



**COUNCIL OF
THE EUROPEAN UNION**

**Brussels, 26 September 2008 (30.09)
(OR. fr)**

13567/08

LIMITE

**ENFOPOL 170
CRIMORG 150**

NOTE

from : Presidency
to : Working Party on Police Cooperation

No. prev. doc.: 11784/08 ENFOPOL 139 CRIMORG 113 + COR 1

Subject : Draft Council conclusions on a concerted work strategy and practical measures to
 combat cyber crime

Delegations will find attached the above draft conclusions, which the Presidency would like to submit to the JHA Council in November.

Draft
**Council conclusions on a concerted work strategy and
practical measures to combat cyber crime**

RECALLING that:

- one of the objectives of the European Union is the progressive establishment of an area of justice, freedom and security by developing common action among the Member States in the field of police and judicial cooperation;
- protecting European citizens is one of the key tasks of the European Union. The Union must therefore be able to detect emerging forms of crime and adapt its activities to ensure that an effective response is rapidly put in place;
- the number of offences detected on the Internet has been rising steadily in recent years and becoming more and more international in character, as the Internet breaks down borders;
- a strategy to combat organised crime and computer crime was prioritised at the European Council in Tampere in October 1999. This priority has since been confirmed in much of the European institutions' work, notably the Commission communication to the European Parliament, the Council and the Committee of the Regions: "Towards a general policy on the fight against cyber crime" of 22 May 2007 and Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems¹, which the Commission intends to update in 2009;
- the Commission and the Council of Europe are already working to enhance public-private partnerships to combat cyber crime;

¹ OJ L 69, 16.3.2005, p. 67.

- the Commission is due to submit a communication on future priorities in the area of freedom, security and justice in Europe, which will prefigure the next multiannual programme (2010-2014), and should tackle cyber crime;
- the Council has adopted conclusions on setting up national arrangements to provide input for a European alert platform for reporting offences noted on the Internet², reflecting this determination to step up police cooperation by giving police services effective and wide-ranging powers;
- lastly, developing an overall anti-cyber crime plan seems the working method best suited to finding solutions to the questions which have arisen or are likely to arise in the near future, and to ensure that implementation of those solutions is followed through.

THE COUNCIL:

- (1) CONSIDERS that it is important to combat cyber crime in all its various aspects and invites the Member States and the Commission to define a concerted working strategy.

The aim of this strategy should be to make it possible to tackle even more effectively the many criminal activities committed using electronic networks, which take such worrying forms as child pornography, all forms of sexual violence, incitement to commit terrorist acts or condoning terrorism.

It should also help respond to specific threats to electronic networks (large-scale attacks on information systems).

Lastly, the strategy should examine means of combating traditional forms of criminal activity committed over the Internet, such as identity fraud, identity theft, fraudulent sales, financial offences and illicit trade on the Internet, especially in drugs and arms.

² 13243/08 ENFOPOL 162 CRIMORG 140.

- (2) CONSIDERS that an effective response to these various Internet-related threats should take the form of cross-cutting measures such as :
- (a) enhanced public-private partnership, with a view to joint formulation of methods of detecting and preventing the damage caused by criminal activity, and reporting to the law enforcement agencies of relevant data on the frequency of offences by companies which have fallen victim to such crime. In particular, the Commission is recommended to work along the guidelines adopted by the Conference on Cooperation against Cybercrime held under the auspices of the Council of Europe on 1 and 2 April 2008, to improve public-private partnership in the fight against cyber crime. In this context, the Council notes the recommendations made at the close of the meeting of experts organised by the Commission on 25 and 26 September 2008;
 - (b) greater understanding between those engaged in combating cyber crime in Europe. In particular, it would like to see : the establishment of a network of heads of computer crime units, of a group of experts whose remit would be to consider future risks, in the framework of the ENISA, and of a European technology monitoring group, together with specialised training;
 - (c) enhanced international technical cooperation with third countries which are increasingly having to face this criminal phenomenon, and technical assistance;
 - (d) implementation of follow-up on data retention, by ensuring follow-up to the European Directive on the subject (Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006³).

³ OJ L 105, 13.4.2006, p. 54.

(3) INVITES Member States and the Commission, with this in mind, to submit measures in order to prepare operational tools for the short or medium term, such as:

(a) in the short term

- setting up a European alert platform for reporting offences committed on the Internet;
- drawing up a specimen European contract for cooperation between law enforcement agencies and private operators;
- joint definition of a specific offence of identity fraud on the Internet;
- setting up national frameworks and establishing exchanges of good practice on cyber patrols, a modern weapon against Internet crime, allowing information-sharing on pseudonyms at European level;
- use of joint inquiry and investigation teams;
- a solution to the problems of roaming in relation to electronic networks;
- updating Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems;

(b) in the medium term

- instituting exchanges of good practice on mechanisms for blocking and/or closing down child pornography sites in all the Member States, by requiring service providers to take such measures. The European alert platform could provide a means of drawing up a joint blacklist;
- measures to facilitate remote computer searches, allowing investigators rapid access to data;
- establishing statistical indicators to reflect different forms of cyber crime.

- (4) INVITES the Commission to coordinate and summarise the activities referred to in points 2 and 3 above. Requests the Member States, therefore, to inform it of their contributions.
- (5) CALLS FOR additional long-term measures to be put in place in the next multi-annual Justice, Freedom and Security programme (2010-2014).

=====