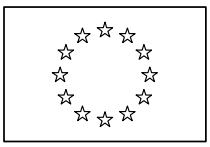

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 22.5.2007
COM(2007) 267 final

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

{SEC(2007) 641}
{SEC(2007) 642}

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

1. INTRODUCTION

1.1. What is cyber crime?

The security of the increasingly important information systems in our societies covers many aspects, of which the fight against cyber crime is a core element. Without an agreed definition of cyber crime, the terms "cyber crime", "computer crime", "computer-related crime" or "high-tech crime" are often used interchangeably. For the purpose of this Communication, 'cyber crime' is understood as "criminal acts committed using electronic communications networks and information systems or against such networks and systems".

In practice, the term cyber crime is applied to three categories of criminal activities. The first covers **traditional forms of crime** such as fraud or forgery, though in a cyber crime context relates specifically to crimes committed over electronic communication networks and information systems (hereafter: electronic networks). The second concerns the publication of **illegal content** over electronic media (i.a. child sexual abuse material or incitement to racial hatred). The third includes **crimes unique to electronic networks**, i.e. attacks against information systems, denial of service and hacking. These types of attacks can also be directed against the crucial critical infrastructures in Europe and affect existing rapid alert systems in many areas, with potentially disastrous consequences for the whole society. Common to each category of crime is that they may be committed on a mass-scale and with a great geographical distance between the criminal act and its effects. Consequently the technical aspects of applied investigative methods are often the same. These commonalities will form the focus of this Communication.

1.2. Latest developments in cyber crime

1.2.1. In general

The combination of constantly evolving criminal activities and a lack of reliable information makes it difficult to obtain an exact picture of the current situation. Nevertheless, some general trends can be discerned:

- The number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised[1]

- Clear indications point to a growing involvement of organised crime groups in cyber crime

[1] The majority of this Communication's statements on current trends have been taken from the Study to assess the impact of a communication on cyber crime, ordered by the Commission in 2006 (Contract No JLS/2006/A1/003).

- However, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase

1.2.2. Traditional crime on electronic networks

Most crimes can be committed with the use of electronic networks, and different types of fraud and attempted fraud are particularly common and growing forms of crime on electronic networks. Instruments such as identity theft, phishing[2], spams and malicious codes may be used to commit large scale fraud. Illegal national and international Internet-based trade has also emerged as a growing problem. This includes trade in drugs, endangered species and arms.

1.2.3. Illegal content

A growing number of illegal content sites are accessible in Europe, covering child sexual abuse material, incitement to terrorist acts, illegal glorification of violence, terrorism, racism and xenophobia. Law enforcement action against such sites is extremely difficult, as site owners and administrators are often situated in countries other than the target country, and often outside the EU. The sites can be moved very quickly, also outside the territory of the EU, and the definition of illegality varies considerably from one state to another.

1.2.4. Crimes unique to electronic networks

Large scale attacks against information systems or organisations and individuals (often through so called botnets[3]) appear to have become increasingly prevalent. Also, incidents with systematic, well co-ordinated and large-scale direct attacks against the critical information infrastructure of a state have recently been observed. This has been compounded by the merging technologies and accelerated interlinking of information systems, which rendered those systems more vulnerable. Attacks are often well organised and used for purposes of extortion. It can be assumed that the extent of reporting is minimised, in part due to the business disadvantages which may be the result if security problems were to become public.

1.3. Objectives

In the light of this changing environment, there is an urgent need to take action – at national as well as European level – against all forms of cyber crime, which are increasingly significant threats to critical infrastructures, society, business and citizens. Protection of individuals against cyber crime is often exacerbated by issues related to the determination of the competent jurisdiction, applicable law, cross-border enforcement or the recognition and use of electronic evidence. The essentially cross-border dimension of cyber crime highlights such difficulties. In addressing these threats, the Commission is launching a general policy initiative to improve European and international level coordination in the fight against cyber crime.

