EUROPEAN UNION
THE COUNCIL

Brussels, 30 March 1998

7278/98
LIMITE

CRIMORG 44

NOTE

from : Presidency

to : Multi-Disciplinary Group on Organised Crime

Subject: High-Technology (Internet) Crime

1. The EU's High Level Group on Organised Crime, in its Action Plan which was endorsed by the Amsterdam European Council in June 1997, has called for:

> "A cross-pillar study on high-tech crime and its use and links with organised crime should be carried out within the Union. This study should pave the way for a policy ensuring an efficient public protection. While avoiding undue restrictions, law enforcement and judicial authorities should have the means, as a complement to the specific responsibilities incumbent on the technology and service providers, to prevent and combat the misuse of these new technologies. Attention should be paid both to illegal practices (such as the use of these technologies by criminal organisations to facilitate their activities) or illegal contents (such as child pornography or dissemination of synthetic drug recipes)". Recommendation 5.

The target date for this to be carried out is the end of 1998.

2. In considering the need for, or the content of, any required study the Multi-Disciplinary Group will wish to take account of work being done in this area in the various international fora. These are principally the G8, the Council of Europe, the Organisation for Economic Co-operation and Development, and the European Union itself including the Commission.

3. The High-Tech Sub-Group of the G8 met 5 times during 1997 under US chairmanship. As a result of the work done by the Sub-Group the Justice and Interior Ministers of the Eight met in Washington in December 1997 following which they issued a communique in which they set out 10 principles for combating high-tech crime, combined with a 10 point action plan. Members will be aware that on 19 March the Justice and Home Affairs Council gave its political endorsement to these principles and the action plan on high-tech crime (attached at Annex A).

4. Action point 1 calls for the establishment of a network of 24-hour points of contact within the G8 to obtain assistance from law enforcement agencies in relation to international high-tech and computer related investigations. This network has now been established and the Presidency is making available to MDG delegates a booklet prepared by the G8 listing the contact points. **The UK in its dual Presidency of the Eight and the European Union invites the MDG delegates from non-G8 Member States of the EU to:**

   a) **make the booklet available to their investigators and prosecutors;**

   b) **arrange for non-G8 Member States to join the network by providing contact points available on a 24-hour basis who can assist investigators and prosecutors in other countries. Additions to the network will be included in a future expanded edition of the booklet.**

5. Action point 2 calls for the training of a sufficient number of law enforcement personnel to deal specifically with the subject of high-tech crime. Training is ongoing and a number of G8 members have created specific computer crime units.

6. Action point 3 calls for a review of legal systems to ensure that they appropriately criminalise abuses of tele-communications and computer systems. Action point 4 considers issues raised by high-tech crimes when negotiating mutual assistance agreements. In view of the fact that work in relation to those action points is being progressed in other fora (see for example paragraphs 13 and 24 below), the High-Tech Sub-Group of the G8 has not so far considered these issues.

7. Action point 5 relates to what is now commonly known as search and seizure techniques which involve trans-border searches and computer searches of data

where the location of that data is unknown. The Sub-Group has discussed "best approaches" and begun drafting specific principles. The primary principle is considered to be that if, following the execution of a search of a computer system in their own country, law enforcement agents become aware that some or all of the data seized during the execution of that search was unknowingly retrieved from a particular foreign country, the searching country shall immediately notify the searched country. The searched country may allow use of the data, object to use of the data, or request a copy of the data in order to conduct its own review. In cases where immediate seizure of data located in another country is necessary to prevent death, serious physical injury, or the destruction of evidence of a serious crime, agents may seize such data and then must notify the searched country as soon as practicable. A number of other principles have been developed from this and work will continue until a comprehensive guiding structure is prepared for consideration by governments. It is recognised that trans-border search principles should protect sovereignty and other public interests of the searched state such as human rights, democratic freedoms and privacy.

