COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.5.2007
SEC(2007) 642

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

IMPACT ASSESSMENT REPORT

{COM(2007) 267 final}
{SEC(2007) 641}

Lead DG:

Justice, Freedom and Security

Commission Legislative Work Programme reference:

2007/JLS/010

1. PROCEDURAL ISSUES AND CONSULTATION OF INTERESTED PARTIES

1.1. Background

After the last Commission Communications on network and information security[1] and cyber crime[2] were adopted in 2001, the use of the Internet has exploded, 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 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.

The Commission adopted two Communications on security and privacy in the Information society in May[3] and November[4] 2006 respectively. Those Communications and other prevention oriented documents have been taken into account in the present Impact Assessment and in the initial planning for the Communication on the fight against cyber crime. It is hard to draw an exact dividing line between the area of network and information security and the area of fight against cyber crime, since no effective crime repression policy can be established without an effective prevention and general security policy supporting it, and vice versa. However, to be brief, it can be considered that this cyber crime communication and its impact assessment build on a criminal law enforcement perspective and therefore concentrate principally, but not exclusively, on third pillar issues.

The assessment of problem areas and the possible policy options presented in this Impact Assessment are based on extensive formal and informal consultations with experts and other stakeholders, mainly - but not exclusively - inside Europe.

During the consultation process it became clear that there is not much data or statistics available. This is due to many factors, but especially to the cross-border and global character of cyber crime, the difficulty to establish that such crimes have taken place and the lack of reporting of such crimes. A true picture of cyber crime incidents in Europe is

---

1 Communication on Network and Information Security: Proposal for an EU policy approach - COM(2001) 298.

2 Communication on enhancing creating a Safer Information Society by improving the security of information infrastructures and combating computer related crime - COM(2000) 890.

3 Communication on a strategy for a Secure Information Society – "Dialogue, partnership and empowerment" - COM(2006) 251.

4 Communication on Fighting spam, spyware and malicious software - COM(2006) 688.

thus very hard to establish. Little statistical data is available and existing data gives a rather disparate picture of the situation at EU-level. The preparations for this report already at an early stage made it clear that no quantitative method could be used and that the only method available to assess the impacts would consist in a qualitative consultation of stakeholders. The lack of quantitative data is due to the fact that cyber crime incidents are rarely reported to law enforcement authorities. In particular companies that have been victims of such crimes fear negative impacts if knowledge of the vulnerability of their information and communication technology systems becomes public.

This lack of data (and details on the current state of national legislations) was thus one of the main reasons why the Commission in 2006 decided to order a study from an external contractor. This external study[5], which was established in the period July-October 2006, constitutes the main support for this impact assessment report. The problems and objectives assessed were defined by the contractor in close consultation with the Commission and on the basis of a desk analysis of appropriate analytical methods and applicable legal documents. The core of the study was carried out through numerous interviews with relevant stakeholders (i.e. European Commission officials, law enforcement bodies, national prosecutors, Internet service providers, Internet security providers, specialists and companies facing specific risks, network and information security associations, public and private cyber crime experts, civil organisations, universities and consumer associations). Subsequently, the Commission services have informally consulted different stakeholders and especially Member States experts[6] in order to confirm the conclusions made in the external study. These consultations confirmed that there is a global consensus among practically all stakeholders regarding the EU needs in this field. Although there is a lack of reliable and quantifiable data, the consultations thus provided a sufficient evidence base for identifying problems and corresponding objectives, and assessing available policy options.

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 report will thus principally deal with strategic policy choices. Part of the strategic options that will be assessed are more specific, operational actions, which are not in all cases of relevance for immediate policy purposes, but could fit into the strategy in a longer term perspective.

1.2. State of play: presentation of existing instruments

For the purpose of this Impact Assessment, the following legislative and non-legislative measures have especially been analysed, particularly in relation to possible "gaps" which will be discussed below. It should be underlined that the list below only described the most important instruments. Many other relevant legal and other acts exist, and can be of relevance for the Commission policy against cyber crime.

---

5 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).

6 Such as the members of the Europol High Tech Crime Experts group.

The **Council of Europe Convention on cyber crime**[7] (hereafter: the CoE Convention) is no doubt the most important and comprehensive international instrument in this field, but its significance depends also on its application as it has by 1 March 2007 entered into force only in ten Member States[8] and nine non EU Member States. The CoE Convention aims to facilitate international cooperation, detection, investigation and prosecution of cyber crime and calls for establishing a common basis for substantive- and procedural law and for jurisdiction. The objectives of the policy outlined in this report will complement and not duplicate what has already been decided through the Convention. It should be underlined that the Convention only covers a number of specific legal and procedural questions, whereas the planned EU anti-cyber crime policy will cover cyber crime from a global perspective.

In comparison with the CoE Convention, the **Framework Decision on Attacks against Information Systems**[9] places emphasis rather on approximation of criminal law improving cooperation between judicial and other authorities, calling for the use of existing networks of operational points.

The **Framework Decision on combating terrorism**[10] currently does not contain direct references to cyber terrorism, but can be of relevance.

The **Council Decision to Combat Child Pornography on Internet**[11] calls Member States to promote and facilitate investigation and prosecution, to encourage internet users to report to competent authorities, to use the existing points of contact, to cooperate with Europol and Interpol and also to build up dialogues with the industry.

The **Directive on Electronic Commerce**[12] is important concerning issues of responsibility as it excludes any obligation of network operators to monitor the information they transmit or store. **The Directive on privacy and electronic communications**[13], besides containing provisions on spam, envisages also an obligation for service providers to take measures to safeguard security and to inform users in case of particular risk of breach of security of the network. **The Directive on the retention of data**[14] is particularly relevant for the purpose of prevention, investigation, detection and prosecution of criminal offences as it ensures at EU level that certain data, in the course of the supply of communications services, are retained for a certain period of time.

