COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.5.2007
SEC(2007) 641

COMMISSION STAFF WORKING DOCUMENT

Accompanying document to the

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE COMMITTEE OF THE REGIONS

Towards a general policy on the Fight against Cyber crime

SUMMARY OF THE IMPACT ASSESSMENT

{COM(2006) 267 final}
{SEC(2006) 642}

SUMMARY

1. INTRODUCTION

The use of the Internet has exploded in recent years, and the appearances of new phenomena and new techniques have created a situation of increased insecurity.

In its **Legislative and Work Programme 2007**, the Commission has considered that a comprehensive update of the Commission's cyber crime policy has become necessary and therefore envisaged the preparation of a Communication on European cyber crime policy.

During the initial consultation process it became clear that there is a lack of data and statistics, which was one of the main reasons why the Commission in 2006 ordered an **external study**[1] (hereafter: the external study), constituting the main support for the impact assessment.

During the preparations, the Commission has also analysed a number of legislative and non-legislative measures, especially in relation to possible "gaps" in the existing regulatory framework. It should be underlined that a particular emphasis has thereby been laid on the **Council of Europe Convention on cyber crime**[2] (hereafter: the CoE Convention) and the **Framework Decision On Attacks Against Information Systems**[3], as these were considered to be the most comprehensive ones in terms of substantive and procedural law.

On the basis of these activities, the Commission is preparing a new general policy initiative, consisting of a Communication on the Fight against Cyber Crime at EU level. The present impact assessment will thus principally deal with strategic questions.

In this context, the Commission would underline its commitment to ensure that the policy on the fight and prosecution of cyber crime will be defined and implemented in a manner which fully respects fundamental rights, in particular the freedom of expression, the right to respect for private and family life and the protection of personal data. This will be done in accordance with the Commission Communication on the compliance with the Charter in Commission legislative proposals adopted in 2005 - COM(2005) 172.

2. PROBLEMS AND OBJECTIVES

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 obviously had numerous positive effects for consumers and citizens. However, the same development has also 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

---

1 Study to Assess the Impact of a Communication on Cyber Crime prepared by Yellow Window Management Consulting (Contract No DG 2006/JLS D 2/03).

2 Council of Europe Convention on Cyber crime, 2001: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3 Framework Decision 2005/222/JHA on attacks against information systems.

obvious difficulties in keeping pace. The intrinsic cross-border character of this new type of crime also creates a need for improved cross-border law enforcement cooperation.

The following eight strategic problem areas have been considered in order to study the overall problem more in detail.

- The growing vulnerability to cyber crime risks for society, business and citizens
- An increased frequency and sophistication of cyber crime offences
- The 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
- The 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 responsibilities and liabilities
- The lack of awareness of the risks emanating from cyber crime

It should be noted that the consultations undertaken in view of the present report indicated strikingly converting views from all stakeholders – be they law enforcement authorities or private companies – regarding current EU problems in this field.

2.1. Who is affected?

Cyber crime affects all sectors of society, and a policy to counter it will also be visible practically everywhere. Considering that the number of citizens using private computers is very high, most individual citizens – already in their capacity of potential victims – may also be affected by any initiative in the area of fight against cyber crime.

There are however also clear indications pointing at increased criminal activity directed against specific groups of victims. An effective anti cyber crime policy could thus have clear beneficial effects for these groups. The information society industry, as well as information society in general, could also be expected to be a major stakeholder in this context, given the important positive economic effects that can be expected if security is strengthened or if an atmosphere of enhanced security were to be established.

2.2. Does the EU have a right to act?

Given the scope and magnitude of security threats, a need to tackle the threats from cyber crime persists and may be growing. Security issues connected to cyber crime have a global dimension and cannot therefore be dealt with only at national level. The threat is international, and so must be at least a part of the answer. It is beyond any doubt that the fight against cyber crime will continue to be most important and effective at a national level, but there is a clear need to interlink and possibly complement national efforts at the European level.

