COUNCIL OF THE EUROPEAN UNION

Brussels, 24 April 2001 (30.04)

8123/01

LIMITE

ENFOPOL 38

NOTE

from:	French delegation
to:	Police Cooperation Working Party
No. prev. doc. :	11357/00 ENFOPOL 62 + COR 1
Subject :	Computer crime – Summary of replies to the questionnaire (11357/00 ENFOPOL 62 + COR 1)

Questionnaire Enfopol 62, a joint initiative of the French and Swedish delegations, was distributed in the Police Cooperation Working Party under the French Presidency on 28 November 2000 with the aim of drawing up an inventory of legislation in force in the Member States and a statistical evaluation of information technology crime.

Although the European Union Member States have no legal definition of computer crime to propose, there is unanimous agreement on the distinction between computer-targeted offences and offences committed through the medium of computers.

The summary of replies to this questionnaire is set out as follows:

1. Analysis of national legislation in relation to information technology as the target of an offence.
2. Information technology as a tool in committing offences.
3. Legal and/or voluntary obligations of those operating in the information technology sector.
4. The EU Member States' wishes in combating cyber-crime.
5. Analysis of Member States' statistics.
6. Conclusion.

1 – Information technology as the target of offences:

Offences against information technology damage both computerised data systems and the confidentiality, integrity or availability of the data they contain.
Most of the Member States have therefore adopted legislation embodying the main features of Council of Europe Recommendation R(89) 9.

Portugal has opted for a straightforward transposition of Recommendation R(89) 9 into national law, incorporating into its Penal Code the offence of unlawful access to a computerised data system. On this point the provisions are akin to the German legislation, making such activity a criminal offence only when directed against an information system specifically protected, which seems to follow the spirit of the European Recommendation ("…in violation of security rules"). The United Kingdom, France, Luxembourg and Belgium propose comparable criminalisation, but without any specific protection of the communication system being required.

Italy takes a different approach by introducing two aggravating factors, one concerning the status of the perpetrator if an agent of the State is concerned, and the other the victim concerned, such as a military target. The same applies to French legislation on espionnage.

It should be pointed out that such unlawful access does not always constitute an offence: Austria has still not made unauthorised access to a computer system or network a criminal offence.

The second significant aspect of computer crime is the protection of data contained in an information system, or the endangering of the system itself.

Here legislation tends to coincide. In each case specific offences have been created to cover such attacks, the UK legislation defining denial-of-service attacks as intentionally overloading the communications to the system or network, or they have been assimilated to ordinary offences.
In a few cases the provisions distinguish between types of criminal behaviour in order to define the acts committed more precisely in criminal terms. Swedish legislation, for instance, defines the same offence as breach of data secrecy, illegal dispossession or harmful offence, depending on the behaviour of the perpetrator. It boils down to taking account of the consequences of the offence, rather than the offence itself.

Taking European legislation as a whole, the conclusion is that computer data and programmes are adequately protected. However, if the aim remains to protect the data themselves, definitions in criminal terms vary enormously and there are many subtle differences from one set of legislation to another.

It should also be noted that such protection frequently involves the application of a number of legislative texts rather than a specific provision. Austria draws a distinction based on the aim sought, giving rise either to the offence of damage to data or to that of fraud through data manipulation. The latter also satisfies the criterion of computer-related fraud provided for in the brief list in Recommendation R(89) 9.

Germany does not require any fraudulent intent for an offence to exist, although certain distinctions introduced by the German Penal Code seem to require such intent.

As regards software counterfeiting, computer programmes are generally considered to be intellectual products and are therefore protected by copyright. There is little divergence between legislation on this point: copies of software are regarded as ordinary forgeries, the specificity lying solely in the originality of the medium.

Nevertheless, some legislators have chosen to reinforce the usual provisions, with Sweden, for instance, in addition to the offence of traditional counterfeiting, making it illegal to sell or lease devices intended solely for facilitating unauthorised removal or circumvention of a device placed in order to protect a computer program against unauthorised reproduction. Most States have included specific offences in the telecommunications regulations to deal with fraud against telecommunications systems.

2 – Information technology as a tool in committing offences:

Apart from fraud against telecommunications systems or software counterfeiting as referred to above, a large number of ordinary offences can be committed using a computer or facilitated by the use of a network. One of the most commonly recorded information technology offences is fraud prompted by the perpetrator's potential financial gain. Fraud has become increasingly common with the rise in the number of Internet users.