---

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

8 Bulgaria, Cyprus, Denmark, Estonia, France, Hungary, Lithuania, the Netherlands, Romania and Slovenia.

9 Framework Decision on attacks against information systems (2005/222/JHA).

10 Framework Decision on combating terrorism (2002/475/JHA).

11 Council Decision of 29 May 2000 to combat child pornography on the Internet (2000/375/JHA).

12 Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce in the Internal Market.

13 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

14 Directive 2006/24/EC on the retention of data generated of processed in connection of the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

All the instruments just presented, including the CoE Convention, have in common that they cover only some aspects of the fight against cyber crime. The initiative discussed in the present report aims at a more strategic and horizontal perspective, covering the whole range of the cyber crime problem area.

1.3. The Impact Assessment Board

On 9 March 2007, the Impact Assessment Board of the European Commission delivered an opinion regarding a preliminary version of this Impact Assessment report. In the opinion, the Board in brief stated that:

- A more focused analysis should be presented of the problem, objectives and policy options, giving particular attention to the justification for EU action and providing a realistic picture of its likely added value
- The definition of problems and objectives should be clarified, ranked and focused
- The presentation of policy options should be simplified and strengthened as regards the subsidiarity and value added aspects
- A clearer discussion of economic and social impacts was advisable

The present version of the Impact Assessment report has been completely restructured and significantly redrafted, with a view to taking these recommendations fully into account. However, the recommendation to rank the objectives has only been followed to the extent possible. The objectives of this policy are very closely connected to each other and not interchangeable; a ranking between them can thus only be of tentative character.

2. PROBLEM DEFINITION

2.1. Overall problem

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. The new sector also contributes considerably to economic growth in many areas in Europe. 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 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.

In section 2.2 below, eight strategic problem areas will be used in order to explain the overall problem more in detail. 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.

2.2. Strategic problem areas in detail

2.2.1. The growing vulnerability to cyber crime risks for society, business and citizens

The importance of the internet is growing as companies and organisations are interlinked and become more and more depending on communication systems, especially the internet. Due to new spam techniques and enlarged spam volumes and to other new phenomena such as phishing, botnets, malware, theft of codes and of different personal information, insecurity has increased and the level of trust has been reduced. The fight against cyber crime is one of the most important factors in the efforts to strengthen security, but also one of the most difficult. Besides the difficulties of discovering crimes and the cross-border nature of cyber crime, the determination of the competent jurisdiction and applicable law, the cross-border enforcement and the recognition and use of electronic evidence enhances difficulties to prevent and prosecute crime.

It can be assumed that the continuously enhanced globalisation and interoperability of information systems will make the cyber environment even more vulnerable, although new security techniques and strategies may also complete the picture in compensating for this increased vulnerability.

2.2.2. An increased frequency and sophistication of cyber crime offences

The lack of information on cyber crime in Member States makes it difficult or even impossible to identify and quantify the crime level. The external study mentioned above has given some indicative data only. In the absence of reliable global statistics, the following general indicative trends in cyber crime can however be discerned:

- New sophisticated techniques are increasingly used by criminals
- Cyber crime attacks are more and more often targeted at specific groups of victims
- Crimes, particularly fraud, are increasingly often committed with the help of identity thefts and phishing[15]
- The most serious threat lately seems to be the appearance of so called botnets, which make it possible to, for example, infect a large number of computers in order to use a whole network to commit crimes at a large scale
- A trend towards more organised crime on the Internet, focused only on financial profit, has been observed

As an indicative example of the increased frequency in one particularly serious form of crime, the publication of child sexual abuse material, it should be underlined that 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.

[15] Phishing signifies attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.

2.2.3. The lack of a coherent EU-level policy and legislation for the fight against cyber crime

As EU integration continues, the need for better coordination of criminal policies is accentuated. This is true in particular for the field of fight against cyber crime. All Member States have national policies against cyber crime or certain aspects of cyber crime. There are also different multinational projects to interconnect these policies. These projects often concern particular aspects of the problem area, such as the fight against child pornography or the fight against illegal trade. Despite the existence of organs and structures such as the Europol High Tech Crime group, it can not be claimed that an elaborated coherent horizontal policy in Europe on the fight against cyber crime exists. A continuing situation of uncoordinated policies in Europe would increase the problem by leading to fragmented anti cyber-crime actions, a state of affairs which could potentially be exploited by criminals.

The risk that criminals would exploit differences between Member States is even more concrete when it comes to differences in legislation. Criminals may choose to set up shop in a country in which a specific activity is punished more mildly or is not even criminalized. In view of studying this problem, a preliminary analysis of **legal gaps** in and between Member States has been carried out through the external study, but the analysis of this very complex issue must be deepened before any final conclusions can be drawn. The analysis has been done on the basis of the CoE Convention, which is probably the most comprehensive legal act that exists in this field.

In this context, it should be noted that to date, two different approaches have been applied to the definition of cyber crime. The first approach considers only computer- or network-specific crimes. The second approach includes also computer- or network-related crimes, thus covering also traditional crimes committed with the support of a computer or over a network. According to the first approach, legislation needs to include only computer- or network-specific crimes because non- computer- or network-specific crimes are often sufficiently covered by the provisions against traditional crimes. The second approach deems necessary the adoption of specific provisions for computer- or network-related crimes, taking into account the principle prohibiting the interpretation of penal law through analogy, and demanding a precise definition of acts that are considered to be crimes. When legal gaps between Member States are analyzed, this difference in approaches must be kept in mind. In view of the rapid evolution of cyber crime and the increase in the different types of cyber crimes that are being perpetrated, it is important to consider a development of a categorisation of cyber crimes that finds the right balance between these two approaches.

