MEMO/07/199

Brussels, 22 May 2007

The commission communication "towards a general policy on the fight against cyber crime"

The use of the term cyber crime in this communication

There is no agreed definition of "cyber crime". From a strictly legal point of view, it can be questioned whether there is any need for the term at all – it could be argued that "cyber space" is just a new specific instrument used to commit crimes which are not new at all. The term may thus be most interesting from an operational point of view, i.e. the operational instruments and procedures to fight against this type of crime must be developed.

In this communication, the term cyber crime is applied to three categories of criminal activities. The first covers **traditional forms of crime** such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of **illegal content** over electronic media (i.a. child sexual abuse material or incitement to racial hatred). The third includes **crimes unique to electronic networks**, i.e. attacks against information systems, denial of service and hacking.

Background

The rapid development of Internet and other information systems has given rise to a completely new economic sector and to new rapid flows of information, products and services across the internal and external borders of the EU. This has opened many new possibilities for criminals. A pattern of new criminal activities against the Internet, or with the use of information systems as a criminal tool, is clearly discernible. These criminal activities are in permanent evolution, and legislation and operational law enforcement have obvious difficulties in keeping pace. The intrinsic cross-border character of this new type of crime creates a need for improved cross-border law enforcement cooperation.

During the consultations undertaken by the Commission, in particular eight problem areas were identified:

- A growing vulnerability to cyber crime risks for society, business and citizens
- An increased frequency and sophistication of cyber crime offences
- A lack of a coherent EU-level policy and legislation for the fight against cyber crime
- Specific difficulties in operational law enforcement cooperation regarding cyber crime, due to the cross-border character of this type of crime, the potential great distance between the crime perpetrator and the crime victim and the extreme speed with which crimes can be committed
- A need to develop competence and technical tools (training and research)
- The lack of a functional structure for cooperation between important stakeholders in the public and the private sector
- Unclear system of responsibilities and liabilities for the security of applications as well as for computer soft- and hardware
- The lack of awareness among consumers and others of the risks emanating from cyber crime

Although consultations undertaken with public and private stakeholders seem to indicate that there is a general agreement in Europe regarding the need for the EU to take action in this field, the powers of the EU in this field are limited. The actions now planned can not go beyond what is required and what is clearly adding value at EU-level. The main feature of all planned EU actions in the short term will be of a coordinating nature, and the measures taken might seem to be insufficient in relation to the real problem. However, the benefits of EU-level coordination in this field should not be underestimated.

The proposed Communication is consistent with the Council and Commission Action Plan implementing the Hague Programme, in which the need for urgent action to improve European coordination and cooperation between high-tech crime units in Member States and with private sector has been identified.

Statistics and numbers

For many reasons, there are no reliable statistics on cyber crime: cyber crime is a vast area and covers innumerable crimes and no common statistics system exists. There is also evidence suggesting that cyber crime incidents are very rarely reported – this is especially the case when the criminal activity is directed towards companies: any report might be perceived as a security problem and lead to competition disadvantages. However, the following indicative figures can be given to illustrate the scope of the problem:

1) As an indicative example of the increased frequency of one particularly serious form of crime, the publication of child sexual abuse material, the UK-based Internet Watch Foundation has estimated that the number of sites with this type of illegal material has increased with 1 500 percent in the period 1997-2005.

2) It has been estimated that 750 000 computers are infected through Botnets[1] every year in Germany.

3) The UK Financial Service Authority has estimated that the number of bank frauds through Phasing has increased with 8 000 percent in the last two years.

One outcome of the new cyber crime communication may be that more information on crime is collected and that the statistics can be improved. The development of a comprehensive and coherent EU strategy to measure crime and criminal justice, as announced in the EU Action Plan adopted in 2006.[2]

The Communication

The main objective of the draft Communication is to formulate a general policy on the fight against cyber crime at EU level. In the light of identified needs and the limited powers of the EC and the EU in this field, this policy will as a first phase concentrate on actions to improve international cooperation and coordination in general, to reinforce operational cross-border law enforcement cooperation, including anti-cyber crime training, and to strengthen public-private cooperation in the field of fight against cyber crime. The Communication also includes a list of actions planned by the Commission in the next period of time.

The Communication is the result of extensive consultations with public and private stakeholders during several years. In particular, an important study to assess the impacts of different options in the fight against cyber crime from 2006 should be mentioned. The main lines of the Communication have been inspired by these consultations.