Generally speaking, European legislation has adapted somewhat to the use of the Internet for illicit purposes. Conventional offences such as threats against persons, malicious accusations, the dissemination of pornographic messages or pictures involving one or more minors, etc., offences against property such as fraud, or offences categorised in France as media offences, such as incitement to commit crimes and offences, the denial of crimes against humanity, defamation, abuse, justification of and incitement to terrorism, can all be perfectly executed using information technology. For this reason the majority of European States have opted for assimilation rather than specification in criminalising ordinary criminal conduct using a new medium.

The adoption of broad, generic legislation for "conventional" offences is a protection against future aberrations. In fact, the differences between European bodies of legislation are more marked in the definition of specifically information-technology offences than in the treatment of more traditional crime that adapts to new methods of commission.

3 – The rights and obligations of those involved in new technology in the European area:

It should be made clear from the start that no State has made provision in its criminal procedure for a specific framework of investigation for the Internet and the digital networks that are only one of the components of the information system in the broad sense. This is certainly due to the fact that the combating of computer crime fits perfectly into the existing frameworks.

Moreover, European States have incorporated into their legislation provisions to safeguard the processing of personal data. In the majority of cases these provisions are implemented in a law on telecommunications and correspond to the proposals in Recommendations R(95) 4 and13 on the protection of personal data and to EC Directives 95/46 of 24/10/1995 and 97/66 of 15/12/1997. Operators must ensure that personal data are protected by adopting appropriate technical measures. Each operator is generally required to delete the traffic data or render them inaccessible at the end of each call (or at the latest when the time required for their commercial processing has elapsed).

The question of victims:

From an analysis of each body of legislation it appears that there is no obligation on the victims of computer-related crime to report the offence. However, this approach is clearly untenable where the offence has more serious consequences, particularly where it is likely to endanger persons. In this case the victim is bound to report the offence, on pain of himself being found guilty of an offence. This obligation is comparable to the concept of failure to assist a person in danger, which exists in most European countries' legislation.

Luxembourg has also introduced an obligation on financial sector operators to report offences in an attempt to combat money laundering. A similar obligation exists in other countries' legislation, without targeting a specific offence.

Obligations on service providers:

One of the bases for computer crime investigations are the connection data. These technical data alone can enable the law-enforcement officials to penetrate to the perpetrator or the source of the offence and are thus the virtually unavoidable starting-point for any investigation in the information technology area. The issue of storing connection data therefore seems crucial. Two apparently contradictory interests have to be reconciled:

– the protection of personal data and, more generally, respect for privacy;
– the need for investigators to have access to the data stored by the service providers for the purposes of the investigation.

At present the issue of the storage of connection data and the length of that storage is clearly the weak link in the fight against cyber-crime. As witness, few countries have a legal requirement concerning the length of time connection data must be kept.

The Netherlands requires Internet service providers to store connection data for three months following the initial processing. Belgian legislation also requires Internet service operators to store call data for a certain period, which may not be less than 12 months. Failure to comply is an offence punishable with a prison sentence. Subject to legislation not looked at, the other States have not adopted any provisions in the matter, but France is currently preparing a draft law requiring telecommunications and network operators to store connection data for twelve months.

While no legislative provisions exist, some States, such as the United Kingdom, have concluded informal arrangements with national service providers whereby the UK investigative departments hope that connection data will be stored for 12 months. Nevertheless, voluntary cooperation, however spontaneous, is always conditional on the good will of the operator and does not constitute a legal obligation.

Faced with the legislative vacuum, Italian service providers have adopted a self-regulation code involving active collaboration with the police. It should nevertheless be noted that a substantial number of operators spontaneously store such data for periods that range from one month to 18 months, where national legislation does not require them to destroy such data quickly, i.e. once the commercial imperatives no longer require them to be stored.

Investigators in the majority of Member States have access to data, via a court order, where those data have been stored.