8. Action point 6 calls for the development of expedited procedures for obtaining traffic data from communications carriers and action point 7 calls for work jointly with industry to ensure that new technologies facilitate the efforts of law enforcement to combat high-tech crime. The UK has been developing initiatives to establish a dialogue between law enforcement and communication and internet service providers (ISPs) including:

- creation in the UK of the Internet Watch Foundation, an independent organisation funded by internet service providers and overseen by an independent policy board with membership from a wide range of interest groups including government. The Foundation receives complaints about illegal contents and monitors and traces originators of such material.

- formation in the UK of a group comprised of representatives of law enforcement, ISPs, public tele-communications operators, prosecutors and government to discuss matters of common concern including:

  - the legal framework for industry co-operation with investigations by law enforcement;

  - practical arrangements for such co-operation, including points of contact; and

  - possibilities for industry and law enforcement to adapt operational practices in order to minimise burdens on industry.

This approach has been adopted by the Sub-Group and members have agreed to continue dialogue with their own industry representatives on the basis of a commonly agreed agenda. In this way dialogue between law enforcement and industry will be co-ordinated across the Eight.

9. Actions points 8 (response to mutual assistance requests) and 9 (encouragement of internationally recognised standards- making bodies to provide reliable and secure tele-communications) have not been progressed because of work being done in other fora.

10. Action point 10 calls for the development and employment of compatible forensic standards for use in criminal investigations and prosecutions. The Sub-Group has asked the International Organisation on Computer Evidence (IOCE) which is known to be working in this area to conduct a study and report back to the Sub-Group.

COUNCIL OF EUROPE - Committee of Experts on Crime in Cyberspace (PC-CY)

11. The Committee of Experts on Crime in Cyberspace (PC-CY) was formed at the instigation of the European Committee on Crime Problems (CDPC) in February 1997. Its terms of reference reflect the fact that the trans-border character of offences in relation to computer systems and telecommunications networks when committed through the internet is in conflict with the territoriality of national law enforcement authorities. Consequently the CDPC asked the PC-CY to examine computer-related crime and problems of criminal procedural law connected with information technology and to draft a binding legal instrument on the following subjects:

- cyberspace offences, in particular those committed through the use of telecommunication networks, eg the internet;
- other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation;
- the use, including the possibility of trans-border use, and the applicability of coercive powers in a technological environment;
- the question of jurisdiction in relation to information technology offences, the question how to solve positive jurisdiction conflicts, and how to avoid negative jurisdiction conflicts;
- questions of international co-operation in the investigation of cyberspace offences.

12. The Committee first met in plenary in April 1997 when it examined its terms of reference and invited some of its members to prepare a report on specific questions in order to

facilitate its discussions. The second meeting of the Committee was held in October 1997 when reports in relation to offences, liability of service providers, interception of telecommunications, search and seizure in a computer environment, jurisdiction, other means of collecting evidence, data protection issues, and international co-operation were discussed. These subjects were considered suitable for inclusion in a future draft convention.

Offences

13. The drafting group has considered that the prime offence should be hacking and discussion is continuing on whether other qualifying elements such as infringement of security measures should be included in the definition. Other offences include unauthorised use (including use of time) computer damage and computer sabotage (including alteration of data), computer fraud and forgery, unauthorised reproduction and use, data protection offences, and communication and contents offences (including child pornography).

Liability of Service Providers

14. Discussion on this topic is to establish the conditions of an ISPs responsibility, depending on whether the person in question stores information or not and whether he controls it or not (ie knows the content and is able to react). Several forms of responsibility, for example as carriers, publishers and distributors, are being examined whilst taking into account common elements such as knowledge of the harmful nature of the material, reasonableness of action, duty of care, real function.

