EN

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, xxx
COM(2000) 890 final

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

Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime



Summary

Europe's transition to an information society is being marked by profound developments in all aspects of human life: in work, education and leisure, in government, industry and trade. The new information and communication technologies are having a revolutionary and fundamental impact on our economies and societies. The success of the information society is important for Europe's growth, competitiveness and employment opportunities, and has far-reaching economic, social and legal implications.

The Commission launched the *e*Europe initiative in December 1999 in order to ensure that Europe can reap the benefits of the digital technologies and that the emerging information society is socially inclusive. In June 2000, The Feira European Council adopted a comprehensive *e*Europe Action Plan and called for its implementation before the end of 2002. The Action Plan highlights the importance of network security and the fight against cybercrime.

Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct. These criminal activities may take a large variety of forms and may cross many borders. Although, for a number of reasons, there are no reliable statistics, there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society. Some recent examples of denial of service and virus attacks have been reported to have caused extensive financial damage.

There is scope for action both in terms of preventing criminal activity by enhancing the security of information infrastructures and by ensuring that the law enforcement authorities have the appropriate means to act, whilst fully respecting the fundamental rights of individuals.

The European Union has already taken a number of steps to fight harmful and illegal content on the Internet, to protect intellectual property and personal data, to promote electronic commerce and the use of electronic signatures and to enhance the security of transactions. In April 1998, the Commission presented to the Council the results of a study on computer-related crime (the so-called 'COMCRIME' study). In October 1999, the Tampere Summit of the European Council concluded that high-tech crime should be included in the efforts to agree on common definitions and sanctions. The European Parliament has also called for commonly acceptable definitions of computer-related offences and for effective approximation of legislation, in particular in substantive criminal law. The Council of the European Union has adopted a Common Position on the Council of Europe cybercrime convention negotiations and has adopted a number of initial elements as part of the Union's strategy against high-tech crime. Some EU Member States have also been at the forefront of relevant G8 activities.

This Communication discusses the need for and possible forms of a comprehensive policy initiative in the context of the broader *Information Society* and *Freedom, Security and Justice* objectives for improving the security of information infrastructures and combating cybercrime, in accordance with the commitment of the European Union to respect fundamental human rights.

In the short-term, the Commission believes that there is a clear need for an EU instrument to ensure that Members States have effective sanctions in place to combat child pornography on the Internet. The Commission will introduce later this year a proposal for a Framework

Decision which, within the wider context of a package covering issues associated with the sexual exploitation of children and trafficking in human beings, will include provisions for the approximation of laws and sanctions.

In the longer-term, the Commission will bring forward legislative proposals to further approximate substantive criminal law in the area of high-tech crime. In accordance with the conclusions of the European Council in Tampere in October 1999, the Commission will also consider the options for mutual recognition of pre-trial orders associated with cybercrime investigations.

In parallel, the Commission intends to promote the creation of specialised computer-crime police units at the national level, where they do not already exist, support appropriate technical training for law enforcement and encourage European information security actions.

At the technical level and in line with the legal framework, the Commission will promote R&D to understand and reduce vulnerabilities and will stimulate the dissemination of know-how.

The Commission intends also to set up an EU Forum in which law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organisations, consumer representatives, data protection authorities and other interested parties will be brought together with the aim of enhancing mutual understanding and co-operation at EU level. The Forum will seek to raise public awareness of the risks posed by criminals on the Internet, to promote best practice for security, to identify effective counter-crime tools and procedures to combat computer-related crime and to encourage further development of early warning and crisis management mechanisms.

INVITATION TO COMMENT ON THIS COMMUNICATION

The European Commission would like to invite comments from all interested parties on the issues addressed in this Communication. Comments may be sent up to 23.03.2001 via e-mail to the following address:

infso-jai-cybercrime-comments@cec.eu.int

Comments will in principle be published on the web, unless the sender explicitly requests the comment not to be published. Anonymous comments will not be published. The Commission reserves the right not to publish comments it receives (e.g., because the comments contain offensive language). Comments will be available via a link at the following website:

http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html

Suggestions as to the technical format and details of the publications policy will be available at this web-site. It is advised to check this site before sending in your comments.

PUBLIC HEARING

The European Commission will also organise a public hearing of interested parties on the issues addressed in the Communication. This hearing will take place on 7.03.2001. Requests for an invitation to submit a statement at this hearing may be sent up to 20.02.2001 via e-mail to the following address:

infso-jai-cybercrime-hearing@cec.eu.int

or by post to the following address:

European Commission
Office BU33-5/9
200 Wetstraat/Rue de la Loi
B-1049 Brussels
Belgium

The European Commission reserves the right to make a selection of parties to be heard. Any selection will be based on the number of requests and the wish to have a wide coverage of interests.

TABLE OF CONTENTS

Summary

1. OPPORTUNITIES AND THREATS IN THE INFORMATION SOCIETY

1.1. National and international responses

2. SECURITY OF INFORMATION INFRASTRUCTURES

3. COMPUTER-RELATED CRIME

4. SUBSTANTIVE LAW ISSUES

5. PROCEDURAL LAW ISSUES

5.1. Interception of communications

5.2. Retention of traffic data

5.3. Anonymous access and use

5.4. Practical co-operation at international level

5.5. Procedural law powers and jurisdiction

5.6. Evidential validity of computer data

6. NON-LEGISLATIVE MEASURES

6.1. Specialised units at the national level

6.2. Specialised training

6.3. Improved information and common rules for record keeping

6.4. Co-operation between the various actors: the EU Forum

6.5. Direct industry actions

6.6. EU-supported RTD projects

7. CONCLUSIONS AND PROPOSALS

7.1. Legislative proposals

7.2. Non-legislative proposals

7.3. Action in other international fora

1. OPPORTUNITIES AND THREATS IN THE INFORMATION SOCIETY

The increasing affordability and use of the Information Society Technologies (ISTs) and the globalisation of the economy are characteristics of our era. Further technological development and growth in use of open networks, such as the Internet, over the coming years will provide major new opportunities and will pose new challenges.

At the Lisbon Summit of March 2000, the European Council stressed the importance of the transition to a competitive, dynamic and knowledge-based economy, and invited the Council and the Commission to draw up an *e*Europe Action plan to make most of this opportunity.[1] This Action Plan, prepared by the Commission and the Council, adopted by the Feira Summit of the European Council in June 2000, includes actions to enhance network security and the establishment of a co-ordinated and coherent approach to cybercrime by the end of 2002.[2]

The information infrastructure has become a critical part of the backbone of our economies. Users should be able to rely on the availability of information services and have the confidence that their communications and data are safe from unauthorised access or modification. The take up of electronic commerce and the full realisation of Information Society depend on this.

The new digital and wireless technologies are already all pervasive. They give us the freedom to be mobile and yet always be connected, connected to a myriad of services built upon networks of networks. They give us the possibility to participate; to teach and to learn, to play together and to work together, to get involved in the political process. As societies though become increasingly reliant on these technologies, effective practical and legal means will have to be employed to help manage the associated risks.

Information Society Technologies (ISTs) can be and are being used for perpetrating and facilitating various criminal activities. In the hands of persons acting with bad faith, malice, or grave negligence, these technologies may become tools for activities that endanger or injure, the life, property or dignity of individuals or damage the public interest.

The classical security approach called for strict organisational, geographic and structural compartmentalisation of information according to sensitivity and category. This is no longer really feasible in this digital world since information processing is distributed, services follow mobile users and interoperability of systems is a prerequisite. Innovative solutions relying on emerging technologies are replacing traditional security approaches. These solutions involve the use of encryption and digital signatures, new access control and authentication tools and software filters of all kinds[3]. Ensuring secure and reliable information infrastructures not only requires a range of technologies but also their correct deployment and effective use. Some of these technologies already exist but often users are either not aware of their existence, of the ways to use them, or of the reasons why they may even be necessary.

---

1 Presidency Conclusions of the Lisbon European Council of 23 and 24 March 2000, available at http://ue.eu.int/en/Info/eurocouncil/index.htm.

2 http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm.

3 Information flows are filtered and controlled at all levels; from the firewall that looks at data packets, through the filter that looks for malicious software, the e-mail filter that discretely eliminates spam, to the browser filter that prevents access to harmful material.

1.1. National and international responses

Computer-related crimes are committed across cyber space and do not stop at the conventional state-borders. They can, in principle, be perpetrated from anywhere and against any computer user in the world. It has been generally recognised that effective action to combat computer-related crime is necessary at both national and international level.[4]

On the national level, comprehensive and internationally oriented answers to the new challenges of network security and computer crime are often still missing. In most countries, reactions to computer crime focus on national law (especially criminal law), neglecting alternative preventive measures.

Despite the efforts of international and supranational organisations, the various national laws world-wide show remarkable differences, especially with respect to the criminal law provisions on hacking, trade secret protection and illegal content. Considerable differences also exist with respect to the coercive powers of investigative agencies (especially with respect to encrypted data and investigations in international networks), the range of jurisdiction in criminal matters, and with respect to the liability of intermediary service providers on the one hand and content providers on the other hand. Directive 2000/31/EC [5] on electronic commerce amends this as regards the liability of intermediary service providers on certain intermediary activities. The Directive also prohibits Member States from imposing such intermediary service providers a general obligation to monitor the information which they transmit or store.