4 – Member States 'wishes:

From an analysis of Member States' replies it is possible to draw up a list of subjects which the law enforcement authorities would like to see the European institutions tackle in the near future in the context of a policy to combat computer crime:

- The Member States are seeking standardisation or at least harmonisation of legislation, at any rate as regards its basic legal principles, given that the 1989 Recommendation of the Council of Europe, on which the national legislation of many Member States is based,is not binding. On the other hand, ratification and implementation of the draft Convention (PC-CY) of the Council of Europe would represent considerable progress in the fight against computer crime, particularly since the European Community could accede ex officio to this criminal law Convention aimed at combating network crime.

- The provisions relating to technical data, where they exist, are too diverse. All the representatives considered that access and on-line service providers should be obliged to store connection data for a minimum period. As regards the length of storage, the Belgian example, providing for a minimum period of 12 months, appears to be the most balanced solution both from the point of view of the principle of the protection of privacy and in terms of the need for judicial investigation in order to respect the right of victims to obtain compensation for damage suffered.

- At a technical level, it would be necessary to encourage the industry to speed up the establishment of version 6 of the Internet protocol (IPv6) having regard to the new safeguards proposed to achieve a considerable reduction in piracy via the Internet.

- It is also imperative that a solution be found to the problems raised by the various forms of anonymity on the World Wide Web, the most significant example being cybercafés, which have been the source of a number of cases of fraud.

- Developing cooperation between the private sector of manufacturers and laboratories, universities and state bodies in order to provide appropriate responses to questions raised by a new technology or the emergence of a new mode of operation used by cyber criminals.

- The creation at European level of an observatory or cell for the protection of networks, a body to centralise information on the various types of attack recorded on the network which is able to give sound advice on the security standards to be adopted and which is sufficiently operational to give advance warning of any threat.

- The holding (twice a year) of a seminar such as the one which took place in Poitiers (France) in November 2000 (Investigation in cyberspace) which would bring together experts and representatives of the European Union in order to conduct a review, at regular intervals, of computer crime and to pool ideas and any new investigative techniques, an exercise which is indispensable if genuine and practical harmonisation of European legislation is to be achieved.

5 – Computer crime in Europe

Traditionally, a distinction is made between three forms of crime: actual, visible and convicted. Actual crime consists of all crimes and offences committed by a given population at a particular period of time, whether or not those illegal acts were reported and prosecuted. Visible crime is that brought to the attention of the judicial authorities, particularly the police. Finally, convicted crime refers to illegal acts which have resulted in a criminal conviction by a court of law.

Computer crime is characterised by a very marked difference between actual crime as it can be assessed through surveys of companies carried out by private bodies, and visible crime. In France it is estimated that there are between 30 000 and 40 000 attacks a year on computer systems in mainland France, whereas in 1999 no more than 105 official complaints were recorded in this field.

That very great difference between actual and visible crime has a number of causes:

– the invisibility of such crime; in the case of most intrusions the firms or individuals are unaware that they have been attacked;
– the absence of any legal obligation on victims to make a complaint before they can obtain compensation for damage from their insurance company;
– the reluctance on the part of companies to report to judicial or police authorities the fact that they have been the victim of computer crime, for fear of having weaknesses in their computer systems revealed, with resultant damage to their company image.

These various factors contribute to a major hidden statistic for actual crime, which is taken into account only very partially by law-enforcement agencies.

The information on computer crime provided by the Member States in response to the European Union questionnaire therefore concerns only visible crime, which is statistically measurable by means of the facts reported to the police.

Globally, the extent of computer crime is difficult to assess because in some Member States there is no system for the centralisation of information so that reliable, consistent and regularly updated figures may be obtained or else the compilation of statistics was initiated only in 2000.

Four countries, Italy, Luxembourg, the Netherlands and Portugal, stressed the difficulties involved in the collection of such information in the absence of a body specifically responsible for the collection, centralisation and processing of statistics. That is the main reason why those countries cannot provide figures in the field of computer crime.

Although they have no body that centralises statistics, Belgium, Denmark and Greece nevertheless provide figures for the activities of their agencies specialising in computer crime, which are either criminal investigation or technical assistance departments. That information is sufficient, however, to give an idea of this new form of crime in those countries.

Austria, France and the United Kingdom are able to provide statistics of attacks on computer systems, but not of computer-related crime, i.e. those cases in which computer technology is used as a tool in committing the offence, as the operating methods that identify and characterise these forms of offences are not generally taken into account in national statistics. Germany supplied the most comprehensive statistics.