The objective is to strengthen the fight against cyber crime at national, European and international level. Further development of a specific EU policy, in particular, has long been recognised as a priority by the Member States and the Commission. The focus of the initiative

---

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

[3] Botnet refers to a collection of compromised machines running programs under a common command.

will be on the law enforcement and criminal law dimensions of this fight and the policy will complement other EU actions to improve security in cyber space in general. The policy will eventually include: improved operational law enforcement cooperation; better political cooperation and coordination between Member States; political and legal cooperation with third countries; awareness raising; training; research; a reinforced dialogue with industry and possible legislative action.

The policy on the fight and prosecution of cyber crime will be defined and implemented in a manner fully respecting fundamental rights, in particular those of freedom of expression, respect for private and family life and the protection of personal data. Any legislative action taken in the context of this policy will be first scrutinised for compatibility with such rights, in particular the EU Charter of Fundamental Rights. It should also be noted that all such policy initiatives will be carried out in full consideration of Articles 12 to 15 of the so called e-commerce Directive[4], where this legal instrument applies.

The objective of this Communication can be divided into three main operational strands, which can be summarised as follows:

- To improve and facilitate coordination and cooperation between cyber crime units, other relevant authorities and other experts in the European Union

- To develop, in coordination with Member States, relevant EU and international organisations and other stakeholders, a coherent EU Policy framework on the fight against cyber crime

- To raise awareness of costs and dangers posed by cyber crime

2. EXISTING LEGAL INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME

2.1. Existing instruments and actions at EU level

The present Communication on cyber crime policy consolidates and develops the 2001 Communication on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime[5] (hereafter: the 2001 Communication). The 2001 Communication proposed appropriate substantive and procedural legislative provisions to deal with both domestic and trans-national criminal activities. From this, several important proposals followed. In particular, these include the proposal leading to the Framework Decision 2005/222/JHA on attacks against information systems[6]. In this context, it should also be noted that other, more general, legislation covering also aspects of the fight against cyber crime has been adopted, such as the Framework Decision 2001/413/JHA on combating fraud and counterfeiting of non-cash means of payment[7].

---

4 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ L 178, 17.7.2000, p. 1).

5 COM(2000) 890, 26.1.2001.

6 OJ L 69, 16.3.2005, p. 67.

7 OJ L 149, 2.6.2001, p. 1.

The Framework Decision 2004/68/JHA on sexual exploitation of children[8] is a good example of the particular focus put by the Commission on the **protection of children**, especially in relation to the fight against all forms of child sexual abuse material illegally published using information systems, a horizontal priority which will be kept in the future.

To tackle security challenges for the information society, the European Community has developed a three-pronged approach for network and information security: specific network and information security measures, the regulatory framework for electronic communications and the fight against cyber crime. Although these three aspects can, to a certain extent, be developed separately, the numerous interdependencies call for tight coordination. In the related field of Network and Information security, a 2001 Commission Communication on Network and Information Security: A proposal for an EU policy approach[9], was adopted in parallel to the 2001 communication on cyber crime. The ePrivacy directive 2002/58/EC lays down an obligation for providers of publicly available electronic communication services to safeguard the security of their services. Provisions against spam and spyware are also laid down there. The Network and Information security policy has since been developed through a number of actions, most recently in Communications on a Strategy for a secure Information society[10] that sets out the revitalized strategy and provides the framework to carry forward and refine a coherent approach to Network and Information security, and on Fighting spam, spyware and malicious software[11], and in the 2004 creation of ENISA[12]. The main objective of ENISA is to develop expertise to stimulate cooperation between the public and private sectors, and provide assistance to the Commission and Member States. **Research results** in the area of technologies to secure information systems will also play an important role in the fight against cyber crime. Accordingly, Information and Communication Technologies as well as Security are all mentioned as objectives in the EU Seventh Research Framework Programme (FP 7), which will be operational during the period 2007-2013[13]. The review of the regulatory framework for electronic communications might result in amendments to to enhance the effectiveness of the security-related provisions of the ePrivacy Directive and the Universal Service Directive 2002/22/EC[14].