On the international and supranational levels, the need to effectively combat computer-related crime has been broadly recognised and various organisations have been co-ordinating or attempting to harmonise relevant activities. The G8 Justice and Home Affairs Ministers adopted a set of principles and a 10-point action plan in December 1997, which was endorsed by the G8 Birmingham summit in May 1998 and is currently being implemented.[6] The Council of Europe (C.o.E.) started preparing an international convention on cyber-crime in February 1997 and is expected to complete this task in 2001.[7] Combating cybercrime is also on the agenda in bilateral discussions the European Commission has with some governments (apart from the EU). A Joint EC/US Task Force on Critical Infrastructure Protection has been established.[8]

---

4 See, e.g., the *e*-Europe Action Plan at http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm, and statements of European Commissioner Antõnio Vitorino at http://europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-19-09-en_brussels.pdf, and French Prime Minister Lionel Jospin at http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html.

5 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain aspects of Information Society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce").

6 The EU JHA Council on 19 March 1998 endorsed the 10 Principles to combat high-tech crime adopted by the G8 and invited the non-G8 Countries Member States of the EU to arrange for to join the network. Available on European Judicial Network website http://ue.eu.int/ejn/index.htm.

7 The Draft text is available on the web, in two languages, in French : http://conventions.coe.int/treaty/fr/projets/cybercrime.htm. and in English: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

8 Under the auspices of the Joint Consultative Group of the EC/US Science and Technology Co-operation Agreement.

The UN and OECD have also been active in this area, and it is being discussed in international fora such as the Global Business Dialogue and the Trans-Atlantic Business Dialogue.[9]

At the European Union level, until recently, legislative action has mainly taken the form of measures in the fields of copyright, the protection of the fundamental right to privacy and data protection, conditional access services, electronic commerce, electronic signatures and in particular the liberalisation of trade in encryption products, which are indirectly related to computer crime.

A number of important non-legislative measures have also been taken in the last 3-4 years. These include the Action Plan against illegal and harmful content on the Internet which co-finances awareness actions, experiments in rating and filtering of content and hot-lines, and initiatives concerning the protection of minors and human dignity in the information society, child pornography and interception of communications for law-enforcement purposes.[10] The EU has for a long time been supporting R&D Projects which aim at promoting security and trust in information infrastructures and electronic transactions and has recently increased the associated IST Programme budget allocations. Research and operational projects aimed at promoting specialised training of law enforcement personnel as well as co-operation between law enforcement and industry have also been supported in the framework of the Third Pillar Programmes such as STOP, FALCONE, OISIN and GROTIUS.[11]

The Action Plan to combat organised crime, adopted by the JHA Council in May 1997 and endorsed by the European Council of Amsterdam, included a request for a study on computer related crime to be prepared by the Commission by the end of year 1998. This study, the so-called 'COMCRIME study,' was presented by the Commission to the Council Multi-Disciplinary Working Group against organised crime in April 1998.[12] This Communication is partly a follow-up to the JHA Council request.

---

9 The United Nations produced a comprehensive "Manual on the prevention and control of computer-related crime," which has recently been updated. In 1983, the OECD undertook a study of the possibility of an international application and harmonisation of criminal laws to address the problem of computer crime or abuse. In 1986, it published "Computer-Related Crime: Analysis of Legal Policy," a report that surveyed the existing laws and proposals for reform in a number of Member States and recommended a minimum list of abuses that countries should consider prohibiting and penalising by criminal laws. Finally, in 1992, the OECD developed a set of guidelines for the security of information systems, which is intended to provide a foundation on which States and the private sector could construct a framework for the security of information systems.

10 Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity;
Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services; COM(96) 483, October 1996, http://europa.eu.int/en/record/green/gp9610/protec.htm;
Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions –Illegal and harmful content on the Internet (COM(96) 487 final);
Resolution on the Commission communication on illegal and harmful content on the Internet (COM(96)487 - C4-0592/96);
Council Resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 04.11.1996, pp. 1– 6).

11 http://europa.eu.int/comm/justice_home/jai/prog_en.htm.

12 "Legal Aspects of Computer-related Crime in the Information Society – COMCRIME." The study was prepared by Prof. U. Sieber of the University of Würzburg under contract with the European Commission. The final report is available at: http://europa.eu.int/ISPO/legal/en/crime/crime.html.

Before drafting this Communication, the Commission considered it appropriate to undertake informal consultations with representatives from Member States law enforcement and data protection supervisory authorities[13] and from the European industry (mostly ISPs and telecommunications operators).[14]

On the basis of the analysis and the recommendations made by the study, the conclusions drawn from the consultation process, the new possibilities provided for by the Treaty of Amsterdam and the work already accomplished in the EU, the G8 and the C.o.E., this Communication will examine various options for further action by the EU against computer-related crime. On the European Union level the chosen solutions should not lead to any impediment for and fragmentation of the Internal Market, nor to measures which undermine the protection of fundamental rights[15].

2. SECURITY OF INFORMATION INFRASTRUCTURES

In the information society, user-controlled global networks are gradually replacing the older generation of national communication networks. One of the reasons for the success of the Internet is that it has given users access to the very newest technologies. Moore's Law[16] predicts that computing power doubles every 18 months. Communications technology however is developing at an even faster pace.[17] One result of this is that the volume of data carried over the Internet has been doubling in periods of less than a year.

The classical telephone networks were constructed and operated by national organisations. Its users had little choice of services and no control over the environment. The first data networks that were developed were built on the same philosophy of a centrally controlled environment. Security within these environments reflected this.

The Internet and other new networks are very different, and security needs to be handled accordingly. Intelligence and control in these networks is mostly at the periphery, where the users and services are. The core of the network is simple and efficient, and essentially dedicated to the task of transmitting data. There is limited checking or control of content. It is only at the final destination where the bits become the sound of a voice, the image of an x-ray or the confirmation of a bank transaction. Security is therefore to an important extent a responsibility of the users, as only they can appreciate the value of the bits being sent or received, and can determine the level of protection needed.

---

13 At EU level, the data protection supervisory authorities constitute the Article 29 Data Protection Working Party, which is the independent EU advisory body on privacy and data protection, see art. 29 and 30 of Directive 95/46/EC.

14 Two meetings with law enforcement took place on 10.12.1999 and 1.3.2000. A meeting with Internet industry representatives took place on 13.3.2000. A meeting with a small number of personal data protection experts took place on 31.3.2000. A final meeting with all the above took place on 17.4.2000. Minutes of the meetings can be obtained by writing to: European Commission, Unit INFSO/A4, or to: European Commission, Unit JAI/B2, Wetstraat/Rue de la Loi 200, 1049 Brussels, Belgium.

15 EU Charter on Fundamental Rights (http://europa.eu.int/comm/justice_home/unit/charte_en.htm), Article 6 of the TEU and jurisprudence of the European Court of Justice.

16 The observation made in 1965 by Gordon Moore, co-founder of Intel, about the speed at which the density of transistors in integrated circuits was increasing. This density is now approximately doubling every 18 months and this has a direct impact on the price and performance of computer chips. Many experts expect this to hold for at least another decade.

17 The latest technology makes it possible for a single optical fibre cable to simultaneously carry the equivalent of 100 million voice calls.

The user environment is therefore a key part of the information infrastructure. Security techniques have to be implemented there with the permission and participation of the user and according to his/her needs. This is particularly important when one considers the increasing range of activities that people are carrying out from the same terminal. They work and play, they watch television and authorise bank transfers, all from the same device.

Several security technologies are available and new technologies are being developed. The advantages of open source development in terms of security are becoming clearer. Much work has been done on formal methods and on security evaluation criteria. The use of encryption technologies and electronic signatures are becoming indispensable, particularly with the growth in wireless access. An increasing variety of authentication mechanisms is required to meet our different needs in the environments in which we interact. In some environments, we may need or wish to remain anonymous. In others, we may need to be able to prove a certain characteristic while not revealing our identity, such as being an adult or being an employee or a client of a particular company. In yet other situations, it may be necessary to give proof or our identity. Also software filters are becoming ever more sophisticated, and enable us to protect ourselves or those in our care from data we do not want, such as undesirable content, spam mail, malicious software and other forms of attack. The implementation and management of such security requirements within the Internet and new networks also involve considerable expense to industry and users. Therefore it is important to encourage innovation and commercial use of security technology and services.

Naturally, also the shared infrastructure of communication links and name-servers has its security aspects. Data transmission depends on the physical links whereby data is routed from one computer to another. These links have to be put in place and protected in such a way that transmission remains possible in spite of accidents, attacks and an ever increasing volume of traffic. Communication also depends on critical services such as those provided by the name servers, and in particular on the small number of root name servers, that provide the needed addresses. Each of these components will also need appropriate protection, which will vary according to the part of the name space and the user base that is being served.

Driven by the objective of bringing more flexibility and responsiveness to people's needs, information infrastructure technologies have become increasingly complex with often insufficient design effort devoted to security. In addition, this complexity involves more and more sophisticated and interconnected software programmes, which sometimes include weaknesses, security holes, that may easily be exploited for attacks. As cyberspace gets more and more complex and its components more and more sophisticated, new and unforeseen vulnerabilities may emerge.

Several technological mechanisms already exist and new ones are being developed to improve security in cyber-space. The response includes measures:

- To secure critical elements of the infrastructure through the deployment of public-key infrastructures (PKI), the development of secure protocols, etc.

- To secure private and public environments through the development of quality software, firewalls, anti-virus programs, electronic rights management systems, encryption, etc.

- To secure authentication of authorised users, use of smart cards, biometric identification, electronic signatures, role-based technologies, etc.

This calls for an increased effort to develop security technologies, involving co-operation in order to achieve a necessary interoperability between solutions through agreements on international standards.

It is important also that any future conceptual framework for security be an integral part of the overall architecture, addressing threats and vulnerabilities from the outset of the design process. This contrasts with traditional add-on approaches, which have necessarily attempted to plug the holes exploited by an increasingly sophisticated criminal community.