In addition, it must be noted that the manner in which police forces are organised in the Member States, whether centralised or not, national, federal or regional, influences the statistics communicated.
For example, the data that the United Kingdom provided concerned only England and Wales.

Another difficulty with the precision of the data collected concerns the main description used by the department responsible for the collection of statistical data in the event of compound offences. In the case of a fraud perpetrated by means of fraudulent access to a computer system, for example, the conventional offence of fraud is more likely to be used than that of computer crime.

Furthermore, the statistical tools used are not sufficiently precise. The concept of "fraud" would appear to be too vague, as it can be applied not only to the fraudulent use of bank cards but also to intrusions and the alteration of data, etc. In parallel with an effort of semantic definition, the quantitative analysis of computer crime therefore ought to be combined with qualitative analysis that is both more precise and more relevant.

In general, the measurement of computer crime is tricky because of the variability of the descriptions used by different European legislations. Some clarification will be required to refine the different concepts of computer crime, which is made sufficiently complex by its multiple aspects for it to be impossible to find or even invent a universal definition. That is the reason for the formal approach adopted in 1989 by the Council of Europe, whose Recommendation ought to be brought up to date in order to take into account the new offences that have come into being because of digital networks in general and the Internet in particular.

6 – Conclusion

In conclusion, it can be seen that at the beginning of the third millenium computer crime is developing extremely well in a supranational context in which national criminal law is generally inappropriate and Community law is still at the embryonic stage.

The speed at which a criminal law system common to all the countries of the European Union is developed to combat this new form of crime will determine the success of the fight against the computer crime affecting telecommunications networks across frontiers. Measures are needed to harmonise national laws and produce a statistical tool for use by all Member States so that computer crime in Europe can be measured quantitatively and qualitatively.

The draft Council conclusions (7277/01 ENFOPOL 23 ECO 101) raise the problem of connection data, and if those conclusions are adopted they could form the important first stage in the implementation of the measures necessary to enable the judicial and police authorities to investigate criminal acts committed by means of electronic communications systems.

The second stage could be the implementation of the Commission proposals, as presented to the Police Cooperation Working Party at its meeting on 6 April 2001 [COM(2000) 890], i.e. increasing system security, improving mutual knowledge in the field of computer crime and training law-enforcement agencies' investigators in the field of cyberspace.

COMPUTER CRIME OFFENCES															
COUNTRY	Counterfeiting			Telephone use			Miscellaneous fraud			Attacks on computer systems and data			Personal data protection		
	1997	*1998*	*1999*	*1997*	*1998*	*1999*	*1997*	*1998*	*1999*	*1997*	*1998*	*1999*	*1997*	*1998*	*1999*
A										**9**	**10**	**16**			
B		**2**	**5**					**1**	**9**		**3**	**5**			
D	**1318**	**1151**	**2224**	**6506**	**6465**	**4474**		**2458**	**1536**	**400**	**593**	**512**			**37**
DK		**2**	**86**				**31**	**49**	**84**	**31**	**73**	**894**		**3**	**4**
F	**51**	**80**	**75**	**291**	**304**	**357**	**284**	**488**	**679**	**82**	**78**	**100**	**9**	**9**	**7**
GB										**7**	**16**	**13**			
GR	**1**	**1**	**0**						**1**						
LUX															
SW										**157**	**199**	**304**			
Total	**1370**	**1236**	**2390**	**6797**	**6769**	**4831**	**315**	**2996**	**2309**	**686**	**972**	**1844**	**12**		**48**

OFFENCES INVOLVING THE USE OF THE INTERNET FOR ILLEGAL PURPOSES									
COUNTRY	Child pornography			Use of bank account numbers			Frauds, trafficking, racism		
	1997	*1998*	*1999*	*1997*	*1998*	*1999*	*1997*	*1998*	*1999*
AU							**53**	**8**	**37**
B		**58**	**287**						**10**
D			**2002**						**90**
DK		**2000**	**3003**						
F	**32**	**55**	**58**	**351**	**779**	**2287**	**30**	**94**	**125**
GB									
GR	**1**	**2**	**1**	**4**	**7**	**11**	**4**	**6**	**3**
LUX						**2**			
SW							**849**	**673**	**1300**
Total		**2115**	**5351**	**355**	**786**	**2300**	**936**	**781**	**1565**