COUNCIL OF THE EUROPEAN UNION

Brussels, 11 July 2008 (16.07) (OR. fr)

11784/08

LIMITE

ENFOPOL 139
CRIMORG 113

NOTE

from :	Presidency
to :	COREPER/Council
Subject :	Comprehensive plan to combat cyber crime

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. Cyber crime is currently one of the most serious worldwide threats. Every day the digital economy is of greater importance in the lives of Europe's citizens. Its limits are as yet unknown.

Cyber crime, a threat now and in future

Like all the major innovations which have changed people's lives throughout history, the Internet is both an extraordinary tool promoting progress, and a potential weapon in the hands of criminals.

It can be used as a tool without borders in several areas and provides a large degree of impunity for its users, because of its special nature as regards the location of sites and the anonymity of activities:

- It is the medium for scams such as "phishing", a technique by which criminals seek to obtain confidential information from their victims by imitating messages or the sites of institutions or companies which the internet user trusts. As well as being used to falsely obtain bank details, or to assume the internet user's identity to carry out illegal activities, such scams are also used to dispose of considerable quantities of stolen, prohibited or counterfeit goods, particularly pharmaceutical products.
- It is also a very effective means of communication and recruitment between terrorists all over the world.
- It makes illegal content generally available. Such material glorifies violence and terrorism and incites racial hatred. It displays images of sexual violence against children. It also makes it easier to search for victims under false pretences.
- The Internet and the digital economy may themselves be the victim of criminal attacks. The security of systems which are essential for public safety, the sovereignty of the State, or its economic life, may be threatened. One Member State of the European Union has recently been the victim of cyber attacks.

Reaction by the European Union and the international community

The international community, and particularly the European Union, have not been inactive in this area. International legal instruments have been adopted, such as the Council of Europe's 2001 Convention on cybercrime. The G8's specialised "Lyon-Roma" Group has also worked on this. However, these elements do not seem to add up to an overall solution: the Council of Europe Convention has not been ratified by all its members, and the G8's work has run into serious difficulties as regards the identification of hosted sites.

Some texts have also been adopted in the European Union context. Some specifically address a particular aspect of cyber crime, such as Framework Decision 2005/222/JHA on attacks against information systems. Others contain a chapter on the use of the Internet in the context of a specific crime problem, such as Framework Decision 2004/68/JHA which relates to child protection. Directive 2002/58/EC on privacy and electronic communications obliges service providers to safeguard the security of their services. The creation in 2004 of a European Network and Information Security Agency (ENISA) was a positive step towards alerting Member States and European citizens to the issue of information system security and establishing the foundations of a common European culture of making information systems secure. This issue is also addressed in the EU's 7th Research Framework Programme.

Work is currently under way at the Commission, for example on draft recommendations on public-private partnerships and the training of high-level specialist investigators.

More broadly, in 2007 the Council and the Commission looked at key concepts for the future. On 25 May 2007 the Commission forwarded a Communication to the European Parliament, the Council and the Committee of the Regions, entitled "Towards a general policy on the fight against cyber crime" which sets out an overall framework and lists relevant measures. The European Council of 8 and 9 November 2007 welcomed the Commission recommendation and highlighted the importance of the training of police and judicial authorities, dialogue between the public and private sectors, and the Council of Europe Convention of 23 November 2001.

The emergence of new issues

There are many instruments and projects already in existence, but they are not constantly followed up. Also, new issues appear in addition to those already covered. Often they require common approaches:

- the legal system for "blocking" sites containing child pornography, which has been adopted or is being adopted by some Member States;
- the use of investigations under pseudonyms (cyber patrols) and their possible extension to areas other than child protection (for example in relation to attacks on automatic data processing systems);
- the area of remote computer searches, which are a delicate issue because of their cross-border nature.

The action proposed by the French Presidency

- **Defining operational tools**

The French Presidency of the Council of the European Union proposes to create a European platform for issuing alerts about offences detected on the Internet. Hosted by EUROPOL, this structure would receive alerts on offences from the national platforms of the European Union's Member States. A seminar was held in Reims in June 2008 where the outline of this mechanism was established. In parallel, those Member States which do not yet have such a platform at national level are being invited to create one.

The Presidency also wishes to promote a strengthening of the "Check the web" project initiated during the Portuguese Presidency to combat terrorist propaganda and recruitment on the Internet, and to seek a solution to the problem of roaming in electronic networks.

- **Seeking an overall plan**

It would therefore seem desirable to seek the best working method at Union level to find solutions to all the questions which have arisen or are likely to arise in the near future, and to ensure that the implementation of those solutions is followed through. These instruments and measures could be arranged in chapters for each of the main areas related to cyber crime, for example:

- relations between the public and private sectors;
- joint action by the Member States in international bodies (UN, G8);
- specific tools appropriate for the different forms of cyber crime;
- harmonisation of legislation in the Member States, where this provides added value;
- joint training and research for the Union's police.

Conclusion

In the Union, several methods are used to tackle major issues horizontally: in particular, action plans and lists of priorities. The Presidency therefore asks the relevant working parties at the Council and the Commission to make proposals with a view to the drafting of an action plan, while continuing the work they already have under way on specific tools. The broad outline of this plan, which will be based in particular on the European Council conclusions of November 2007 and the Commission's recommendations, could be submitted to a forthcoming meeting of the Council of Ministers.