The EU Information Society Technologies (IST) Programme,[18] in particular work relating to information-, and network security, and other confidence-building technologies,[19] provides a framework to develop capability and technologies to understand and tackle emerging challenges related to computer crime. These technologies include technical tools to protect against infringement of the fundamental rights to privacy and personal data and other personal rights and to fight computer crime. In addition, in the context of the IST Programme, a dependability initiative has been launched. This initiative will contribute towards trust and confidence in highly inter-linked information infrastructures and in tightly networked embedded systems by promoting dependability awareness and dependability enabling technologies. An integral part of this initiative is international co-operation. The IST Programme has developed working relationships with DARPA and NSF and has established, in collaboration with the US Department of State, a Joint EC/US Task Force on Critical Infrastructure Protection.[20]

Finally, the implementation of security obligations following in particular from the EU Data Protection Directives[21] contributes to enhancing security of the networks and of data processing.

3. COMPUTER-RELATED CRIME

Modern information and communications systems make it possible to perform illegal activities from anywhere to anywhere in the world at any time. There are no reliable statistics available on the full scale of the computer-related crime phenomenon. The number of intrusions detected and reported up to now, probably under-represent the scope of the problem. Because of limited awareness and experience of system administrators and users, many intrusions are not detected. In addition, many companies are not willing to report cases of computer abuse, to avoid bad publicity and exposure to future attacks. Many police forces do not yet keep statistics on the use of computers and communication systems involved in these and other crimes. However, the number of illegal activities can be expected to grow as computer and network use increases. There is a clear need to gather reliable evidence on the significance of computer-related crime.

In this Communication, computer-related crime is addressed in the broadest sense, as any crime that in some way or other involves the use of information technology. However,

---

[18] The IST Programme is managed by the European Commission. It is part of the 5th Framework Programme, which runs from 1998 to 2002. More information is available at http://www.cordis.lu/ist.

[19] In Key Action 2 - New Methods of Work and Electronic Commerce.

[20] Under the auspices of the Joint Consultative Group of the EC/US Science and Technology Co-operation Agreement.

[21] See Article 4 of Directive 97/66/EC (including also an obligation to inform about remaining security risks) and Article 17 of Directive 95/46/EC.

different views exist on what constitutes "computer-related crime." The terms "computer crime," "computer-related crime," "high-tech crime" and "cybercrime" are often used interchangeably. A difference can be made between computer specific crimes and traditional crimes performed with the aid of computer technology. A topical example of this can be found in the realm of Customs where the Internet proves to be an instrument for committing typical crimes against Customs Law, such as smuggling, counterfeit, etc. Whereas the computer-specific crimes require updates of the definitions of crimes in national criminal codes, the traditional crimes performed with the aid of computers call for improved co-operation and procedural measures.

Yet all of them benefit from the availability of information and communication networks which are borderless and from the circulation of data which is intangible and extremely volatile. These characteristics call for a review of existing measures to address illegal activities performed on or using these networks and systems.

Many countries have passed legislation to address computer-related crime. In European Union Member States, a number of legal instruments have been issued. Other than a Council Decision on child pornography on the Internet, there are no EU legal instruments so far directly addressing computer-related crime, but there are a number of indirectly relevant legal instruments.

The main issues addressed by legislation in relation to computer specific crimes at EU or Member State level are:

Privacy Offences: Various countries have introduced criminal law addressing illegal collection, storage, modification, disclosure or dissemination of personal data. In the European Union, two Directives have been adopted that approximate the national laws on the protection of privacy with regard to the processing of personal data.[22] Article 24 of the Directive 95/46/EC clearly obliges Member States to adopt all suitable measures to ensure the full implementation of the provisions of the Directive, including sanctions to be imposed in case of infringements of the provisions of national laws. The fundamental rights to privacy and data protection are furthermore included in the Charter of Fundamental Rights of the European Union.

Content-related offences: The dissemination, especially via the Internet, of pornography, in particular child pornography, racist statements and information inciting violence raises the question as to what extent these acts could be confronted with the help of criminal law. The Commission has supported the view that what is illegal off-line should also be illegal on-line. The author or the content provider[23] may be liable under criminal law. A Council Decision has been adopted to combat child pornography on the Internet.[24]

---

22 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Art. 24 of Directive 95/46/EC obliges Member States to lay down sanctions to be imposed in case of infringement of data protection provisions.

23 The content provider should not be confused with the service provider.

24 Council Decision of 29 May 2000 to combat child pornography on the Internet (OJ L 138, 9.6.2000, p.1).

The liability of the intermediary service providers, whose networks or servers are used for the transmission or storage of third-party information, has been addressed by the Directive on electronic commerce.

Economic crimes, unauthorised access and sabotage: Many countries have passed laws that address computer-specific economic crime and define new offences related to unauthorised access to computer systems (e.g., hacking, computer sabotage and distribution of viruses, computer espionage, computer forgery, and computer fraud[25]) and new forms of committing offences (e.g., computer manipulations instead of deceiving a human). The object of the crime is often intangible, e.g., money in bank deposits or computer programmes. At present, there are no EU instruments regarding such types of illegal activity. Concerning prevention, the recently adopted revised dual-use goods regulation contributed significantly to liberalise the availability of encryption products.

Intellectual Property Offences: Two Directives have been adopted, on the legal protection of computer programs and of databases,[26] relating directly to the Information Society and providing for sanctions. A Common Position on a proposal for a Directive on copyright and related rights in the Information Society has been adopted by the Council . This is expected to be adopted early 2001.[27] The violation of copyright and related rights as well as the circumvention of technological measures designed to protect these rights are to be sanctioned. As regards counterfeiting and piracy, the Commission will present, before the end of 2000, a Communication taking stock of the consultation process initiated with its 1998 Green Paper and announcing a relevant action plan. As the Internet becomes more and more important commercially, we are beginning to see new disputes around domain names related to cybersquatting, warehousing and reverse hijacking, and, naturally, there are also calls for rules and procedures to help deal with these problems.[28]

Enforcement of taxation obligations also needs to be addressed. In the case of commercial transactions where the recipient of on-line supply of an electronic service is located in the EU, this will in most cases give rise to tax obligations in the jurisdiction where consumption of such a service is deemed to take place.[29] Failure to comply with tax obligations exposes an

---

25 The media has given much attention to the recent "distributed Denial of Service" attacks on large web-sites and the distribution of the so-called LoveBug virus. This however should be kept in perspective. Denial of service attacks, either deliberate or accidental, and e-mail related viruses have been around for many years. The Morris worm and the IBM Xmas-tree email were earlier examples. There exist products and procedures to help deal with these. There is also a great deal of good co-operation within the Internet community to limit the damage from such incidents as they happen. There is similar co-operation to limit spamming abuses.

26 Council Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs (OJ L 122 , 17.5.1991, pp. 42 – 46).
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77 , 27.3.1996, pp. 20 – 28).

27 Common Position adopted by the Council with a view to the adoption of a Directive of theEuropean Parliament and of the Council on harmonization of certain aspects of copyright and related rights in the Information Society (CS/2000/9512).

28 Communication from the Commission to the Council and the European Parliament, The Organisation and Management of the Internet; International and European Policy Issues 1998 – 2000, April 2000, COM(2000) 202.

29 The Commission has proposed a series of amendments to the EU VAT system aimed at clarifying the jurisdiction of tax liability (COM (2000) 349 - Proposal for a Council Directive amending Directive 77/388/EEC as regards the Value Added tax Arrangements applicable to certain services supplied by electronic means) which is currently under consideration in the Council and the Parliament. In some circumstances, however, the liability to pay tax may fall on the supplier, even when the supplier has no physical presence in the taxing jurisdiction.

operator to civil (and in some cases criminal) sanctions which may include seizure of bank accounts or other assets. Although voluntary compliance is always the preferred option, such obligations must ultimately be enforceable.

Co-operation between tax administrations is a key element in achieving this objective. Giving the possibility to some people to protect their lawful transactions will also give the same means to criminals to protect their unlawful transactions. The tools that give us secure e-commerce can also be used to support drug trafficking. Priorities will need to be identified and choices will need to be made.

Protecting the victims of computer-related crime also needs to cover issues of liability, redress and compensation which arise when computer-related crimes do occur. Confidence depends not only on appropriate technology being used, but also on the accompanying legal and economic guarantees. These questions will need to be examined across the range of computer-related crimes.

There is a need for effective substantive and procedural law instruments approximated at global, or at least at European level, to protect the victims of computer-related crime and to bring the perpetrators to justice. At the same time, personal communications, privacy and data protection, access to and dissemination of information, are fundamental rights in modern democracies. This is why the availability and use of effective prevention measures are desirable so to reduce the need to apply enforcement measures. Any legislative measures that might be necessary to tackle computer-related crime need to strike the right balance between these important interests.

4. SUBSTANTIVE LAW ISSUES

Approximation of substantive law in the area of high tech crime will ensure a minimum level of protection for victims of cybercrime (for example, victims of child pornography), will help to meet the requirement that an activity must be an offence in both countries before mutual legal assistance can be provided to assist a criminal investigation (the dual criminality requirement), and will provide greater clarity for industry (for example, on what constitutes illegal content).

In fact, an EU legislative instrument approximating substantive criminal law in the field of computer-related crime has been on the EU agenda following the Tampere Summit of the European Council in October 1999.[30] The Summit included high-tech crime in a limited list of areas where efforts should be made to agree on common definitions, incriminations and sanctions. This is included in Recommendation 7 of the European Union strategy for the new Millennium on the prevention and control of organised crime adopted by the JHA Council in March 2000.[31] It is also part of the Commission Work Programme for the Year 2000 and the Scoreboard for the establishment of an area of Freedom, Security and Justice, produced by the Commission and adopted by the Justice and Home Affairs Council on 27 March 2000.[32]

The Commission has followed the work of the Council of Europe on the Cybercrime Convention. Four categories of criminal offences are listed in the current draft C.o.E.