Regarding the *substantive legislation*, there is a constant need to monitor crime definitions in order to make sure that they are still valid, considering the quick technology changes and new emerging crime types. Definitions need to be as technology neutral as possible. One example is the notion of "*computer system*" in the CoE Convention, which has given rise to some problems such as the exclusion, according to the case-law in some states, from the sphere of application, of mobile telephones or other wireless technology. In the Framework Decision 2005/222/JHA, the notion "*information system*", which should be more technology neutral, has been used instead. Considerable general differences between Member States still exist in formal crime definitions. It is however hard to make any conclusion on the basis of this, since the lack of explicit

legislation does not always mean that there is no law (in the form of case-law or other non codified regulation). For example in many Member States computer *fraud and forgery* fall under traditional terms of criminal law, and no specific legislation is then considered to be needed.

A specific problem concerns *identity theft*, which is often used as an instrument to commit crimes. In many Member States, identity theft as such is not criminalised, which may lead to considerable problems in cross-border law enforcement and judicial cooperation. It has also been confirmed by stakeholders that the legal means to fight identity theft before another crime is committed are, partly for this reason, limited. It should be considered that identity theft is the core activity of many cyber crimes, and that cyber criminals find it relatively easy to steal identities.

Generally speaking national legislations are rarely uniform, or even close to harmonized, regarding *content-related offences.*

Specific *procedural measures* are provided by the CoE Convention, such as preservation of stored computer data, production order, search and seizure of stored computer data, or real-time collection of computer data, but the Convention has not been ratified by all Member States, and the majority of them still apply general procedural provisions to cyber crimes. Many stakeholders have underlined a need for European procedural rules defining types of data, modalities to preserve and produce evidence.

The conclusion would be that many differences exist between legislations within the EU and that this may cause a problematic situation in Europe.

2.2.4. Specific difficulties in operational law enforcement cooperation regarding cyber crime

The fight against cyber crime often implies a need to act very quickly against a criminal activity. Criminals may often change web addresses, Internet services providers or user names, especially when there is a risk of intervention from law enforcement authorities. If the criminal activities are to be stopped, there is thus often a clear need of extremely rapid action and information exchange, often border-crossing. The current procedures for intra-European and international law enforcement cooperation are not adapted to the fight against cyber crime in this respect. It should be noted that the difficulties in this context are not a result of EU integration, but rather of intrinsic cross-border technologies and the general impact of globalization. The borders of the EU are very seldom the borders of cyber crime activities.

As a consequence of the technical evolution, criminals are now using with fast networks allowing them to commit crimes over different national judicial territories in a very short period of time and also to eliminate evidence, just as quickly. Due to the cross border nature of cyber crime, criminals can also easily obtain significant comparative advantages in relation to law enforcement authorities. In addition to the fact that cyber criminals do not have to be present physically while committing the crime, weak or nonexistent legislation or a lack of law enforcement specialists on cyber crimes can give criminals an advantage. Law enforcers also have the problem of getting used to continuous new forms of crime, of handling the increasing number of cases and of reacting quickly within the national jurisdiction as well as across other jurisdictions.

The pressure on the system is enhanced by the time consuming procedures that are necessary to access data, to separate relevant from irrelevant data and to secure electronic evidence. The procedures which law enforcers need to use to get relevant information are also perceived to be much too slow. As an example, the fact that law enforcement in one country can not directly contact a network operator in another state, even though a crime in their own state may have been committed via the foreign operator, makes work very difficult.

There are a number of organisations and mechanisms, such as Interpol, the G8 and Council of Europe 24/7 contact points, Europol, CEPOL and Eurojust, which are dealing with trans-border crimes. Theoretically, international cyber crime could be handled by these bodies. However, experience shows that this does not often happen. It would thus seem that good structures exist, but that they are not used in anything close to an optimal way.

2.2.5. The need to develop competence and technical tools: Training and research

The fast evolution in cyber criminality means that there is also a situation of increased need for training at all concerned levels. It should be noted that there is a global need for training of the entire population, but the present point of focus will be on analysing training needs for law enforcement and judicial authorities. Due to the fact that technology is changing extremely quickly, there is an obvious need for continuous training not only for specialised units, but also for any police officer, judge or prosecutor who could be confronted with cyber crime activities. The cross-border character of cyber crime makes it easy for criminals to move their activities from one state to another at short notice. Criminal activities may be moved to states considered to have weak law enforcement in this area. Already for this reason, there is a clear European interest in making sure that law enforcement authorities in all Member States are sufficiently trained to meet the cyber crime threat.

Closely linked to the training issue is the need to build on and take forward relevant research in this area. In particular the development of technological tools to trace criminals and victims and to prevent or stop criminal cyber activities need to be promoted.

2.2.6. The lack of a functional structure for cooperation between important stakeholders in the public and the private sector

Industry has often shown a very positive attitude towards assisting public authorities in the fight against cyber crime, but the public authorities are very often not aware of programmes and actions run by the private sector, which could in fact serve as an important support to traditional law enforcement and crime prevention activities. There are very few initiatives in Europe to centralise existing information platforms.

Public authorities and law enforcement are also not always informed of criminal attacks against private companies. Private sector operators are often, in order to protect business models and secrets, reluctant to report or share information on crime incidences with law enforcement authorities. However, such information is needed if the public authorities are to be able to formulate an efficient and well-adjusted anti-crime policy. The willingness of companies to report criminal incidents may be linked to the fact of

whether or not police officers make an official case out of each report they receive, or to the fact that the perception is such that police cannot follow-up on reported crimes anyhow.