2.2. Existing international instruments

Due to the global nature of information networks, no policy on cyber crime can be effective if efforts are confined within the EU. Criminals can not only attack information systems or commit crimes from one Member State to another, but can easily do so from outside the EU's jurisdiction. Accordingly, the Commission has actively participated in international discussions and cooperation structures, i.a. the G 8 Lyon-Roma High-Tech Crime Group and Interpol-administered projects. The Commission is in particular closely following the work of the network for 24-hour contacts for International High-Tech Crime (the 24/7 network)[15], of which a considerable number of states worldwide, including most EU Member States, are

---

8 OJ L 13, 20.1.2004, p. 44.
9 COM(2001) 298.
10 COM(2006) 251.
11 COM(2006) 688.
12 Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (OJ L 77, 13.3.2004, p. 1).
13 The European Union has already under the 6th Framework Programme for Research and and Technological development supported a number of relevant, and successful, research projects.
14 COM(2006) 334, SEC(2006)816, SEC(2006) 817.
15 See Article 35 in the Council of Europe Convention on cyber crime.

members. The G8 network constitutes a mechanism to expedite contacts between participating states, with 24-hour points of contact for cases involving electronic evidence, and those requiring urgent assistance from foreign law enforcement authorities.

Arguably, the predominant European and international instrument in this field is the Council of Europe's 2001 Convention on cyber crime[16]. The Convention, which was adopted and entered into force in 2004, contains common definitions of different types of cyber crime and lays the foundation for a functioning judicial cooperation between contracting states. It has been signed by many states, including the United States of America and other non-European states, and by all Member States. A number of Member States have however not yet ratified the Convention or the additional protocol to the Convention dealing with acts of racist and xenophobic nature committed through computer systems. Considering the agreed importance of the Convention, the Commission will encourage Member States and relevant third countries to ratify the Convention and consider the possibility for the European Community to become a party to the Convention.

3. FURTHER DEVELOPMENT OF SPECIFIC INSTRUMENTS IN THE FIGHT AGAINST CYBER CRIME

3.1. Strengthening operational law enforcement cooperation and EU-level training efforts

The lack, or underutilisation, of immediate structures for **cross-border operational cooperation** remains a major weakness in the area of Justice, Freedom and Security. Traditional mutual assistance when confronted with urgent cyber crime cases has proven slow and ineffective, and new cooperation structures have not yet been sufficiently developed. While national judicial and law enforcement authorities in Europe cooperate closely via Europol, Eurojust and other structures, there remains an obvious need to strengthen and clarify responsibilities. Consultations undertaken by the Commission indicate that these crucial channels are not used in an optimal way. A more coordinated European approach must be both operational and strategic and also cover the exchange of information and best practices.

The Commission will in the near future lay particular emphasis on **training** needs. It is an established fact that the technological developments produce a need for continuous training on cyber crime issues for law enforcement and judicial authorities. A reinforced and better coordinated financial support from the EU to multinational training programs is therefore envisaged. The Commission will also, in close cooperation with Member States and other competent organs such as Europol, Eurojust, the European Police College (CEPOL) and the European Judicial Training Network (EJNT), work to achieve an EU level coordination and interlinking of all relevant training programmes.

The Commission will organise a **meeting** of law enforcement experts from Member States, as well as from Europol, CEPOL and the EJTN, to discuss how to improve strategic and operational cooperation as well as cyber crime training in Europe in 2007. Among other things, the creation of both a permanent EU contact point for information exchange and an

[16] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

EU cyber crime training platform will be considered. The 2007 meeting will be the first in a series of meetings planned for the near future.