---

30 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

31 The Prevention and control of organised crime: A European Union strategy for the beginning of the new Millennium (OJ 2000 C124, 3.5.2000).

32 http://europa.eu.int/comm/dgs/justice_home/index_en.htm.

Cybercrime Convention: 1) Offences against the confidentiality, integrity and availability of computer data and systems; 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights.

EU approximation could go further than the C.o.E. Convention, which will represent a minimum of international approximation. It could be operational within a shorter period of time than the entry into force of the C.o.E. Convention.[33] It would bring computer crime within the realms of EU law and introduce EU enforcement mechanisms.

The Commission attaches great importance to ensuring that the European Union is able to take effective action in particular against child pornography on the Internet. The Commission welcomes the Council Decision on combating child pornography on the Internet, but shares the view of the European Parliament that further action is required to approximate national laws. The Commission intends to introduce later this year a proposal for a Council Framework Decision that will include provisions for the approximation of laws and sanctions on child pornography on the Internet.[34]

In accordance with the Tampere conclusions, the Commission will bring forward a legislative proposal under Title VI of the TEU to approximate high tech crime offences. This will build on the progress made at the Council of Europe, and will address in particular the need to approximate legislation relating to hacking and denial of service attacks. The proposal will include standard definitions for the European Union in this area. This could also go further than the draft Council of Europe Convention by ensuring that serious cases of hacking and denial of service attacks are punishable by a minimum penalty in all Member States.

Furthermore, the Commission will examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a proposal for a Council Framework Decision under Title VI of the TEU covering both off-line and on-line racist and xenophobic activity. This will take account of the forthcoming evaluation of the implementation by Member States of the Joint Action of 15 July 1996 concerning action to combat racism and xenophobia.[35] The Joint Action was a first step towards approximation of criminal offences relating to racism and xenophobia, but there is a need for further approximation within the European Union. The importance and sensitivity of this issue has been highlighted by the decision of a French court on 20 November 2000 requiring Yahoo to block French users from accessing sites selling Nazi memorabilia.[36]

Finally, the Commission will consider how to improve the effectiveness of efforts against the illicit drugs trade on the Internet, the importance of which is recognised in the European Union Drugs Strategy 2000-2004 endorsed at the European Council in Helsinki.[37]

---

33 Entry into force of the C.o.E. Convention will only take place after ratification.

34 This initiative is part of a package of proposals which also covers wider issues associated with the sexual exploitation of children and trafficking in human beings, as announced in the Commission's Communication on trafficking in human beings of December 1998. The text of the proposal for a Council Framework decision is annexed to the Communication from the Commission to the Council and the European Parliament on combating trafficking in human beings an the sexual exploitation of children: two proposals for Framework Decisions which is being published in parallel with this Communication.

35 OJ, L185, 24.7.1996, p. 5-7. Also available on the European Judicial Network website http://ue.eu.int/ejn/index.htm.

36 Tribunal de Grande Instance de Paris, Ordonnance de Référé rendue le 20 November 2000, No. RG 00/05308.

37 EU Action Plan to Combat Drugs (2000 – 2004). COM(1999) 239 final, http://europa.eu.int/comm/justice_home/unit/drogue_en.htm.

5. PROCEDURAL LAW ISSUES

The very nature of computer-related criminal offences brings procedural issues to the forefront of national and international attention as different sovereignties, jurisdictions and laws come into play. More than in any other transnational crime, the speed, mobility and flexibility of computer crime challenge the existing rules of criminal procedural law.

Approximation of procedural law powers will improve the protection of victims by ensuring that law enforcement agencies have the powers they need to investigate offences on their own territory, and will ensure that they are able to respond quickly and effectively to requests from other countries for co-operation.

It is also important to ensure that measures taken on the basis of criminal law, which generally falls with the competence of Member States and Title VI of the TEU, are in accordance with Community law requirements. In particular, the Court of Justice has consistently held that such legislative provisions may not discriminate against persons to whom Community law gives the right to equal treatment or restrict the fundamental freedoms guaranteed by Community law.[38] Any new powers for law enforcement need to be assessed against Community law and their impact to privacy.

5.1. Interception of communications

In the European Union, there is a general principle of confidentiality of communications (and related traffic data). Interceptions are illegal unless they are authorised by law when necessary in specific cases for limited purposes. This follows from Article 8 of the European Convention of Human Rights, referred to in Article 6 of the TEU and more particularly from Directives 95/46/EC and 97/66/EC.

All Member States have a legal framework in place to allow law enforcement to obtain judicial orders (or, in the case of two Member States, a warrant personally authorised by a senior Minister) for the interception of communications on the public telecommunications network.[39] This legislation, which has to be in line with Community law to the extent that it applies, contains safeguards protecting individuals' fundamental right to privacy, such as limiting the use of interception to investigations of serious crimes, requiring that interception in individual investigations should be necessary and proportionate, or ensuring that the individual is informed about the interception as soon as it will no longer hamper the investigation. In many Member States, interception legislation contains obligations for (public service) telecommunications operators to provide for interception capabilities. A 1995 Council Resolution was aimed at co-ordinating interception requirements.[40]

---

38 Case C-274/96 Bickel & Franz (1998) ECR I-7637 para 17, Case C-186/87 Cowan (1989) ECR 195 para 19. In particular, the administrative measures or penalties must not go beyond what is strictly necessary, the control procedures must not be conceived in such a way as to restrict the freedom required by the Treaty and they must not be accompanies by a penalty which is so disproportionate to the gravity of infringement that it becomes an obstacle to the exercise of that freedom (Case C-203/80 Casati (1981) ECR 2595 para 27).

39 Two Member States do not allow intercepted communications as evidence in criminal proceedings.

40 Council Resolution of 17 January 1995 on the lawful interception of telecommunications (OJ C 329, 4.11.1996, pp. 1– 6). The Annex contains a list of law-enforcement interception requirements that Member States were requested to take into account in the definition and implementation of relevant national policies and measures. In 1998, the Austrian Presidency proposed an EU Council Resolution to extend the scope of the 1995 Resolution to cover new technologies, including Internet and satellite communications. This has been the subject of debate in two European Parliament Committees, the

Traditional network operators, in particular those offering voice services, have in the past established working relations with law enforcement to facilitate lawful interception of communications. Telecommunications liberalisation and the explosion of Internet use have attracted many entrants to the marketplace, who have been confronted afresh with interception requirements. Questions on regulations, technical feasibility, allocation of costs and commercial impact will need to be discussed in government-industry dialogues together with all other parties concerned including data protection supervisory authorities.

New technologies make it essential that Member States work together if they are to maintain their capabilities for lawful interception of communications. Where Member States introduce new technical interception requirements on telecommunications operators and Internet service providers, the Commission believes these standards should be co-ordinated internationally to prevent distortion of the Single Market, to minimise the costs for industry and to respect privacy and data protection requirements. The standards should be public and open where possible and should not introduce weaknesses into the communications infrastructure.

In the context of the EU Convention on Mutual Assistance in Criminal Matters,[41] an approach has been agreed to facilitate co-operation on legal interception.[42] The Convention contains provisions on the interception of satellite telephone communication,[43] and on interception of communications of a person on the territory of another Member State.[44] The Commission believes that the interception rules in the Mutual Legal Assistance Convention constitute the maximum possible at the current stage. The text of the Convention is technology neutral; it will have to be tested how it will work in practice before any improvements can be considered. The Commission will review its implementation with Member States, industry, users and data protection supervisory authorities to ensure that relevant initiatives are effective, transparent and well balanced.

Committee on Civil Liberties and Internal Affairs and the Committee on Legal Affairs and Citizens' Rights, which reached different conclusions. The former considered this resolution to be a clarification and update of the old one and thought it was acceptable. The latter was strongly critical, both on potential human rights infringements and on the costs to operators, rejecting the EU Council proposal and calling on the Commission to draw up a new proposal once the Treaty of Amsterdam had entered into force. The draft Council Resolution has not been actively considered by the Council or its working parties in recent months.

41 O J C 197 of 12.7.2000, p.1. The Convention was adopted 29 May 2000. The interception provisions in the Convention apply only to the Member States of the European Union and not to third countries.

42 The Convention provides for minimum safeguards concerning the protection of privacy and personal data.

43 The initial purpose of the negotiations was to provide an interception capability concerning persons using satellite telephones on the territory of the intercepting Member State. Technically, the critical point to intercept these communications is at the satellite ground station. It was therefore necessary to seek technical assistance from the Member State where the ground station was located. The Convention contains two options that address this issue: an expedited mutual legal assistance procedure which requires individual requests for assistance to the Member State with the satellite ground station, and a technical solution based on remote access to the satellite ground station from the intercepting Member State which does not require individual requests.

44 The Convention also provides for a legal framework for requests for interception of the communications of a person on the territory of another Member State (the requested Member State). In this case, the intercepting Member State and the requested Member State both need to obtain interception warrants under their domestic laws. Finally, the Convention establishes rules to cover situations where the intercepting Member State may have the possibility to intercept the communications of a person on the territory of another Member State without the need to seek technical assistance from that Member State.

Abusive, indiscriminate use of interception capabilities, particularly internationally, will raise human rights questions and will undermine citizens' trust in the Information Society. The Commission has seen with grave concern reports on alleged abuses of interception capabilities.[45]

5.2. Retention of traffic data

To investigate and prosecute crimes involving the use of the communications networks, including the Internet, law enforcement authorities frequently use traffic data when they are stored by service providers for billing purposes. As the price charged for a communication is becoming less and less dependent on distance and destination, and service providers move towards flat rate billing, there will no longer be any need to store traffic data for billing purposes. Law enforcement authorities fear that this will reduce potential material for criminal investigations and therefore advocate that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes.[46]

In accordance with the EU personal Data Protection Directives, both the general purpose-limitation principles of Directive 95/46/EC and the more specific provisions of Directive 97/66/EC, traffic data must be erased or made anonymous immediately after the telecommunications service is provided, unless they are necessary for billing purposes. For flat rate or free-of-charge access to telecommunications services, service providers are in principle not allowed to preserve traffic data.