One other main problem regarding the fight against cyber crime is the lack of adequate statistics. Individual users do not report incidents, because often they are not aware of the attack, do not care about it, do not know where and how to report or simply they do not want to inform authorities. Nonetheless, it is important to note that the analysis conducted has shown that companies in general do appreciate the advantages of better exchanges of information. Indeed, raising customer awareness can enable the consumers to protect themselves more effectively, or to better accept the needs as well as the cost and possible inconveniences of higher protection. Information on victims may also highlight security problems in certain sectors, which in turn may improve policy and legislation makers' understanding of the need to protect those particular sectors.

It should be noted that there is a generally satisfactory operational cooperation between network operators and web hosts and law enforcement bodies concerning closing down of web sites, especially those containing child pornography, and the blocking of crime-related communication between specific users. In spite of the lack of clear provisions on shutting down sites, network operators frequently close down such web pages on their own initiative. In many cases cyber crimes and criminals can hardly be detected unless the private sector cooperates with law enforcement authorities. There is thus a public interest in having network operators taking an active part in investigations and in legal proceedings. The role of network operators is especially important in relation to blocking specific web sites with illegal content or which are used to support botnets, as they are in a special position regarding communications on the Internet. It should also be noted that investigations are often pursued by private companies, without the knowledge of the authorities.

It can thus be stated, as a conclusion, that a clear and urgent need and scope for improvement of the cooperation between the public and the private sector in this field has been identified. An effective programme for the fight against cyber crime can only be truly effective if it includes a strategy for cooperation between the public sector, especially law enforcement authorities, and private sector operators. For this, an atmosphere of trust and confidence is needed.

2.2.7. Unclear system of responsibilities and liabilities

A specific issue regarding both possible EU legislation and EU public-private relations in the fight against cyber crime concern the responsibilities and liabilities of different actors in cyber space. The lack of clear responsibilities of all actors has been identified as a problem area in Europe. Even if the fight against cyber crime is the object of this report, it should be noted that repression is not possible without prevention, and that prevention is indeed the top priority in terms of efficiency. Setting clear responsibilities for all actors in the cyber world would represent enormous advantages for all those involved, whether they are victims or law enforcers and prosecutors. Four main categories of actors could be considered: (1) end users, (2) providers of services directly linked to Internet, (3) providers of e-services and (4) manufacturers of hardware or software tools etc. Network operators, in particular, have a clear technical capacity to identify and prevent a large

number of cyber crime offences, but also manufacturers of software could make their products crime proof.

2.2.8. The lack of awareness of the risks emanating from cyber crime

The financial and social risks emanating from cyber crime attacks can be enormous. It appears that these risks are not known widely enough or are partly neglected. This is also due to the reluctance to report crime (referred to in section 2.2.6). The lack of reliable data and statistics[16] is likely to contribute to lack of awareness of the risks emanating from cyber crime, especially among particularly vulnerable potential victims, such as small companies, organisations and individual citizens. There is a general need to better protect all users of electronic information systems, and this can mainly be done if awareness of existing risks is enhanced. Campaigns should especially be directed towards consumers and other identified potential vulnerable victim groups. It is however important that awareness raising programmes do not undermine the trust and confidence of consumers and users by focusing only on negative aspects of security.

2.3. 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. As an example, it would seem that phishing and other tools used to commit fraud crimes appear to be used in a more targeted fashion against more vulnerable potential victim groups, such as very young persons or small companies with less developed financial control mechanisms. An effective anti cyber crime policy could thus have clear beneficial effects for these groups. In the short term, the main public stakeholders of an EU level policy against cyber crime would be all authorities with an anti-cyber crime programme, *ie* mainly law enforcement authorities.

2.4. 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.

The EU actions discussed in this impact assessment report will not go beyond what is required and what is clearly adding value at the EU-level. Already the limited EU legal competence in this field implies that the main feature of all planned EU actions in the

[16] Proposals for an improved framework for collection of data can be found in the Communication on a strategy for a Secure Information Society – Dialogue, partnership and empowerment - COM(2006) 251.

short term will be of a coordinating nature. The fight against cyber crime will also in the future primarily be a responsibility of Member States, and the scale of EU intervention will remain limited. However, the benefits of EU-level coordination in this field should not be underestimated. Operational law enforcement work against cross-border criminal activities would be considerably facilitated and a more structured exchange of information and best practices could provide a clear added value for national law enforcement bodies. Such efforts could also create synergies and, in turn, add a clear value also at EU level. The intrinsic international and cross-border character of cyber crime is proof enough that actions are needed both at global international and at EU-level. The Commission, fully respecting the subsidiarity principle, is ideally placed to coordinate such actions, in close cooperation with Member States and other international organisations. It should again be underlined that the EU level policy can at this point in time only be a supplement to national and other international policies. A reinforced EU coordination should mainly be regarded as a limited but nevertheless very important contribution to the national and global actions against cyber crime.

The policy to be outlined in this report will include a number of future and more concrete actions, including the organisation of conferences, the setting up of formal or informal networks, as well as legislation. Those future actions will be assessed in time, in order to certify that they add value at EU-level before they are undertaken. In the same way, the legal bases for these actions will be defined later after a close study of the content of the particular actions.

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 six 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, while avoiding to undermine the trust and confidence of consumers and users by focusing only on negative aspects of security

An EU policy against cyber crime would need to include all these strategic objectives, since they are closely interlinked and could hardly be followed separately in an effective way. The priority order tentatively set out above thus only has a limited validity. All policy options discussed in the present report will thus be attempts to address all these objectives.