Interception of Telecommunications

15. The Committee has distinguished between the collection of traffic data (trap and trace) and the interception of content traditionally covered by interception (wire tapping) orders. Both are considered indispensable law enforcement tools in the investigation of computer crime and it is recognised that in the field of international investigation the ability to obtain trap and trace information will be required much more speedily than has hitherto been the case. The Convention will therefore seek to clarify the conditions under which traffic data can be obtained very quickly from abroad while respecting sovereignty and privacy limitations.

Search and Seizure in a Computer Environment

16. The Committee has accepted the need for an international mechanism which permits the search of computer systems based abroad and seizure of data in a way that adequately responds to the urgency of investigations given the volatile nature of computer data. A Canadian paper which has been prepared to inform the Council of Europe discussions on this subject was also submitted to the High-Tech Sub-Group of the G8. Further discussion is therefore likely to mirror that taking place in the G8.

Jurisdiction

17. The growth of international computer networks and their use by criminal organisations gives rise to problems of jurisdiction. During the course of a criminal enterprise an offender may access a network in one country, store data in another, and the effects of his criminality be felt in a third. Problems such as territoriality, dual criminality and double jeopardy may arise. Clear principles must therefore be established which will resolve conflicts of jurisdiction.

International Co-operation

18. The Committee considers that specific mechanisms of international co-operation will be necessary for the prosecution of high-tech crimes and the trans-border application of coercive powers. International treaties will need to have the widest ratification possible in order to avoid the creation of data havens. National structures, both law enforcement and judicial, will need to be capable of providing prompt assistance.

19. These broad aims taken together with the other subjects previously discussed will form the basis of the proposed Convention's international co-operation provisions. A drafting group has been established to prepare a preliminary text of the Convention for the next plenary meeting of the Committee. Completion is due by the end of 1999.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)

20. The OECD has issued guidelines governing the protection of privacy and the trans-border flow of personal data. All 29 Member States of the OECD have endorsed the guidelines. In addition the OECD was the first international body to attempt to deal with the criminal law problems related to computer crime. An ad hoc committee, following a comparative

analysis of substantive law of the Member States, suggested a list of offences which could be adopted by the Member States. The list of offences is similar to that now being considered by the Council of Europe.

21. The OECD and in particular its Committee for Information, Computer and Communications Policy (ICCP) is currently undertaking a study aimed at reviewing the existing legislation and practices in Member States concerning the internet and in particular illegal and harmful content. The study is expected shortly. The OECD has also issued guidelines for cryptography policy which recognise the significance of cryptography with regard to the development of electronic commerce whilst acknowledging the requirement for law enforcement to be able to uncode data.

The European Union

22. A great deal of work on high-tech crime is being done in the European Union and the following is intended to be representative rather than exhaustive. The EC Data Protection Directive with regard to progress of personal data and the Telecommunication Data Protection Directive, both of which have an implementation date of October 1998, are particularly important as they cover among other things:

- principles relating to processing of data;
- codes of conduct;
- confidentiality of communications;
- traffic and billing data.

23. Also important is the Council Resolution (adopted on 17 February 1997) on Illegal and Harmful Content on the Internet. The Resolution invites Member States to:

- encourage and facilitate self-regulatory systems including representative bodies for internet service providers and users, effective codes of conduct and possibly hot line reporting mechanisms available to the public;
- encourage the provision to users of filtering mechanisms and the setting up of rating systems, eg the PICS standard;
- foster co-ordination at Community level of self-regulatory and representative bodies;

- promote and facilitate the exchange of information on best practice in this area;
- consider further the question of legal liability for internet content;
- recommend that the Commission and Member States take all necessary steps to enhance the effectiveness of the measures referred to in this Resolution through international co-operation and in discussions in other international forums. The Commission's communication in response to the Resolution recommends suitable measures for implementation by Member States.

24. Other relevant instruments include the 1995 Council Resolution on Interception of Telecommunications, associated work on intercepting the internet, and the Commission communication "Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption", all of which are being progressed in the Police Co-operation Working Group.

