COUNCIL OF
THE EUROPEAN UNION

Brussels, 30 October 2007

13893/2/07
REV 2

LIMITE

CRIMORG 148
CATS 110

NOTE

from:	Presidency
to:	COREPER/Council
Subject:	Draft Council Conclusions on Cybercrime

The move towards an information society has seen profound changes in the way in which people and institutions live and in life in general. The new communication technologies are having great impact on economies and on society, making for growth, competitiveness, and smoothness and speed of economic dealings, as well as for mobility and interaction on the part of people in different countries.

However, just as computer systems facilitate performance of a multitude of activities by people and institutions, overcoming geographical obstacles in next to no time, they also make it possible to perpetrate, aid and abet all manner of criminal activities. This raises another aspect of the matter, crime committed by means of or against computer systems, or cybercrime, which poses one of the new challenges faced by our societies. This is a serious threat, of worrying proportions, to public and private bodies alike, which defies geographical borders, knowing no barriers or boundaries. When misused, or used for the wrong purposes, information technologies can serve as tools for activities endangering or harming people's life, property or dignity, or causing serious damage to economies and to society in general. This is a real concern for a democracy based on the rule of law.

Cybercrime can basically be committed from anywhere in the world, with effects in a completely different place. The true scale of the problem is not very well known, since this is an ever-changing, constantly evolving type of crime. It is nevertheless possible to point to some especially problematic areas, including intrusion upon privacy, content-related crime, economic crime, unauthorised access and sabotage, intellectual property infringements, system or network attacks, identity theft, phishing and spam. There are also worrying forms of cybercrime in connection with terrorism (incitement and recruitment), money laundering and sexual exploitation of minors, such as child grooming.

In view of the above and following the discussions at the MDG of 24 October and the JHA Counsellors meeting at 28 October 2007, the Presidency presents the redrafted Council conclusions set out in the annex to this note.

COREPER is asked to invite the Council to adopt the attached Conclusions.

ANNEX

Council conclusions of

…..2007

on combating cybercrime

In view of:

1) The significant rise of cybercrime figures in recent years and the increasing links with organised crime;

2) The prioritisation of a strategy to combat organised crime and computer crime at the European Council meeting in Tampere in October 1999;

3) The Council Decision of 29 May 2000 to combat child pornography on the Internet, which requires Member States to take the necessary measures to encourage Internet users to inform law enforcement authorities, either directly or indirectly, of suspected distribution of child pornography material on the Internet, if they come across such material;

4) The Commission communication of 26 January 2001 to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, "Creating a safer information society by improving the security of information infrastructures and combating computer-related crime";

5) The Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, which aims to improve cooperation between judicial and other competent authorities, including the police and other specialist law enforcement agencies of the Member States, in particular by harmonizing criminal law rules in the area of attacks against information systems;

6) The Council and Commission action plan implementing the Hague programme on strengthening freedom, security and justice in the European Union, which mentions the possibility of issuing a recommendation on minimum standards for capturing and exchanging electronic evidence;

7) The Commission communication of 31 May 2006 to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, "A strategy for a secure information society – Dialogue, partnership and empowerment";

8) The European Council conclusions from June 2007, welcoming the communication from the Commission on the fight against cybercrime and calling for the development of a policy framework in this field.

The Council,

1) In the efforts to combat cybercrime, welcomes and attaches considerable importance to (...) the Commission communication of 22 May 2007 to the European Parliament, the Council and the Committee of the Regions, "Towards a general policy on the fight against cyber crime", which represents a further step towards adopting a coherent EU policy to prevent and combat cybercrime;

2) Considers the Commission's intention to strengthen EU-wide cooperation on training for police and judicial authorities as highly significant, especially as regards the establishment of a permanent cybercrime training platform. This is especially important since constantly evolving cybercrime also requires constant updating of those who prevent, investigate and judge it;

3) Welcomes the Commission's intention of stepping up dialogue between the public sector and the private sector, in order to facilitate the prevention and detection of computer crime, since in present-day reality most communications operators are privately owned and considering the important role of the private sector in developing security technologies. (...) It should be added that it is usually private parties who detect attacks against their information systems as well as illegal content on networks, who are also usually responsible for blocking or removing it and who are required to record and retain communications data. Therefore, police and judicial authorities need to be able to seek the assistance of the private sector in taking action against offenders;

4) Supports and encourages the confidence placed in the Council of Europe Convention of 23 November 2001 on Cybercrime;

5) Attaches the greatest importance to promoting cooperation with non-member countries in preventing and combating cybercrime, more specifically, given the pivotal role of the Council of Europe Convention on Cybercrime (...) by supporting the introduction of that globally oriented legal framework, in liaison with the Council of Europe, especially in countries where development and technical assistance is being provided;

6) Considers it vital to call for swift implementation in all countries of legal instruments to combat all forms of cybercrime (...);

7) Sees a strong need of implementing all relevant EU and international instruments fighting the sexual exploitation of children, in particular child pornography;

8) Believes that consideration should be given whether there is a need, in each Member State, to enact legislation on identity theft, particularly by way of cybercrime (...) and whether further action at EU level is needed;

9) Sees a strong need to enhance coordination and further improve the performance of all available players and resources, in Member States as well as in organs such as Europol and Eurojust and international bodies like Europol;

10) Underlines the need to put into practice and assess the working of arrangements for cooperation between authorities in different countries, with particular reference to the 24/7 network provided for in Framework Decision 2005/222/JHA of 24 February 2005, which ensures round-the-clock cooperation between authorities seven days a week, thus speeding up the response to cybercrime (…);

11) Looks forward to receiving the Commission report on the implementation of the Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems;

12) Wishes to associate itself with efforts being made to promote a more secure information society, which strikes a balance between fundamental rights and access to information via computer systems and networks, as well as responding to all of the needs met with in preventing and combating cybercrime.