Union is presently doing in this field.

4) INVITES the Commission to assess the progress made in preparing the implementation of the actions provided for in the above mentioned points 2 and 3. Consequently, requests the Member States to inform it of the contributions they make.

5) CALLS for the setting up of additional measures in the longer term within the scope of the next long-term JLS programme (2010-2014).

1. Law enforcement authorities and the private sector[1] should be encouraged to engage in operational and strategic information exchange to strengthen their capacity to identify and combat emerging types of cybercrime. Law enforcement authorities should be encouraged to inform service providers about cybercrime trends.

2. In particular, the Member States are encouraged to set up standardised system for trusted operational and strategic information exchange between law enforcement and the private sector. Essential components of such a system include the following structures and procedures:

3. Permanent contact points: Law enforcement permanent contact points – and private sector equivalents – should be established in order to improve the clarity and efficiency of request and response processes. The private sector equivalent should also provide an 'out of hours' service in order to respond to urgent law enforcement requests. The qualification of 'urgent' should be agreed between law enforcement and the private sector.

4. The private sector and law enforcement are encouraged to assist each other with education, training and other support on their services and operations.

5. Standard Request Form: At the national level, and if possible with 3rd countries, law enforcement should standardise and structure the form used for sending requests and for responding to requests. The private sector should use the latter form when responding to law enforcement requests. As a minimum, requests from law enforcement should be in writing, preferably in electronic format, and contain the following information:
   - Reference number
   - Reference to legal basis

[1] The term 'private sector' includes not only private sector companies, but also other relevant stakeholders in the information and communication technologies industry (ICTs) including computer emergency response teams (CERTs).

- The specific data requested
- Time zone
- Information to verify the source of the request

6. Request Prioritisation Levels: A system for prioritization of law enforcement requests to the private sector should be agreed by law enforcement and the private sector.

7. Law enforcement and the private sector should be mindful of the costs involved in creating and responding to requests. Procedures should be developed with consideration of the financial impact of these activities and issues of cost reimbursement or fair compensation to relevant parties should be considered.

8. The European Commission, Member States and private sector stakeholders are called upon to facilitate the exchange of best practices in respect of points 1-7 above, with a view to bringing national mechanisms closer together and, at term, the creation of a system for exchange of operational and strategic information at EU-level.