Under the EU Data Protection Directives, Member States may adopt legislative measures to restrict the scope of the obligation to erase traffic data when this constitutes a necessary measure for, amongst others, the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the telecommunications system.[47]

However, any legislative measure at national level that may provide for the retention of traffic data for law enforcement purposes would need to fulfil certain conditions: the proposed measures need to be appropriate, necessary and proportionate, as required by Community law and international law, including Directive 97/66/EC and 95/46/EC, the European Convention for the Protection of Human Rights of 4 November 1950 and the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data of 28 January 1981. This is particularly relevant for measures that would involve the routine retention of data on a large part of the population.

Some Member States are taking legal initiatives requiring or allowing service providers to store certain categories of traffic data, not needed for billing purposes, after the provision of the service but which are considered useful for criminal investigations.

---

45 A long, extensively documented report by Mr Campbell (http://www.gn.apc.org/duncan/stoa_cover.htm) on an intelligence interception network called ECHELON was the subject of a European Parliament public hearing. The report argues that ECHELON was conceived for national security purposes but has also been used for industrial espionage. The European Parliament has set up a temporary Committee that will study the subject and will submit a report to the plenary within a year.

46 These would include criminal investigations in cases that are not related to computers or communications networks, but where the data may help to resolve the crime.

47 Art. 14 of Directive 97/66/EC and art 13 of Directive 95/46/EC.

The scope and form of these initiatives varies considerably, but they are all based on the idea that more data should be available for law enforcement authorities than would be the case if service providers only process data which are strictly needed for the provision of the service. The Commission is examining these measures in the light of existing Community law.

The European Parliament is sensitive to privacy issues and generally has taken a stance in favour of strong protection of personal data. However, in discussions on combating child pornography on the Internet, the European Parliament has expressed an opinion favouring a general obligation to preserve traffic data for a period of three months. [48]

This illustrates the importance of the context in which a sensitive topic such as traffic data retention is discussed and the challenge facing policy makers seeking to strike appropriate balances.

The Commission considers that any solution on the complex issue of retention of traffic data should be well founded, proportionate and achieve a fair balance between the different interests at stake. Only an approach that brings together the expertise and capacities of government, industry, data protection supervisory authorities and users will succeed in meeting such goals. A consistent approach in all Member States on this complex issue would be highly desirable, to meet the objectives of both effectiveness and proportionality and to avoid the situation where both law enforcement and the Internet community would have to deal with a patchwork of diverse technical and legal environments.

There are quite different important concerns to be taken into account. On one hand, data protection supervisory authorities have considered that the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes.[49] On the other hand, law enforcement authorities have stated that they consider the retention of a minimum amount of traffic data for a minimum period of time necessary to facilitate criminal investigations.

Industry has an interest to co-operate in the fight against crimes like hacking and computer-fraud, but should not be confronted with measures that are unreasonably costly. The economic impact of any measures should be carefully analysed and compared with the effectiveness of such a measure in the fight against cybercrime in order to avoid making the Internet more costly and less affordable for users. Adequate security of any retained traffic data would have to be ensured.

In any case, industry will have a key role to play in contributing, to the process of creating a safer Information Society. Users should have confidence in the safety of the Information Society and feel protected from crime and from infringements of their privacy.

---

48 Legislative resolution embodying Parliament's opinion on the draft Joint Action, adopted by the Council on the basis of Article K.3 of the Treaty on European Union, to combat child pornography on the Internet, Amendment 17 (OJ C 219,30.7.1999, pp. 68 ff., on p. 71).

49 "Large-scale exploratory or general surveillance must be forbidden…the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes and that national laws should not oblige telecommunications operators, telecommunications service and Internet Service providers to keep traffic data for a period of time longer than necessary for billing purposes," Recommendation 3/99 of the Art. 29 Data Protection Working Party of 7 September 1999, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

The Commission fully supports and encourages a constructive dialogue between law enforcement, industry, data protection authorities and consumer organisations as well as other parties that might be concerned. Within the framework of the proposed EU Forum (see point 6.4 of this Communication), the Commission will urge all the parties concerned to discuss in-depth, as a matter of priority, the complex issue of retention of traffic data with a view to jointly finding appropriate, balanced and proportionate solutions fully respecting the fundamental rights to privacy and data protection.[50] On the basis of the outcome of this work, the Commission will be able to assess the need for any legislative or non-legislative actions at EU level.

5.3. Anonymous access and use

Law enforcement experts have expressed concern that anonymity may result in non-accountability and could seriously impede the possibility to catch certain criminals. Anonymous use of mobile telephony is possible in some countries through pre-pay cards (not in others). Anonymous access to and use of the Internet is offered by some service and access providers, including re-mailers and Internet cafés. A degree of anonymity is also facilitated by the system of dynamic Internet addressing, in which addresses are not allocated to users on a permanent basis but only for the duration of a given session.

In their discussions with the Commission, some representatives from industry have not been in favour of full anonymity, partly for their own security, anti-fraud and network integrity purposes. The London Internet Exchange has pointed to best practice guidelines they had issued which had proved useful in the UK.[51] However, other industry representatives and privacy experts have stated that without anonymity it is not possible to guarantee fundamental rights.

The Art. 29 Data Protection Working Party has issued a Recommendation on the subject of anonymous use of the Internet.[52] It considers the issue of anonymity on the Internet as being at the centre of a dilemma for governments and international organisations. On the one hand the possibility of remaining anonymous is essential if the fundamental rights to privacy and freedom of expression are to be maintained in cyberspace. On the other hand the ability to participate and communicate on-line without revealing one's identity runs against the grain of initiatives being developed to support other key areas of public policy, such as the fight against illegal and harmful content, financial fraud or copyright infringements. Of course such apparent conflict between different public policy objectives is not new. In the context of the more traditional off-line modes of communication, such as letter and parcel post, the telephone, newspapers, or broadcasting via radio and television, a balance between these objectives has been achieved. The challenge facing policy-makers today is to ensure that this balanced approach, which guarantees basic rights while permitting proportionate restrictions to these rights in limited and specified circumstances, is maintained in the new context of cyberspace. Central to this balance will be the extent of, and limits to, a person's ability to participate on-line in an anonymous fashion.

---

50 As incorporated in the European Convention on Human Rights (Article 8, right to privacy), the EU Charter on Fundamental Rights, the EU Treaty and EC Data Protection Directives.

51 http://www.linx.net/noncore/bcp/.

52 Working Party on the Protection of Individuals with regard to the Processing of Personal data. Recommendation 3/97 Anonymity on the Internet. Adopted by the Working Party on 3 December 1997. http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

In the concluding Declaration of the Ministerial Conference in Bonn on Global Information Networks, 6-8 July 1997, it was stated that the principle should be that where the user can choose to remain anonymous off-line, that choice should also be available on-line. There is a clear consensus therefore that activity on networks should be viewed using the basic legal principles that apply elsewhere. The Internet is not an anarchic ghetto where society's rules do not apply. Equally, though, the ability of governments and public authorities to restrict the rights of individuals and monitor potentially unlawful behaviour should be no greater on public networks than it is in the outside, off-line world. The requirement that restrictions to fundamental rights and freedoms be properly justified, necessary and proportional in view of other public policy objectives, must also apply in cyberspace.

In the Article 29 Data Protection Working Party recommendation it is indicated in detail how this may be achieved in specific cases (for example concerning e-mail, newsgroups, etc).[53] The Commission shares the views expressed by the Working Party.

5.4. Practical co-operation at international level

In the recent past, world-wide combined law enforcement operations, such as Operations Starburst and Cathedral against paedophile rings, have shown the value of co-ordinated international action by law enforcement and judiciary, both in exchanging information at the preliminary stage and in preventing the tipping off of other ring members when arrests and seizures are made. The Internet has also proved to be a valuable and efficient tool for police and customs investigations where it is used as an instrument for committing traditional crimes, such as counterfeiting and smuggling.On the other hand, these operations have also revealed the major legal and operational difficulties with which law enforcement and judiciary were confronted while managing this action, such as preparation of cross border evidence or *commission rogatoire*, victim identification, and the role of intergovernmental organisations dealing with police issues (Interpol and Europol in particular).

In the field of practical international co-operation measures international networks for the exchange of information are becoming increasingly important for police and customs authorities.

Within the G8, a 24 hour/7 day information network of law-enforcement points of contact has been established and is already operational. Its main purpose is to receive and respond to urgent requests for co-operation in cases involving electronic evidence. The network has been used successfully in a number of cases. The EU JHA Council on 19 March 1998 endorsed the 10 Principles to combat high-tech crime adopted by the G8 and invited the non-G8 Countries of the Member States of the EU to join the network.[54] These contact points should co-operate directly, supplementing existing structures of mutual assistance and channels for communications.[55]

Creation of such a network is also foreseen by the draft C.o.E. Convention. Reference to a 24h/7d network of points of contact exists also in the Council Decision on combating Child Pornography on the Internet and in the EU Common Position on the draft C.o.E. Convention

---

53 http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm .

54 Apart from the G8 Members, five EU Member States have so far joined the G8 24/7 network.

55 At the World Conference against Commercial Sexual Exploitation of Children in Stockholm on 28 August 1996 proposals were made to include INTERPOL in the mentioned networks. The Decision of the EU Council on combating child pornography on the Internet foresees also the involvement of Europol in this field.

on cyber-crime[56] and in the Council decision endorsing the G8 action plan,[57] but no concrete EU-specific initiatives have yet been taken.