4. STRATEGIC POLICY OPTIONS

4.1. Formulation of 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.

There are many possible ways to address the problems described above. The Commission services have considered a number of concrete actions, which are complementing each other rather than constituting completely separate alternatives. These policy options are presented in more detail in the preparatory external study. In order to choose a concrete coherent policy for the next few years, a policy which will be presented in a Communication planned for adoption in 2007, the objectives set out above have resulted in four "option packages" (hereafter: general policy options), each including a number of specific potential actions.

All of these general policy options, except the first one ("status quo"), include elements which will contribute to all of the objectives presented in section 3 above. In brief, the second option concentrates on the setting up of a regulatory framework and new formal structures, the third looks at informal and self-regulatory networks and action, whereas the fourth general policy option is a combination of regulatory and informal measures. The options packages have been discussed with public and private external stakeholders, who have in general agreed on the choices proposed in this report.

4.2. The four general policy options

4.2.1. 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 continue to play its role as policy initiator and propose legislation when needed, but no horizontal strategy for this activity in the area of fight against cyber crime would be launched.

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

The Commission would continue to actively participate in the European efforts to strengthen network and information security. It would also continue to actively follow external work, for example in the Council of Europe or in the G 8 Roma-Lyon High Tech Crime Group.

- 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

The Commission would also in the future support different projects through its financial programmes, especially the programme "Prevention of and Fight against crime".

4.2.2. 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 is already active in this area; although only with regard to specific single crimes. As an example of efforts to harmonize crime definitions, the Framework Decision on Attacks against cyber crime can be mentioned. No global strategy to generalise this effort has however existed. The action suggested would mean that actions to achieve harmonized or unified crime definitions in the whole field of fight against cyber crime would be undertaken.

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

The Commission is already active in this area, in basically the same way as described above regarding harmonized and unified crime definitions. No global strategy to make this effort general has however existed. The action suggested would mean that actions to achieve minimum standards of criminalization and minimum penalties in the whole field of fight against cyber crime in the EU would be undertaken.

- Generally applicable rules on responsibilities and liabilities - in particular rules imposing legal obligations for network operators, producers and consumers to take specific security measures to fight cyber crime - would be proposed

The Commission would in this case consider strengthening the obligation for the network operators to remove or to disable access to the information when they are aware or have knowledge of illegal activity or information.

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

The Commission would in this case propose or take a formal decision to set up a specific public-private platform. This formalized structure, which could take the form of networks or expert groups, would be provided with their own rules of procedure, and would also deal with awareness raising issues.

- A formal law enforcement network would be created

The Commission would in this case propose or take a formal decision to set up a new body dealing permanently with EU coordination of the operational fight against cyber crime. Training and research issues would also be handled by this body. A continuous analysis of potential legal gaps and EU legislative needs could also be within the remit of the group, which could be given the competence to formulate recommendations.

4.2.3. General policy option 3: Creation of informal cyber crime and public-private networks, combined with the setting up of voluntary schemes for certification of products and services at different levels

This option would mean that the Commission, alone or together with other institutions, would formally set up networks or expert groups of cyber crime. This would imply that:

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

The Commission would, through the organisation of regular dedicated meetings, set up an informal network of law enforcement experts. The network would be asked to informally coordinate operational law enforcement activities and of creating a informal coordination points all over Europe, dealing also with areas such as exchange of information and best practices as well as training and research issues in the very specific field of fight against cyber crime. The network could build on, and coordinate with, existing structures, such as the Europol High Tech Crime or the Council of Europe/G 8 24/7 network. The network would thus also be in contact with international partners.

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

The Commission would set up or contribute to the setting up of an informal but permanent platform of law enforcement experts as well as private sector network and information security experts. The network would complement the network mentioned in the point above and the two networks should be closely coordinated. In particular, the network would have the task of creating models for the exchange of sensitive non-personal information between the sectors. It could also be linked to public and private actors in neighbouring countries.

4.2.4. 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

This would in particular include actions to improve exchange of information and best practices between Member States, training for law enforcement and judicial authorities (with the possible setting up of a permanent EU training platform and the increased use of existing and future financing programmes to support multi-national training initiatives in the field of fight against cyber crime), awareness raising campaigns among law enforcement personnel and support for relevant research. Expenditures for existing coordinating instruments in the EU would be increased.

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

The Commission would take a pro-active role in networking and the setting up of public-private task forces and working groups, which would be given the task of addressing common cyber crime problems. These efforts would also contribute to an atmosphere of confidence, facilitating common goal-setting.

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

The Commission would take action to strengthen global international cooperation. Efforts should be made both to make existing instruments, such as those developed by the Council of Europe and G 8, more effective, and to develop new instruments or cooperation structures. Efforts would also be made to make existing international instruments more efficient.

- Targeted legislative measures when this is needed

The need for new legislation would be continuously assessed. In the short term, rules on a minimum penal legislation on identity theft would be proposed. Reflections on the possibility to introduce additional rules on responsibilities and liabilities would also be launched by the Commission. In the longer term, further legislation with a view to harmonising relevant criminal and criminal procedural law, both within the EU and internationally, would remain an objective.

5. ASSESSMENT OF POLICY OPTIONS

The general policy options have been assessed on the basis of a number of set criteria (see below). 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. It should also be noted

that the view has been taken that the anti-cyber crime policy actions examined will not have any noticeable environmental impact; that issue will thus not be assessed.

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

5.1.1. Social impacts

The main direct consequences of a "no new action" scenario regarding law enforcement would be that law enforcement authorities and prosecutors would continue to encounter important problems in cooperating effectively across borders and that cyber criminals could continue to actively exploit these differences between jurisdictions and possibly actively seek out “free havens”. The fight against cyber crime and especially prevention efforts would thus continue to be fragmented and no horizontal approach aiming at finding synergies and structures for horizontally exchanged information and best practices would be established. Anti-cyber crime activities in the EU would risk an emerging internal incoherence. As regards relevant training and research, the situation would continue to be fragmented, with different, uncoordinated initiatives.