3.2. Strengthen the dialogue with industry

Both private and public sectors have an interest in jointly developing methods to identify and prevent harm resulting from the activities of crime. Shared private and public sector participation, based on mutual trust and a common objective of harm reduction, promises to be an effective way of enhancing security, also in the fight against cyber crime. The public-private aspects of the Commission's cyber crime policy will in time be part of a planned global EU policy on dialogue between the public and the private sector, covering the whole area of European security. This policy will in particular be taken forward by the European Security Research and Innovation Forum, which the Commission plans to create shortly and which will regroup relevant stakeholders from the public and the private sector.

The development of modern information technologies and electronic communication systems is largely controlled by private operators. Private companies carry out threat assessments, establish programmes for the fight against crime and develop technical solutions to prevent crime. Industry has displayed a very positive attitude to assisting public authorities in the fight against cyber crime, especially in efforts to counter child pornography[17] and other types of illegal content on the Internet.

Another issue concerns the apparent lack of exchange of information, expertise and best practices between the public and the private sector. Private sector operators are often, in order to protect business models and secrets, reluctant, or are under no clear legal obligation, to report or share relevant information on crime incidences with law enforcement authorities. However, such information may be needed if public authorities are to formulate an efficient and appropriate anti-crime policy. The possibilities to improve cross-sector information exchange will be considered also in the light of existing rules on protection of personal data.

The Commission already plays an important role in various public-private structures dealing with cyber crime, such as the Fraud Prevention Expert Group[18]. The Commission is convinced that an effective general policy for the fight against cyber crime must also include a strategy for cooperation between the public sector and private sector operators, including civil society organisations.

To achieve broader public-private cooperation in this field, the Commission will in 2007 organise a conference for law enforcement experts and private sector representatives, especially Internet Service Providers, to discuss how to improve public-private operational cooperation in Europe[19]. The conference will touch upon all subjects deemed to add value for both sectors, but especially:

---

17 One recent example of cooperation in this field is the cooperation between law enforcement and credit-card companies, through which the latter have assisted the police in tracking down purchasers of online child pornography.

18 See http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 The Conference could be regarded as the continuation of the EU Forum presented in Section 6.4 in the computer-crime communication.

- Improving operational cooperation in the fight against illegal activities and content on the Internet, specifically in the areas of terrorism, child sexual abuse material and other illegal activities particularly sensitive from a child protection perspective

- Initiating public-private agreements aiming at the EU-wide blocking of sites containing illegal content, especially child sexual abuse material

- Devising a European model for the sharing of necessary and relevant information across the private and public sectors, one consideration being to cultivate an atmosphere of mutual confidence and take the interests of all parties into account

- Establishing a network of law enforcement contact points in both private and public sectors

3.3. Legislation

General harmonisation of crime definitions and national penal laws in the field of cyber crime, is not yet appropriate, due to the variety of the types of offences covered by this notion. Since effective cooperation between law enforcement authorities often depends on having at least partly harmonised crime definitions, it remains a long-term objective to continue harmonising Member States' legislation[20]. With regard to certain key crime definitions, an important step has already been taken with the Framework Decision on attacks against information systems. As described above, new threats have subsequently appeared and the Commission is closely following this evolution given the importance of continuously assessing the need for additional legislation. The monitoring of the evolving threats is closely coordinated with the European Programme for Critical Infrastructure Protection.

Targeted legislation against cyber crime should however also be considered now. A particular issue which may require legislation relates to a situation where cyber crime is committed in conjunction with **identity theft**. Generally, "identity theft" is understood as the use of personal identifying information, e.g. a credit card number, as an instrument to commit other crimes. In most Member States, a criminal would most likely be prosecuted for the fraud, or another potential crime, rather than for the identity theft; the former being considered a more serious crime. Identity theft as such is not criminalised across all Member States. It is often easier to prove the crime of identity theft than that of fraud, so that EU law enforcement cooperation would be better served were identity theft criminalised in all Member States. The Commission will in 2007 commence consultations to assess if legislation is appropriate.