The Commission considers that given the need for appropriate expertise and expedited action in this field, the Council's intentions should be implemented without delay**.** To be successful, however, such a network would require both legally and technically literate staff, which implies appropriate training.

There is a similar need to intensify co-operation and information exchange between customs authorities. Existing forms of co-operation should be enhanced, and new means of managing joint operations and exchanging information should be developed. With due regard to data protection requirements, there is a growing consensus among customs authorities that international information networks should be formed to further facilitate the exchange of information. There is also a need for greater resources to be invested in this area, both regarding the upgrade of computer systems but also in educating personnel, in order for customs authorities to perform their duties more effectively.

5.5. Procedural law powers and jurisdiction

At the domestic level, and once the necessary conditions enshrined in law are fulfilled, law-enforcement authorities need to be able to search and seize data stored in computers speedily enough to prevent the destruction of criminal evidence. Law-enforcement authorities consider that they should have sufficient coercive powers to be able, within their jurisdiction, to search computer systems and seize data, order persons to submit specified computer data, order or obtain the expeditious preservation of specific data in accordance with normal legal safeguards and procedures. At present, however, the safeguards and procedures are not approximated.

Questions may arise if, when accessing a computer, law-enforcement authorities find that a number of computers and networks are involved which are located all over the country. Issues become much more complicated if, while searching a computer or simply pursuing an investigation, a law-enforcement authority finds itself accessing or needing to access data located in one or more different countries. Important sovereignty, human rights and law-enforcement interests are at stake and need to be balanced.

Existing legal tools for international co-operation in criminal law matters, i.e., mutual legal assistance, may not be appropriate or sufficient, since their implementation normally takes several days, weeks or months. There is a need for a mechanism by which countries can investigate offences and obtain evidence quickly and efficiently, or at least not lose important evidence in cross-border law-enforcement procedures, in a manner consistent with principles of national sovereignty and constitutional and human rights, including privacy and data protection.

New proposals under consideration in the Council of Europe draft Convention on Cybercrime to address these problems include orders for the preservation of data to assist specific

---

[56] Article 1.4 of the Common Position: "Member States should support the establishment of provisions, which will facilitate international co-operation including provisions concerning mutual legal assistance to the widest extent possible. The Convention should facilitate the swift co-operation regarding computer-related and computer-aided offences. This form of co-operation may include the setting of 24-hour law enforcement points of contact, which supplement existing structures of mutual assistance."

[57] Available on the European Judicial Network website http://ue.eu.int/ejn/index.htm.

investigations. However, other issues, such as transborder search and seizure, present difficult and as yet unresolved policy questions. More discussion among all parties concerned is clearly required before any concrete initiatives may be envisaged.

The G8 high-tech crime subgroup has discussed the issue of transborder search and seizure and, in anticipation of a subsequent more permanent agreement, has reached consensus on provisional principles[58]. Important questions, however, related in particular to when expedited search and seizure in particular situations is possible prior to informing the searched state, and appropriate safeguards to respect fundamental rights will need to be established. In the EU Common Position relating to the C.o.E. Draft Convention on Cybercrime, the Ministers have adopted an open-ended position.[59]

In transborder computer-related crime cases, it is also important that there are clear rules on which country has jurisdiction for prosecution. In particular it should be avoided that no country has jurisdiction. The main rules proposed by the draft Council of Europe Convention are that jurisdiction be established by a state when the offence is committed in its territory or by one of its nationals. When more than one state claims jurisdiction, the states concerned should consult with a view to determining the most appropriate jurisdiction. However, a lot will depend on effective bilateral or multilateral consultation. The Commission will keep this issue under review to see whether any further action may be required at EU level.

The Commission, having participated in both the C.o.E. and the G8 discussions, recognises the complexity and difficulties associated with procedural law issues. But effective co-operation within the EU to combat cybercrime is an essential element of a safer Information Society and the establishment of an Area of Freedom, Security and Justice.

The Commission intends to continue its consultations with all parties concerned over the coming months with a view to building on this work. This issue will also be considered in the wider context of its work on implementing the conclusions of the European Council in Tampere in October 1999. In particular, the Tampere Summit asked the Council and the Commission to adopt, by December 2000, a programme of measures to implement the principle of mutual recognition of judicial decisions. The Commission has already published a Communication on Mutual Recognition of Final Decisions in Criminal Matters.[60] As part of its contribution to implementing the part of the programme of measures dealing with enforcement of pre-trial orders, the Commission will consider the options for mutual recognition of pre-trial orders associated with cybercrime investigations with a view to bringing forward a legislative proposal under Title VI of the TEU.

5.6. Evidential validity of computer data

Even in cases in which law-enforcement authorities have accessed computer data which seem to be criminal evidence, they need to be able to retrieve and authenticate them for use in

---

58 Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organised Crime-Moscow, 19-20 October 1999 (see http://www.usdoj.gov/criminal/cybercrime/action.htm and also http://www.usdoj.gov/criminal/cybercrime/principles.htm).

59 OJ L 142/2: "Subject to constitutional principles and specific safeguards in order to respect appropriately the sovereignty, security, public policy or other essential interests of other States, a transborder computer search for the purpose of the investigation of a serious criminal offence, to be further defined in the Convention, may be considered in exceptional cases, and in particular where there is an emergency, for example, as far as necessary to prevent the commission of an offence that is likely to result in the death of or serious injury to a person."

60 COM (2000) 495, Brussels 26.7.2000.

criminal investigations and prosecutions. This is not a very easy task given the volatile nature and ease of manipulation, falsification, technological protection or deletion of electronic data. It is addressed by computer forensics**,** which encompasses the development and use of scientific protocols and procedures for searching computers and analysing and maintaining the authenticity of data that has been retrieved.

At the request of the G8 experts, the International Organisation of Computer Evidence (IOCE) has agreed to develop recommendations for standards, including the definition of common terms, identification methods and techniques to be used and establishment of a common format for forensic requests. The EU should be associated with this work, both at the level of Member States specialised computer-crime investigation bodies and through the R&D supported by the 5th Framework Programme (IST Programme).

6. NON-LEGISLATIVE MEASURES

Appropriate legislation at both national and international level is necessary but not in itself sufficient for effectively combating computer-related crime and network misuse. A number of supplementary, non-legislative conditions are also required to complement the legislative measures. Most have been included in the recommendations of the COMCRIME study, the G8 has proposed such in its 10-point action plan and they have received broad support in the informal consultation process that preceded the drafting of this Communication. They include:

- the creation of special computer-crime police units at the national level, where they do not already exist ;
- improved co-operation between law enforcement, industry, consumer organisations and data protection authorities;
- encouraging appropriate industry and community-led initiatives, including on security products.

The issue of encryption is likely to remain important in this context. Encryption is an essential tool to facilitate the implementation and adoption of new services, including electronic commerce, and can make a substantial contribution to the prevention of crime on the Internet. The Commission's policy on encryption has been laid down in its Communication on trust and confidence in electronic communication of 1997,[61] in which the Commission indicated that it would try to abolish all restrictions on the free circulation of all encryption products at the level of the European Community. The Communication further stated that domestic restrictions on the free circulation of encryption products have to be compatible with Community law and that it will examine whether such national restrictions are justified and proportionate, notably with respect to the free circulation provisions of the Treaty, the case law of the Court of Justice and the requirements of the Data Protection Directives. Nevertheless, the Commission recognises that encryption also presents new and difficult challenges for law enforcement agencies.

The Commission therefore welcomes the recently adopted revised dual-use goods regulation that significantly contributed to liberalise the availability of encryption products, while

---

61 COM(97)503.

recognising that this needs to be accompanied by a better dialogue between users, industry and law enforcement. For its part, the Commission intends to promote this dialogue at EU level through the proposed EU Forum. The EU wide availability of security products, including strong encryption products, where appropriate certified to agreed evaluation criteria, would improve both crime prevention possibilities and users' trust in information society processes.

6.1. Specialised units at the national level

Given the technical and legal complexity of some of the computer-related criminal acts, the setting up of specialised units at national level is essential. Such specialised units, consisting of knowledgeable, multidisciplinary (law enforcement and judiciary) personnel should be equipped with adequate technical facilities and operate as rapid contact points for the purposes of:

- responding quickly to requests for information on suspected offences. Common formats for the exchange of such information will need to be defined, although discussions at G8 experts level have shown that this may not be an easy task, given differences in national legal cultures;

- acting as the law enforcement-interface nationally and internationally for hotlines[62] receiving complaints about illegal content from Internet users;

- improving and/or developing specialised computer investigation techniques for the purpose of detecting, investigating and prosecuting computer-related crimes;

- acting as a centre of excellence on cyber-crime issues for the purpose of sharing best practices and experience.

Within the EU some Member States have already set up these specialised units dealing specifically with computer-related crimes. The Commission considers that the setting up of such specialised units is a Members State prerogative and strongly encourages Member States to take steps in that direction. Purchasing the latest hardware and software for these units and training their personnel involves substantial cost and presupposes priorities and political decisions at appropriate government levels.[63] The experience of already existing Member States units may be particularly valuable. The Commission will encourage the exchange of such experience.

---

62 So far, hotlines exist only in a limited number of countries. Examples are Cybertipline in the US and Internet Watch Foundation (IWF) in the UK, which, since Dec. 1996, has operated a telephone and e-mail hotline for members of the public to report material encountered on the Internet, which they consider illegal. The IWF judges whether the material is illegal, informs the ISPs and the police. Other monitoring bodies exist also in Norway (Redd Barna), the NL (Meldpunt), Germany (Newswatch, FSM and Jugendschutz), Austria (ISPAA) and Ireland (ISPAI). In the framework of the EU Daphne Programme, Childnet International is currently undertaken a project directly related to this issue ("International Hotline Providers in Europe Forum"). The UNESCO Expert Meeting in Paris in January 1999 supports and encourages also national hotlines and the creation of networks of hotlines or an international "electronic watchtower."