No global initiative to interlink public and private efforts to fight cyber crime would be achieved. Public authorities would continue to lack sufficient information on what is done in the private sector, which would reduce the possibilities to formulate an adequate policy in this field. The global responses to cyber crime from all legal actors would continue to be fragmented.

The absence of a horizontal legislative strategy could contribute to increasing the risk of a continuing or even growing legal uncertainty at EU-level. Existing and emerging gaps in legislation and differences in Member States' legislation would lead to a continuous and sometimes even growing legal insecurity for potential cyber crime victims.

The lack of any horizontal initiative would also produce a clear risk of a growing feeling of insecurity in the EU. This could also affect the further development of Information Society industry - and thereby also the employment market - negatively. The position of vulnerable potential crime victim groups, such as consumers and small companies, would also risk being weakened, especially when new cyber crime phenomena emerge.

5.1.2. Economic impacts

The "no new action" option would not produce any direct economic impacts. However, there are clear indications that the costs resulting from cyber crime are already high for industry citizens and society in general. These costs would continue to be high or increase. It could thus be argued that this option is expensive, in that the present state of lack of coordination and unclear responsibilities probably increases costs at all levels in society. Growing disparities in legislation – due to new crime phenomena leading to even more disparate legislation in Member States – could also create additional administrative burdens for all stakeholders. In particular multinational private sector operators would have to carry increased costs if they had to adapt to completely different legislation in each Member State in which they are active.

5.1.3. Costs for public administration

No new costs would occur for public administrations.

5.1.4. Degree of coherence with policy objectives

This general option would only meet the objectives outlined in section 3 above to a lesser degree.

5.1.5. Added value and respect of the subsidiarity principle

No new action that could add value would be taken. It should be recalled, however, that this option leaves the door open for continued targeted activities, but the added value of such activities would need to be assessed separately.

5.1.6. Feasibility

A "no new action" option is obviously feasible from a theoretical point of view. However, a decision not to take any horizontal action in this field would risk strong political criticism already in the near future. As regards the lack of a horizontal legislative policy, there are very important, sometimes insoluble, political and legal problems surrounding any attempt to achieve common categorization of crime definitions or harmonised definitions, and a no new action policy would for this reason possibly be the most feasible solution.

5.1.7. Conclusion

Due to the reasons explained below, 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

5.2. General policy option 2: General legislation

5.2.1. Social impacts

As regards harmonized or unified crime definitions and common minimum standards for criminalization and penalties, one social impact would be the general improvement of legal certainty and increased likelihood of covering all types of cyber crime. Cross-border operational and jurisdictional cooperation would also be facilitated considerably. A negative social impact linked to this option could possibly be perceived regarding the general political atmosphere (see feasibility below). A more uniform law would possibly fail to take regional and cultural specificities into account.

5.2.2. Economic impacts

This policy option could produce a considerable economic impact in the long perspective. A higher degree of legal certainty may provide important advantages on the Information Society market, which could be economically advantageous for all stakeholders. Filling existing legal gaps would improve the potential of repression, which would strengthen the prevention side. This, in turn, could result in considerable positive economic impacts in society. At the same time, the introduction of a number of new

European legal measures, in particular as regards responsibilities and liabilities, might however also entail a significant implementation costs for companies.

5.2.3. Costs for public administration

There are no direct costs associated with this option. The indirect costs connected to the preparation and implementation of new legislation could be substantial. These costs would need to be separately assessed later, depending on the specificities of every single proposal for new legislation.

5.2.4. Degree of coherence with policy objectives

A common legal framework would facilitate intra EU and international operational cooperation. On the basis of the framework, a functional public-private cooperation, relevant training and specific awareness raising campaigns could also be achieved. This general option would no doubt also permit the creation of a truly consistent EU policy with a more effective legal and institutional framework. From a theoretical standpoint, this general policy option is thus fully consistent with the objectives set out.

5.2.5. Added value and respect of the subsidiarity principle

All general legislative initiatives in this field would add a clear European value in that a common European regulatory framework would be established. This would have clear positive impacts for the Internal market, and thereby also for the economic development of the sector in question. The legal security of all stakeholders and the protection of consumers and other potential victims would also clearly be strengthened. On the other hand, it can be questioned whether such a general initiative would not go too far with regard to the subsidiarity principle. It is true that every single legislative proposal would have to be assessed in relation to this principle, but it is possible that the general strategy as such would need to be adjusted in order to be consistent with subsidiarity requirements.

5.2.6. Feasibility

The feasibility is open to question, as a significant resistance both from Member States and from private sector operators can be expected. The main barrier against this type of legislation may be the difficulty in formulating a penal law which is in accordance with national legal practices and traditions. A risk to criminalise non-damaging activities, by failing to take regional specificities into account, also exists. However, if the general strategy were adjusted at the political level, it cannot be excluded that a solution can be found in the long term, especially considering the importance of the problem.

5.2.7. Conclusion

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. However, it should be kept in mind that many legislative proposals are already under way at EU level in areas related to network and information security. One example is the review of the Regulatory Framework for electronic communications which might result in amendments to the security-related provisions of the ePrivacy Directive 2002/58/EC and the Universal Service Directive 2002/22/EC.

5.3. General policy option 3: Creation of informal cyber crime and public-private networks, combined with the setting up of voluntary schemes for certification of products and services at different levels

5.3.1. Social impacts

The social impact of the setting up of a law enforcement network would be high, as this would in the long run certainly increase the number of EU-wide joint operations and prosecutions against cyber criminals. A secondary effect of this could possibly be a slow tendency to further adapt national laws to suit EU harmonisation. The positive impacts for law enforcers and prosecutors would be significant, helping to eliminate many restrictions on international cooperation between law enforcers and prosecutors across the EU. Resources would thus be used more efficiently in the repression process.