25. The Presidency draws attention to the study contracted by the European Commission entitled "Legal Aspects of Computer-related Crime in the Information Society" - the Comcrime Study. The Presidency, in common with other Member States, has only recently received the report but recognises that it is, without doubt, the most comprehensive study undertaken. It also makes a comprehensive set of recommendations to fight computer crime. **The Presidency believes that the Comcrime study probably precludes the need for any further study as envisaged by the High Level Group's Action Plan (Recommendation 5).**

Next Steps

26. The Comcrime Study recognises that the fight against crime in today's international information society requires an integrated international response. As illustrated in this paper a great deal of valuable work is being done in various international fora which is not co-ordinated at a supra-national level. **The Study suggests the organisation of a joint conference or workshop of the major players including the European Union, Council of Europe, G8, OECD, Interpol and the United Nations, with the aim of bringing together and co-ordinating their work. A decision should then be taken on how far the EU should develop the proposals mentioned in this study on its own or whether it should refer to proposals of other international bodies. The Presidency is in favour of this course of action.**

27. There are however a number of measures which members of this group can take now which would assist the future work of any conference or workshop.

1. **Members are invited to make use of the G8's network of 24-hour points of contact, and to provide similar details for inclusion in a future edition of the directory.**

2. The Resolution on illegal and harmful content on the internet and the Commission communication related to it mentioned earlier in this report (para 22) taken together with measures initiated in the G8 (para 8), make recommendations for co-operation with industry. The recent paper from the Netherlands delegation to the Police Co-operation Working Group (Enfopol 23) reports encouraging progress by Member States in introducing practical measures to enhance such co-operation. **The Presidency would like to take these measures further and recommends the establishment of an industry network of 24-hour points of contact with which law enforcement can interface.**

   It is known that the industry already exchanges information (for example traffic data) domestically to prevent fraud, to address customer complaints, and for other reasons. The intention would be to encourage such co-operation on an international basis where necessary, through a single point of contact, to assist law enforcement in investigations. It would not be the intention, at least initially, to allow law enforcement from one Member State to contact the industry representative in another without following the usual protocols. The extent to which this might be possible in the future is likely to be decided by this group as co-operation in and between both networks develops. Much will depend on the willingness of industry to accept this proposal and subject to their approval an industry directory of contacts similar to that for law enforcement can be circulated to participant countries as appropriate.

   The establishment of these two networks would do much to enhance mutual understanding and co-operation in criminal investigation and combined with other industry measures is likely to lead to more informed solutions to the problems identified in the Comcrime study.

3. Crime using computer networks will continue to grow and criminals will no doubt find innovative ways of using new technology. The Presidency was impressed with an initiative raised by the Danish delegate during discussion on high-tech matters at the January meeting of the Multi-Disciplinary Group to establish an

"early warning system" which would inform the international law enforcement community of such use. **The Presidency believes this is a useful idea which should be taken forward as soon as possible and would welcome the views of Member States as to how such a mechanism can be put in place.** Perhaps the 24-hour points of contact network could be useful for this purpose or, alternatively, Europol may have a useful role to play.

28. The Presidency commends the Commission for its foresight in ordering this study (launched before the Council decision of last April and the Amsterdam Summit) and invites the Multi-Disciplinary Group to endorse the principle that the solution to the problems of computer crime can only be achieved through concerted international action.

29. **We therefore recommend that the conference or workshop recommended in the Comcrime report be convened to establish a work programme based on the measures identified in the study for endorsement by the Multi-Disciplinary Group. If the MDG agrees the Presidency, in close consultation with Austria as incoming Presidency, the Commission and with the assistance of the Secretariat, will initiate discussions with other relevant fora on the preparation of such a conference.**

30. The work programme should clearly identify First and Third Pillar responsibility whilst avoiding duplication of effort in the various international fora. The Multi-Disciplinary Group can then decide whether this course of action meets the aspirations of the European Union.