The Communication presents a coherent EU strategy for the fight against cyber crime. This strategy will give the European Commission a central coordinating role in Europe. The Commission will closely coordinate all actions with Member States and other competent bodies. The concrete policy can be divided into four main policy areas or instruments:

- Improved European law enforcement cooperation

[1] Botnet refers to a collection of compromised machines running programs under a common command. The criminal takes control over the whole collection of machines, without the knowledge of the owner/user of the individual computers, and use them to, for example, attack a specific information system.

[2] COM(2006)437 final.

The main feature of this policy instrument is a proactive policy in reinforcing the structures for operational law enforcement cooperation. The Commission will launch a reflection on how this cooperation can be strengthened and improved. This will mainly be done through the organisation of a European law enforcement conference, and possibly – if this is considered necessary after an initial discussion – through a decision to set up a specific task force/working group. The discussions may also lead to a formal proposal to strengthen existing structures, especially the high-tech crime work at Europol and Eurojust. The policy instrument includes actions to improve exchange of information and best practices, initiatives to improve training and awareness-raising within law enforcement authorities.

- Increased European public-private cooperation

This policy instrument aims at strengthening existing public-private cooperation against cyber crime and to create new public-private projects. The Commission will organise a major conference in order to consider how cooperation can be strengthened concerning areas such as the fight against illegal content (such as child pornography and incitement to terrorism) on the Internet, Botnets and other illegal activities. The Commission will especially promote an atmosphere of confidence between the sectors, which could facilitate efficient and rapid actions against illegal activities. The Commission will also support ad hoc initiatives for better cooperation against specific problems. This policy instrument also includes exchange of information and best practices, initiatives to improve training, relevant research and awareness-raising in both the public and private sector.

- International cooperation

This policy instrument aims at better coordinating EU actions against cyber crime with external and international initiatives. In fact, cyber crime in Europe is a phenomenon which may originate or have its effects far beyond the borders of the EU. A global approach is thus especially needed when it comes to the fight against this type of crime. The Commission will promote a common European approach to international cooperation in this field and also take a proactive role in international projects such as the ones initiated by Interpol, the Council of Europe or the G 8 Roma-Lyon High-tech crime group. The policy instrument also includes exchange of information and best practices and initiatives to improve training and relevant research.

- Legislation

As has been made clear above, no general legislation on the fight against cyber crime can be expected to be effective at this moment. However, legislation can be an efficent instrument when the three policy instruments just mentioned prove insufficient. Targeted legislative actions may also prove to be appropriate or needed in specific areas. As an example, the Commission will consider an initiative regarding European legislation against identity theft in 2007. Legislative action could also include developing a regulation on the responsibility of different actors in the relevant sector.

Concrete implementation of actions announced in the Communication

The Commission services have already started planning the implementation of the actions announced in the Communication and intense working-level consultations with Member States, Europol and private sector stakeholders have already begun. The concrete actions planned can be summarized as follows:

- Public-private cooperation at operational level: A conference on public-private cooperation is being organised for November this year. The conference, which will gather around 100 European specialists from both sectors, will concentrate on a few pilote areas. The main idea is to launch a small number of concrete public-private projects, on issues such as the fight against illegal content (especially child sexual abuse material) and strategic information exchange on criminal activities. The outcome may consist of codes of conduct, the setting up of permanent cooperation networks or recommendations for legislation. The principle of the public-private projects will be cooperation at equal level and private stakeholders (in particular EU-level business federations) will be involved already at the planning stage.
- Law enforcement cooperation/coordination: The problem identified in this field is rather that existing EU and international channels are not used or that these channels are not used in an efficient way. The Commission services are currently preparing a questionnaire to Member States and will organise a meeting with MS cyber crime specialists in 2007 to better identify the needs. The main objectives are to clarify the use and achieve better awareness of existing and – if needed – prepare concrete actions to reinforce the cooperation and coordination. The Commission will cooperate closely with Europol in this area.
- Training: The Commission is already discussing how different EU-level and EU-financed training programmes in this field can be interlinked under a common European training umbrella. The Financial Programme "Prevention of and Fight against Crime" will provide for financial means for the setting up of such an umbrella, which could cover both law enforcement only training programmes and programmes involving private sector operators. The Commission is especially looking to involve Europol, Eurojust and CEPOL in the setting up of such a platform.

For more information on the activities of Vice-President Frattini, please visit his website at: http://www.ec.europa.eu/commission_barroso/frattini/index_en.htm