63 On the U.S. experience on this issue, see Michael A. Sussmann "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium," Duke Journal of Comparative and International Law, Vol. 9 Spring 1999, p. 464.

The Commission also believes that Europol can provide further added value at EU level through co-ordination, analysis and other assistance to the national specialised units. The Commission will therefore support the extension of Europol's remit to cover cybercrime.

6.2. Specialised training

A considerable effort is required in the area of continuous, specialised training of both police and judicial staff. Computer-related criminal techniques and capabilities change more rapidly than those in more traditional areas of criminal activity.

Some Member States have been implementing initiatives for the high-tech training of law enforcement staff. They could provide advice and guidance to Member States that have not yet taken similar steps.

Individual projects aiming to achieve this – taking the form of exchanges of experiences, seminars on common challenges faced by the relevant professional categories– have been launched with the support of programmes administered by the Commission (in particular STOP, FALCONE and GROTIUS Programmes). The Commission will propose more activities in this area, including computer and on-line training.

Europol has taken the initiative to host a one-week training session for law-enforcement personnel from the Member States in November 2000, with particular reference to child pornography issues. The scope of such a session could be extended to include computer-related crime in general. Interpol has also been active in this field since a number of years. Its relevant initiatives could be extended to include a larger number of trainees.

The G8 has organised initiatives allowing the exchange of experience amongst law enforcement authorities and the establishment of common investigation techniques on the basis of concrete cases. A further initiative in the field of training is expected to be taken in the second half of year 2001. EU Member States participating in the G8 could share these experiences with the other Member States.

In the specific field of combating child pornography on the Internet, the creation and maintenance of a digital Central Library of child pornography images at an international level (to be made available on the Internet for specialised law enforcement units at national level, with the necessary conditions and limitations as regards access and protection of privacy) would aid the search for victims and perpetrators, help determine the nature of offences and train specialised police officers.[64]

6.3. Improved information and common rules for record keeping

The creation of a harmonised set of rules for police and judicial record-keeping and of the appropriate tools for statistical analysis of computer crime would help law enforcement and judicial authorities to better store, analyse, evaluate the formal information gathered in this still changing area.

---

[64] In this context, the project "Excalibur" developed by the Swedish National Crime Intelligence Division and co-sponsored by the European Commission under the STOP Programme has been a very successful initiative. This project has been set up with the co-operation of police forces from Germany, UK, the Netherlands and Belgium, together with Europol and Interpol. Other projects undertaken by the German BKA (the so-called "Perkeo") and the French Ministry of Interior ("Surfimage" project also co-sponsored under the STOP Programme) have also to be taken into right account.

Also, from the point of view of the private sector, such statistics are required for a proper assessment of the risks involved, and a cost-benefit analysis of their management. This is important not only for operational reasons (such as deciding on what security measures to take) but also for insurance purposes.

A database on computer crime statutes that was provided as part of the COMCRIME study, is being updated and made accessible to the Commission. The Commission will consider improving the content (include laws, court cases and literature) and usability of the database**.**

6.4. Co-operation between the various actors: the EU Forum

Effective co-operation between government and industry within the legal framework has been considered as an essential element of any public policy to tackle computer-related crimes.[65]Law-enforcement representatives have admitted that they have not always been sufficiently clear and precise on what they need from service providers. Industry representatives have expressed a generally positive attitude towards better co-operation with law enforcement whilst underlining the need for an appropriate balance between the protection of the fundamental rights and freedoms of citizens, in particular their right to privacy,[66] the need of combating crime and the economic burdens placed on providers.

Together, industry and law enforcement can raise public awareness on the risks posed by criminals on the Internet, promote best practices for security, and develop effective counter-crime tools and procedures. There have already been relevant initiatives in a number of Member States of which the UK Internet Crime Forum is probably the oldest and most far-reaching.[67]

The Commission welcomes these initiatives and considers they need to be encouraged in all Member States. The Commission intends to establish an EU Forum in which law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organisations, consumer representatives, data protection authorities and other interested parties will be brought together with the aim of fully enhancing co-operation at EU level. At a first stage, this will include public officials to be named by Member States, technology experts, privacy experts to be appointed by the Art. 29 Data Protection Working Party and industry and consumer representatives to be identified in close consultation with industry and consumers associations. At a later stage, this Forum will include representatives from relevant national initiatives.

---

65 In the Communiqué adopted in Washington on 9/10 December 1997 on Principles and 10 Points Action Plan to combat high-tech crime, G8 Ministers of Justice and of the Interior declared that: "it is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent on the industrial sector to play its part in developing and distributing secure systems designed to help detect computer abuse, preserve electronic evidence and assist in ascertaining the location and identity of criminals." The Decision of the EU Council to combat child pornography on the Internet underlines the need that Member States have a constructive dialogue with industry, and in contact with it, shall co-operate by sharing their experiences.

66 As set out in the EU Data Protection Directives, the Council of Europe Convention on Human Rights and the Council of Europe Convention no 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data and relevant national law.

67 Established in 1997, the Internet Crime Forum includes police officers, Home Office and data protection officials and Internet industry representatives; it has plenary meetings 3-4 times a year and a number of permanent working groups.

The EU Forum will be operated in an open and transparent manner, and relevant documents will be published on a website, and comments will be invited from all interested parties.

The EU Forum will be invited to consider in particular the following areas:

- Developing, where appropriate, 24-hours points of contact between government and industry;

- Developing an appropriate standard format for law enforcement requests for information from industry, increasing law enforcement's use of the Internet when communicating with service providers;

- Encouraging the development and/or implementation of codes of conduct and best practices and the sharing of such codes among industries and governments[68]

- Encouraging the exchange of information on trends in high-tech crime between the various parties, particularly industry and law enforcement agencies;

- Exploring law enforcement concerns in the development of new technologies;

- Encouraging further development of early warning and crisis management mechanisms to prevent, identify and handle threats or disrupting events on information infrastructures;

- Providing, where required, an enhanced expert contribution to work underway within the Council and in other international fora, for example the Council of Europe and G8;

- Encouraging co-operation between interested parties including principles shared by law enforcement, industry and users (e.g., Memorandum of Understanding (MOU), Codes of Practice in line with the legal framework).

6.5. Direct industry actions

To a large extent, combating computer-related crime is in the wider community's own interest. If consumers are to have confidence in electronic commerce, measures to prevent computer-related crime need to be an accepted element of good business practice. Many industries, e.g. in the banking, electronic communications, credit card and copyright sectors, and their customers are potential victims of computer-related crime. Companies naturally protect their own names and trademarks, and consequently have a role in fraud prevention. Organisations representing the software and audio industries (e.g., British Phonographic Industry - BPI) have teams investigating piracy (including Internet-related piracy). Internet service providers in a number of Member States have set up hot-lines for the reporting of illegal and harmful content.

The Commission has been supporting some of these initiatives by encouraging their participation in the EU R&D Framework Programme**,** the Internet Action Plan[69] and Title VI Programmes such as STOP and DAPHNE.

---

[68] As far as codes of conduct in the sense of Article 27 of Directive 95/46/EC are concerned (they could cover for example issues falling under Directive 97/66/EC such as interceptions), the Article 29 Data Protection Working Party and national data protection supervisory authorities are involved.

[69] More information about the Internet Action Plan: Action Plan on Promoting Safer Use of the Internet is available at http://158.169.50.95:10080/iap/.

Best practice in these areas will be exchanged in the context of the EU Forum.

6.6. EU-supported RTD projects

In the Information Society Technologies (IST) RTD Programme, which is part of the 5th Framework Programme, 1998 to 2002, emphasis is put on the development and deployment of confidence-building technologies. As such, confidence-building technologies embrace both information and network security technologies as well as technical tools and methods to protect from abuses of the fundamental right to privacy and data protection and other personal rights and to fight computer crime.

The IST Programme, in particular work related to *Information and network security and other confidence-building technologies* in Key Action 2 - *New Methods of Work and Electronic Commerce*, provides the framework to develop capability and technologies to understand and tackle the emerging technology challenges related to preventing and combating computer crime and assure that security and privacy requirements can be met at EU level, at the level of virtual communities and at the level of the individual.

In addition, in order to properly deal with the challenges related to trust and confidence, including preventing and investigating computer crime, a dependability initiative has also been launched in the context of the IST Programme. The role of this initiative is to contribute towards raising and assuring trust and confidence in highly inter-linked information infrastructures and in tightly networked, embedded systems by promoting dependability awareness and dependability-enabling technologies. An integral part of this initiative is international co-operation. The IST Programme has developed working relationships with DARPA and NSF and established, in collaboration with the Department of State, the Joint Task Force on the Critical Infrastructure Protection under the auspices of the EC/US Joint Consultative Group of the S&T Co-operation Agreement.[70]

The Commission's Joint Research Centre (JRC), which has been supporting the dependability initiative in the IST Programme, will focus its efforts on developing appropriate and harmonised measures, indicators and statistics in consultation with other interested parties, including Europol. This will have the aim of developing a proper classification and understanding of illegal activities, their geographical distribution, their rate of increase and the effectiveness of measures taken to counteract them. Where appropriate, the JRC will involve other research groups and integrate their efforts and results. It will maintain an Internet web-site on the issue and report its progress to the EU Forum.

7. CONCLUSIONS AND PROPOSALS

Preventing and effectively combating computer-related crime presupposes the existence of a number of necessary conditions:

- the availability of preventive technologies. This requires an appropriate regulatory environment which gives room and incentives for innovation and research. Public financing can be justified to support the development and deployment of appropriate security technologies.