3.4. Development of statistical data

It is generally agreed that the current state of information concerning the prevalence of crime is largely inadequate, and in particular that much improvement is needed to compare data between Member States. An ambitious five-year plan to tackle this problem was set out in the Communication from the Commission on *Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006 – 2010*[21]. The Expert Group set up under this Action Plan would provide a suitable forum for developing relevant indicators for measuring the extent of cyber crime.

---

[20] This longer-term objective has already been mentioned on page 3 of the 2001 Communication.

[21] COM(2006) 437, 7.8.2006.

4. THE WAY FORWARD

The Commission will now take the general policy for the fight against cyber crime forward. Due to the limited powers of the Commission in the field of criminal law, this policy can only be a complement to the actions undertaken by Member States and other bodies. The most important actions – each of which will imply the use of one, several or all of the instruments presented in Chapter 3 – will also be supported through the Financial Programme "Prevention of and Fight against Crime":

4.1. The fight against cyber crime in general

- Establish a strengthened operational cooperation between Member States' law enforcement and judicial authorities, an action which will begin with the organisation of a dedicated expert meeting in 2007 and which may include the setting up of a central EU cyber crime contact point

- Increase financial support to initiatives for improved training of law enforcement and judicial authorities vis-à-vis the handling of cyber crime cases and take action to coordinate all multinational training efforts in this field by the setting up of an EU training platform

- Promote a stronger commitment from Member States and all public authorities to take effective measures against cyber crime and to allocate sufficient resources to combat such crimes

- Support research beneficial to the fight against cyber crime

- Organise at least one major conference (in 2007) with law enforcement authorities and private operators, especially to initiate cooperation in the fight against illegal Internet activities in and against electronic networks and to promote a more effective non-personal information exchange, and to follow-up on the conclusions from this 2007 conference with concrete public-private cooperation projects

- Take the initiative for and participate in public-private actions aimed at raising awareness, especially among consumers, of the cost of and dangers posed by cyber crime, while avoiding the undermining of the trust and confidence of consumers and users by focusing only on negative aspects of security

- Actively participate in and promote global international cooperation in the fight against cyber crime

- Initiate, contribute to and support international projects which are in line with the Commission policy in this field, e.g. projects run by the G 8 and consistent with the Country and Regional Strategy Papers (regarding cooperation with third countries)

- Take concrete action to encourage all Member States and relevant third countries to ratify the Council of Europe's Cyber Crime Convention and its additional protocol and consider the possibility for the Community to become a party to the Convention

- Examine, together with the Member States, the phenomenon of co-ordinated and large scale attacks against the information infrastructure of member states in view of preventing

and combating these, including co-ordinating responses, and sharing information and best practices

4.2. Fight against traditional crime in electronic networks

- Initiate an in-depth analysis with a view to preparing a proposal for specific EU legislation against identity theft

- Promote the development of technical methods and procedures to fight fraud and illegal trade on the Internet, also through public-private cooperation projects

- Continue and develop work in specific targeted areas, such as in the Fraud Prevention Expert Group on the fight against fraud with non-cash means of payment in electronic networks

4.3. Illegal content

- Continue to develop actions against specific illegal content, especially regarding child sexual abuse material and incitement to terrorism and notably through the follow-up of the implementation of the Framework Decision on sexual exploitation of children

- Invite the Member States to allocate sufficient financial resources to strengthen the work of law enforcement agencies with special attention to identifying the victims of sexual abuse material which is distributed online

- Initiate and support actions against illegal content that may incite minors to violent and other serious illegal behaviour, i.a. certain types of extremely violent on-line video games

- Initiate and promote dialogue between Member States and with third countries on technical methods to fight illegal content as well as on procedures to shut down illegal websites, also with a view to the possible development of formal agreements with neighbouring and other countries on this issue

- Develop EU-level voluntary agreements and conventions between public authorities and private operators, especially Internet service providers, regarding procedures to block and close down illegal Internet sites

4.4. Follow-up

In this Communication, a number of actions aimed at improving cooperation structures in the EU have been outlined as next steps. The Commission will take these actions forward, assess progress on the implementation of the activities, and report to the Council and Parliament.