Subsequently, an increased level of security would in particular have positive effects on the protection of potential victim groups and the further development of Information Society industry. A negative effect could be that new structures could add confusion to the EU situation, insofar as the role of already existing bodies would become more unclear.

The creation of a public-private network could also possibly have important social impacts of the same sort as those just described. Impacts to be considered could be better coherence inside the EU, improved prevention, better awareness, higher efficiency in repression and higher level of trust in e-commerce. In addition, an atmosphere of cooperation, common goal-setting and mutual confidence between all stakeholders – in the private as well as in the public sector – could be achieved. This, in turn, could lead to important synergies and a more effective global strategy in the fight against cyber crime.

5.3.2. Economic impacts

The economic impact is linked mainly with the efficiency of law enforcement and prosecution. A likely decrease in cyber crime will entail fewer economic losses for internet users, increase the trust in the internet by those users and thus entail higher revenues for businesses with activities on the internet. Consumers would also be better protected. The negative economic impact, if any, would be negligible.

5.3.3. Costs for public administration

Costs for public administrations would be fairly moderate. The European Union would finance the different networks, but the costs could be limited to the organisation of a few

meetings a year and some administrative support. The establishment of two networks could possibly be co-financed by the private sector.

5.3.4. Degree of coherence with policy objectives

The general policy option would meet the objectives regarding operational law enforcement cooperation and public-private structures very well. This would probably also contribute to making existing legal and institutional frameworks more effective. It can also be assumed that the objectives regarding promoting skill, knowledge and risk awareness would be met through the work of the different networks described. Since these networks would be rather flexible and informally organised, it could however be questioned whether the objective of pursuing a consistent EU policy would be met in an optimal way through this policy option.

5.3.5. Added value and respect of the subsidiarity principle

The setting up of both networks would clearly add European value. It should however be underlined that the system as well as the networks will only operate in the European environment, and not replace similar instruments at national level. The Commission will in any case take action in this field only if, and insofar as, the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. It is open to question whether formal expert groups are required and if the need could in reality not be covered by less formal structures.

5.3.6. Feasibility

The setting up of the two networks is probably easy to achieve. It could however take considerable efforts to make them operational and make sure that they add concrete value.

5.3.7. Conclusion

This policy option looks 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.

5.4. General policy option 4: A coherent strategic approach

5.4.1. Social impacts

As regards EU-level law enforcement cooperation, positive impacts of some importance are expected for the coordination of investigations and prosecutions, the efficiency of the system and the reduction of the time needed to complete the cases. As the scope would be the EU, to the extent that Member States believe that a part of the problem of cyber crime is better dealt with at an EU level than at the national level, the efforts to bring these measures about will be less cumbersome than similar measures to bring about global cooperation or harmonisation of laws. The impact will however again mainly be

on cyber crime operations within the EU. Therefore there is a risk that criminal activities would shift outside the EU, but continue to target crime victims in the EU. The impact of operational cooperation in individual cases would be high, as this could be expected to significantly increase the number of prosecutions against cyber criminals. Such cooperation could fall within the remit of Europol, Eurojust and CEPOL, and demand efforts which are limited to these institutions. As concerns EU-level relevant training and research, the impacts would firstly touch upon law enforcers and prosecutors, who would gain in competence and knowledge. The measure would eventually contribute not only to more harmonisation and cooperation inside the EU, but also to better international cooperation.

The social impacts relating to private companies, which take part in the public-private networks and conferences, are not easy to predict. It is however beyond doubt that private and public sector, network operators and law enforcement, would benefit considerably in terms of exchange of information and best practices and assist each other in countering illegal activities, especially in the fight against illegal content on the Internet. In the longer term, this could contribute to strengthening the protection of potential victims and the Information Society industry.

If existing international instruments were used more effectively, this could have enormous positive impacts on the repression of cyber crime in the countries concerned, within the EU as well as outside. Positive impacts could be expected especially with regard to the collaboration between EU and non-EU law enforcers and prosecutors. One negative side effect that can be envisaged is that criminal organizations may move away from countries cooperating with the EU and set up shop in other countries further away, but at international level the option does not imply negative impacts for cooperating countries. An increased level of security could be the overall result, which could in particular have positive effects on the protection of potential victim groups and the further development of Information Society industry.

The social impact of targeted legislation, well assessed and adapted to concrete needs, would probably only be positive in that more legal certainty is achieved. In addition, more extensive and possibly burdensome legislation regarding cyber crime could be avoided.

5.4.2. Economic impacts

The economic impact of a strengthened EU-level law enforcement cooperation is expected to be positive both for the EU and its neighbouring area and at global level, as a decrease in cyber crime would entail fewer losses for internet users, increased trust in the internet by those users and thus higher revenues for businesses with activities on the internet. Few negative economic impacts can be foreseen, with the possible exception of negative economic impacts for countries located outside the EU neighbouring area, as criminal activities may move there as a result. Indeed, it could entail more efficiency regarding investments made in EU bodies, which would be better valorised. With specific regard to the objective of strengthening existing structures, the present institutions may only be able to play a more pro-active role if their financial and human resources are increased. If this measure is not well implemented and financed, it could have the negative impact that these institutions would lose their focus on other policy areas which fall under their remit.

The potential positive economic impact of an EU training and/or research initiative could be significant and cover various dimensions. It would especially help to valorise investments and make them sustainable and to improve knowledge in law enforcement bodies and in the judicial system. The exact economic impact of the initiative is not easy to define as it will be quite indirect, for example through increased efficiency of law enforcement processes and a more efficient split in resource utilisation between the private and public sector for an equivalent result.