70 More information about the IST Programme is available at http://www.cordis.lu/ist.

- the awareness of potential security risks and ways to combat them;

- adequate substantive and procedural legislative provisions, as regards both domestic and transnational criminal activities. National substantive criminal laws should be sufficiently comprehensive and effective in criminalising serious computer-related abuses and provide for dissuasive sanctions, helping to overcome dual criminality[71] problems and facilitating international co-operation. Where there is a well-founded need for action by law enforcement to expeditedly search, seize and securely copy computer data within their national territory in order to be able to investigate a computer related crime, this should be made possible by procedural laws, in conformity with the principles and exceptions provided for by Community law and in accordance with the European Convention on Human Rights.The Commission believes that the agreement reached on the interception provisions in the Convention on Mutual Assistance in Criminal Matters is the maximum possible that is achievable at present. The Commission will keep reviewing its implementation with Member States, industry and users to ensure that relevant initiatives are effective, transparent and well balanced;

- the availability of a sufficient number of well trained and equipped law-enforcement personnel. Close collaboration with Internet service providers and telecommunications operators in the field of training will be further encouraged;

- improved co-operation between all the actors concerned; users and consumers, industry, law enforcement and data protection authorities. This is critical to investigating computer crime and protecting public safety. Industry needs to operate within clear rules and obligations. Governments should recognise that the needs of law enforcement may place burdens on industry and thus take reasonable steps to minimise such burdens. At the same time, industry ought to include public safety considerations in its business practices. Increasingly this will need the active co-operation and support of the individual user and consumer;

- continuous industry and community-led initiatives. Hotlines, already in place for reporting illegal and harmful content cases, may be extended to other types of abuse. Industry self-regulation and a multidisciplinary memorandum of understanding could involve the broadest possible number of interested parties and play a multiple role in helping prevent and combat computer crime and increasing awareness and trust;

- the achievements and potential of R&D should be exploited to the maximum extent possible. The strategic focus will be on bringing together affordable and effective security and other confidence building technology developments and EU policy initiatives.

Any measures to be agreed by the EU, however, should take into account the need to gradually bring the candidate countries into the realms of EU and international co-operation in this field and avoid that they are used as computer crime havens. Involvement of representatives of these countries in some or all of the relevant EU meetings should be considered.

The Commission proposals can be divided into the following areas.

---

[71] Where criminal investigations necessitate the assistance of authorities in other countries, many legal systems require that the crime is punishable in both countries as a prerequisite for certain types of mutual legal assistance and for extradition.

7.1. Legislative proposals

The Commission will bring forward legislative proposals under the Title VI of the TEU:

- to approximate Member States' laws in the area of child pornography offences. This initiative will be part of a package of proposals which will also cover wider issues associated with the sexual exploitation of children and trafficking in human beings, as announced in the Commission's Communication on trafficking in human beings of December 1998. Such a proposal will be fully in line with the European Parliament's attempt to turn the Austrian initiative for a Council Decision on child pornography into a Framework Decision requiring approximation of laws. This is also consistent with the Tampere conclusions and the EU strategy for the new Millennium to combat organised crime. This is already part of the Scoreboard for the establishment of an area of Freedom, Security and Justice.

- to further approximate substantive criminal law in the area of high-tech crime. This will include offences related to hacking and denial of service attacks. The Commission will also examine the scope for action against racism and xenophobia on the Internet with a view to bringing forward a Framework Decision under Title VI of the TEU covering both off-line and on-line racist and xenophobic activity. Finally, the problem of illicit drugs on the Internet will also be examined.

- to apply the principle of mutual recognition to pre-trial orders associated with cybercrime investigations and to facilitate computer-related criminal investigations involving more than one Member State with appropriate safeguards concerning fundamental rights. This proposal is consistent with the outline programme of measures for mutual recognition, which refers to the need to consider proposals on the production and freezing of evidence.

The need to take any measures, in particular of a legislative nature on the question of retention of traffic data will be assessed by the Commission amongst other consultations, on the basis of the outcome of the work that will be done by the proposed EU Forum in this area.

7.2. Non-legislative proposals

Action is proposed in a number of areas:

- the Commission will establish and chair an EU Forum in which law enforcement agencies, service providers, network operators, consumer groups and data protection authorities will be brought together with the aim of enhancing co-operation at EU level by raising public awareness on the risks posed by criminals on the Internet, promoting best practices for IT security, developing effective counter-crime tools and procedures to combat computer-related crime as well as encouraging further development of early warning and crisis management mechanisms. This would be an EU version of similar successful fora which exist in certain Member States. Where such fora do not exist the Commission would encourage Member States to set them up. Co-operation between these various fora would be encouraged and facilitated through the EU Forum.

- the Commission will continue to promote security and trust in the context of the *e*Europe initiative, the Internet Action Plan, the IST programme and the next framework programme for RTD. These will include promoting the availability of products and services with an appropriate level of security and encouragement of a more liberalised use of strong encryption through a dialogue amongst all interested parties.

- the Commission will promote further projects under existing programmes to support the training of law enforcement staff on high-tech crime issues and to support research in forensic computing.

- the Commission will consider providing funding for improving the content and usability of the database of Member States' national laws provided by the COMCRIME study, and will launch a study to obtain a better picture of the nature and extent of computer-related crime in the Member States.

7.3 Action in other international fora

The Commission will continue to play a full role in ensuring co-ordination between Member States in other international fora in which cybercrime is being discussed such as the Council of Europe and G8. The Commission's initiatives at EU level will take full account of progress in other international fora, while seeking to achieve approximation within the EU.

* * * * *

FINANCIAL STATEMENT

1 TITLE OF OPERATION

"Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"

2 BUDGET HEADING(S) INVOLVED

B5 302

B5 820

B6 1110, B6 2111, B6 1210

3 LEGAL BASIS

Art. 95, 154 and 155 EC Treaty, and art. 29 and 34 EU Treaty.

4 DESCRIPTION OF OPERATION

4.1 General Objective

The Commission will establish and chair an EU Forum in which law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organisations, consumer representatives, data protection authorities and other interested parties will be brought together with the aim of enhancing mutual understanding and co-operation at EU level. The Forum will seek to raise public awareness of the risks posed by criminals on the Internet, to promote best practice for security, to identify effective counter-crime tools and procedures to combat computer-related crime and to encourage further development of early warning and crisis management mechanisms. Relevant documents will be published on a website.

4.2 Period covered and arrangements for renewal

2001 – 2002. In 2002, it will be evaluated whether to continue the Forum.

5 CLASSIFICATION OF EXPENDITURE OR REVENUE

5.1 Non-compulsory expenditure

5.2 Differentiated appropriations

6 TYPE OF EXPENDITURE OR REVENUE

Meetings: travel expenses reimbursement for experts			
B5 302A	2001		27.000 €
B5 302A	2002		40.500 €
Operation of the Forum, maintenance of a web site			
B6 1110	2001	JRC Missions	10.000 €

B6 2111	2001	JRC Specific credits (various)	15.000 €
B6 1210	2001	JRC Overheads means	50.000 €
B6 1110	2002	JRC Missions	10.300 €
B6 2111	2002	JRC Specific credits (various)	15.450 €
B6 1210	2002	JRC Overheads means	51.500 €
Studies on specific issues			
B6 2111	2001	JRC Specific credits (studies)	25.000 €
B6 2111	2002	JRC Specific credits (studies)	25.750 €
Total	2001 + 2002		270.500 €

7 FINANCIAL IMPACT

Method of calculating the total cost of operation (relation between individual and total costs):

Reimbursement of travel expenses for participants of meetings. We estimate having 2 meetings in 2001 and 3 meetings in 2002. Per meeting, 15 experts will be reimbursed. Average cost of reimbursement per person is estimated at 900 €.

The costs, both in personnel and in specific credits, of infrastructure and administrative and technical support are allocated in proportion to the number of members of staff assigned to the activities concerned. The budget for studies is calculated on the basis of 2 studies per year of about 1 person-month each.

8 FRAUD PREVENTION MEASURES

Routine control. No additional fraud prevention measures are envisaged.

9 ELEMENTS OF COST-EFFECTIVENESS ANALYSIS

9.1 Specific and quantified objectives; target population

Enhancing mutual understanding and co-operation at EU level of different interest-groups. Target participants: law enforcement agencies, Internet Service Providers, telecommunications operators, civil liberties organisations, consumer representatives, data protection authorities and other interested parties.

9.2 Grounds for the operation

The Forum is set up with the aim of enhancing mutual understanding and co-operation at EU level of different interest-groups. The Forum will seek to raise public awareness of the risks posed by criminals on the Internet, to promote best practice for security, to identify effective counter-crime tools and procedures to combat computer-related crime and to encourage further development of early warning and crisis management mechanisms.

9.3 Monitoring and evaluation of the operation

The Commission will organise and chair the meetings of the Forum and participate in the discussions. The Commission will manage the associated web-site. The need to continue the Forum in 2003 and beyond will be evaluated in 2002.

10 ADMINISTRATIVE EXPENDITURE

Requirements in terms of human resources will be covered from existing staff.

10.1 Effect on the number of posts

Type of post	Staff to be assigned to managing the operation		Source		Duration
	Permanent posts	Temporary posts	Existing resources in the DG	Additional resources	
Officials A or B temporary C staff	 0,05	1,75 0,15	1,75 0,15 0,05		Per year over 2 years
Other resources					
Total	0,05	1,9	1,95		

10.2 Overall financial impact of human resources

	Amounts	Method of calculation (2001 + 2002)
Officials	421.200 €	2 years x 108.000 € x 1,95 staff