2.3. Objectives

The overall strategic objective of the proposed policy, based on the problems identified above, can be summarized as follows:

To strengthen and better coordinate the fight against cyber crime at national, European and international level

This overall strategic objective can be divided into the following five strategic level objectives, presented in a tentative order of priority:

- To improve operational cross-border law enforcement actions against cyber crime in general and against serious forms of cyber crime in particular, and to improve exchange of information, intelligence and best practices between law enforcement agencies in Member States and beyond

- To identify and create operational instruments for cooperation and common goal-setting between the public and the private sector and to improve the exchange of information, intelligence and best practices for the fight against cyber crime between the public and the private sector at EU level

- To establish a political platform and structures for the development of a consistent EU Policy on the fight against cyber crime, in cooperation with the Member States and competent EU and international organisations, and to make existing legal and institutional frameworks more effective, also by clarifying responsibilities and liabilities for all relevant actors

- To meet the growing threat from serious forms of cyber crime by promoting skills, knowledge and technical tools; including actions to strengthen relevant training and research

- To raise overall awareness of the threat of cyber crime, especially among consumers and other vulnerable groups of potential victims

3. STRATEGIC POLICY OPTIONS

Any policy for the fight against cyber crime will, due to the nature of the subject-matter, be of a multi-faceted nature. To be truly effective, the police must combine traditional law enforcement activities with other instruments, such as self-regulatory elements and the setting up of structures for cooperation between different stakeholders. A number of problem areas and strategic objectives for the present initiative have been presented above. To reach these objectives, a number of different and combined actions are needed. The Commission has, on the basis of the extensive consultations undertaken, formulated four general policy options, each of them consisting of a number of specific actions:

3.1. General policy option 1: Status quo/no major new action at all

This option would mean that no general horizontal action is taken in this field by the Commission now. This would imply that:

- The Commission would continuously assess the need for targeted legislation or policy action and take appropriate action when needed

- The Commission would follow existing EU and international structures projects against cyber crime

- The Commission would continue to initiate new projects in targeted fields of interest for the fight against cyber crime, but would not take any horizontal policy initiative

3.2. General policy option 2: General legislation

This option would mean that a policy to gradually propose a general regulatory framework for the fight against cyber crime is adopted. Such a policy would imply that:

- The Commission would systematically propose harmonized or unified crime definitions, especially for the EU but also at the international level

- The Commission would propose common minimum standards for criminalization and penalties in the EU

- Formal platforms for the area of public-private cooperation as well as the area of training and research would be created

- A formal law enforcement network would be created

3.3. General policy option 3: Creation of informal cyber crime and public-private networks

This option would mean that the Commission, alone or together with other institutions, would formally set up networks or expert groups of cyber crime experts, and combine this action with the introduction of a voluntary security certification scheme for operators, producers and consumers. This would imply that:

- An informal body of law enforcement cyber crime experts would be set up

- An informal platform/network of public and private cyber crime experts would be set up

3.4. General policy option 4: A coherent strategic approach

This option would mean that a coherent strategy for the fight against cyber crime is introduced at EU-level. The main feature would be the setting up of a strategic framework for the EU-level policy against cyber crime, with the general objective of achieving a better guidance on concrete actions and an optimization of existing means. Other important operational features of this strategy would be:

- An improved EU-level law enforcement cooperation

- The introduction of a strategic structure for public-private cooperation against cyber crime

- The promotion of the establishment of a framework for global international cooperation in the relevant field

- Targeted legislative measures when this is needed

4. ASSESSMENT OF POLICY OPTIONS AND CHOICE OF POLICY OPTION

4.1. Assessment

The general policy options were assessed on the basis of the following criteria:

- Social impacts
- Economic impacts
- Costs for public administration
- Degree of coherence with policy objectives
- Added value and respect of the subsidiarity principle
- Feasibility

The conclusions of the assessment were, in brief:

4.1.1. General policy option 1

It was considered that this option would clearly not be enough in relation to existing challenges. The impacts of the "no new action" option are in principle limited, but it is difficult to assess whether there is a risk of this option leading to a significant impact as the future types of crime are by definition not known. The potential long-term negative impact of a "no new action" scenario is very high, taking into account the current and growing importance of this type of crime.