Economic impacts of actions to increase EU-level public-private cooperation are hard to predict and must be studied further. The costs of the preliminary study and the costs of institutionalizing information sharing and assembling statistics from different national data bases would certainly be high. On the other hand, if more information could be gathered successfully and if patterns of cyber crime could be identified, this would certainly help in curbing costs emanating from cyber crime.

The strategy to introduce targeted and well assessed legislation could lead to a situation where the possibilities to concentrate efforts on where they are really needed would be increased. This would in turn reduce costs in general. The risk that too many efforts are made at a horizontal level - at the cost of possible concrete and effective projects at a sector-specific, national or regional level - would be minimized.

5.4.3. Costs for public administration

The first direct costs for public administrations incurred would be for increased financial resources which might have to be made available for EU-level cooperation structures and training programmes. Another cost which public administrations might incur would be linked to a study needed in order to understand the factors which until now prevented existing institutions deploying their full powers with pro-active initiatives, and taking relevant measures. There are not likely to be other costs for the public sector, or for other stakeholders.

The cost of the concrete actions, which would be decided at a later stage within the framework of the strategy, would have to be assessed separately at that time, when the concrete actions have been defined in detail. It could however be assumed that the direct costs for public administrations for this option would continue to be limited.

5.4.4. Degree of coherence with policy objectives

This general policy option would fully meet all strategic objectives set out in section 3 above.

5.4.5. Added value and respect of the subsidiarity principle

Coordination of cross-border law enforcement as well as public-private cooperation would add a clear European value, by spreading knowledge of best practices and by making sure that resources are well used. The limited legislation which will be part of this policy will only be proposed if such an added value can clearly be established. The Commission, in cooperation with Member States and other partners, is well placed to coordinate this policy. It will in any case take action in this field only if, and insofar as, the objectives of the proposed action cannot be sufficiently achieved by the Member

States, either at central, regional or local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. The implementation of certain actions may however be taken at national, sectoral or regional level. The added value of any concrete action subsequent to the adoption of the strategy will be assessed separately.

5.4.6. Feasibility

The success of this general policy option also depends mainly on the willingness of Europol, Eurojust and CEPOL to take on more responsibility in the area of cyber crime, and on Member States to accept that these institutions do indeed get more responsibility. The feasibility appears to be high; existing instruments have already been accepted by Member States and an overwhelming majority of stakeholders would certainly welcome this policy option. Efforts to strengthen public private cooperation and EU and international cooperation in general would also, it seems, be generally acceptable. The political possibility to adopt targeted legislation to support this policy, for example by strengthening Europol, is not assessed in this report. Some resistance can be expected from some Member States and from some national law enforcement bodies and prosecutors, as the criminal domain is still considered part of the "core" of the national culture.

5.4.7. Conclusion

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.

5.5. Choice of policy option

Already a preliminary analysis, on the basis of the assessments made here above and opinions expressed during the Commissions' own informal and formal stakeholder consultations, 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 objective of making Europe more secure with respect to the cyber crime threat. 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.

6. DATA PROTECTION AND FUNDAMENTAL RIGHTS ISSUES

A number of the options mentioned above could affect fundamental rights, such as the right to respect for private and family life and the right to data protection. When the exact conditions of implementations of preferred options have been settled, an assessment of the impacts of these options with respect to fundamental rights should thus be done.

The Commission is of the opinion that the options presented above, if implemented correctly, would in principle not have a negative impact on fundamental rights. It can however not be excluded that negative effects could occur, depending on the specific modalities and conditions of the implementation. The Commission is taking this risk seriously and will make sure 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. Any legislative action which will be taken in the framework of this policy will be scrutinised for compatibility with the Charter of Fundamental Rights, in accordance with the Commission Communication on the compliance with the Charter in Commission legislative proposals adopted in 2005 - COM(2005) 172.

7. THE PREFERRED POLICY OPTION: THE MAIN ASPECTS OF THE POLICY AND IMPACTS

The option consisting of a coherent strategy on the fight against cyber crime has thus been chosen. This strategy will give the European Commission a central coordinating role in Europe. With regard to its limited competence in this field, it is clear that the

Commission will play this role only when a clear added value can be established. 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:

7.1. Improved European law enforcement cooperation

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 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.

7.2. 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 effective 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.

7.3. 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.

7.4. 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 effective 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.

8. MONITORING AND EVALUATION

In order to measure progress made in the strategy for the fight against cyber crime described above, it is necessary to follow-up and monitor the process. This is also needed in order to decide whether legislative measures, which would be more general in nature, would be more appropriate than the instruments suggested here.

The preferred option discussed above is an EU strategy mainly consisting of reinforced dialogue and cooperation networks. The success of such actions is by its nature very hard to measure, but this is also due to the limited competences at the EU level. Most work against cyber crime will still be carried out at the national level and the specific effects of EU action will be hard to define and measure. One part of the strategy, however, consists of a number of actions planned to be taken in the period 2007-2009. The Commission will assess how these actions have been implemented and report to the Council and the Parliament in 2010.

Depending on the outcome of discussions at the conferences foreseen in 2007 and developments in the field of fight against cyber crime, the Commission may also decide to propose new legislative or other targeted actions. Specific impact assessments such actions will then be carried out as appropriate.

As for the global strategy, the following preliminary set of key indicators could be considered:

- The number of successful meetings and conferences organised in the relevant area
- The quantified and qualitatively perceived change in exchanged strategic information in this field between national law enforcement authorities
- The quantified and qualitatively perceived change in exchanged strategic information in this field between the public and the private sector