4.1.2. General policy option 2

The conclusion was that this policy option could only be pursued very carefully and in the long-term perspective. Detailed legal feasibility studies and long political negotiations would be necessary. The impacts of this option may be very important, but in view of the small likelihood of making real progress in the short term, this option becomes uncertain in the short term perspective. It can also be questioned whether the policy objectives would met as effectively at the level of the actual implementation of the policy actions as they are at a political and theoretical level. Should this policy option prevail, the risk would be that the operational level of fight against cyber crime would not be sufficiently involved in strategic political choices and decisions. Considering the important, associated impacts, the role of the Commission in this respect would also need to be clarified. It could possibly also be claimed that similar results could be achieved with less penetrating measures.

4.1.3. General policy option 3

This policy option was assessed as being very interesting from a strategic point of view, even if the added value and the concrete impacts are hard to foresee. The risk is that the new network structures would achieve few concrete results. The Commission should be ideally

placed for coordinating self-regulatory actions in the relevant field but, in the framework of this policy option, more in the role of coordinator and facilitator that that of strategic leader.

4.1.4. General policy option 4

It was considered that this policy option presents a number of most relevant strategic level actions. Very few negative impacts or major obstacles can be discerned. On the negative side, it could be argued that the direct impacts of the policy are rather modest. This however only goes for the short term perspective; very important impacts may follow when adequate implementation measures are taken. The resulting concrete impacts however remain hard to foresee in detail, since the strategic level will have to be implemented operationally at a later stage. All impacts will be assessed then.

It should again be underlined that the direct impacts of the proposed strategies are limited, and that specific actions undertaken later within the framework of one of these strategies will be assessed separately at that point. This means that the assessment made now is of preliminary nature.

4.2. Choice of policy option

The analysis has clearly pointed at option 4 as the best alternative. Option 4 is also clearly the option which best responds to the general objectives indicated in Section 2.4 above.

The option to take no action at all in this field does not seem to be viable. A passive approach would be likely to result in numerous bilateral cooperation projects on the fight against cyber crime continuing to exist without any possibility to take advantage of a horizontal exchange of best practices or synergy effects. General legislation to create new EU bodies, to harmonize crime definitions and to clarify responsibilities and liabilities of all stakeholders could be interesting, but an analysis of the political situation has clearly shown that proposals for general and horizontal legislation would stand very small chances to be adopted. Furthermore, very few of the stakeholders consulted believed that this can be the most important priority now. General legislation may however still be of relevance in a long-term perspective. The creation of new informal structures for the EU-level law enforcement or public-private cooperation might also be a good idea in a long term perspective, but all stakeholders seem to agree that the existing structures are sufficient, even if they urgently need to be made more effective. As a result of the analysis, the preference has thus been given to option 4, "a coherent strategy". It should be noted that that option does not exclude that a formal structure is created (option 3) or that general legislation (option 2) is adopted later. The preferred option does in fact mean that the doors for new actions are held open.

The preparatory analysis and the discussions held clearly show that the "coherent strategy" is the option which is most likely to achieve the strategic objectives of the policy. Such a strategy is likely to have significant positive impacts on the fight against cross-border cyber crime, since the competencies and roles of all involved in the fight will be clarified and strengthened. It would also contribute to a better dialogue and understanding between the public and private sectors, which in turn could have many positive side effects. From an economic point of view, the preferred option may lead to important synergy effects, decreased level of harm from criminal activities and decreased costs for individual security programmes.

It is however likely that it will take a few years for the expected effects under the chosen option to materialise. It is thus hard to assess all its potential impacts now. This is even more

the case since the concrete details of the policy remain to be decided. It will thus be necessary to assess the specific impacts of concrete elements of the policy at a later stage.