COUNCIL OF THE EUROPEAN UNION

Brussels, 15 September 2000

11357/00

LIMITE

ENFOPOL 62

TRANSLATION PROVIDED BY THE PRESIDENCY

NOTE

from :	Presidency
to :	Police Cooperation Working Party
No. prev. doc. :	10252/00 ENFOPOL 52 ECO 210
Subject :	High-technology crime - Questionnaire

The widespread usage of data processing and communication devices in our society nowadays has become a major ingredient of human and economic growth. The increasing number of offences involving telecommunication devices or computers, used as a mean or as a target itself, at the expense of telecom operators or service providers, and even citizen, does not only impede development of information society but also violates the right to individual privacy.

Detecting and containing such high-tech related crime has become even more difficult with the advent of cross-border crime.

This is the reason why a higher level of co-ordination of methods and means used to deal with the problem is necessary, to better consider and tackle such crime and guarantee therefore smooth progress of information society.

The attached questionnaire shall enable us to make an analysis of the situation on a European scale, and to draw up a report to inform the EU authorities with the aim of rising their awareness on the issue.

As far as possible, replies have to be sent before November 23rd, 2000, to the following address:

Service de **C**oopération **T**echnique **I**nternationale de la **P**olice
Division de la **C**oopération **M**ultilatérale
Bureau de l'Union européenne
101 rue des Trois Fontanot
92000 Nanterre
France

Fax + 33 1 40 97 88 23

Would you need any further information, please contact:
Corinne.GIANNONE@interieur.gouv.fr
Tel + 33 1 40 97 83 16

Hugues.GIBAUD@interieur.gouv.fr
Tel + 33 1 40 97 86 79

Annex

STATISTICS – QUESTIONNAIRE

1. Legal aspects on Computer crime, High-tech crime or Information Technology crime (hereafter referred to as Computer crime) or criminality related to Computer crime.

1.1. Please describe your legal system concerning criminality in computers or against computer-systems (computer crime) including when a computer or a computer-system has been used as a tool to commit the crime.

If you have specific legal definition(s) please specify (In the sense of criminality where a computer system is the target of an offence)

1.2. What kind of offence your legislation (if any), has planned to prosecute the following processes:

- 1.2.a. Unauthorised access to a data processing system
- 1.2.b. Hacking data processing systems (e.g. a Trojan horse, logical bomb, virus, worms).
- 1.2.c. Obstructing operation of data processing systems
- 1.2.d. Counterfeiting software
- 1.2.e. Fraud against telecommunications systems
- 1.2.f. Others, please specify:

1.3. What is your legal definition (if any) of information technology related crime? (In the sense of criminality where a computer system is a tool used to commit an offence)

- 1.3.a. If the use of telecommunication devices or digital networks as a mean to commit a major offence considered a specific offence in itself?

1.3.b. In that case, are there any aggravating circumstances by law?

1.3.c. Is there any specific type of investigation to be carried out in such cases, for example legal or technical procedures urged by law?

1.4. Are there other offences related to telecommunication or digital networks fraud which you have not mentioned when answering the questions under point 1.2 and 1.3 (for example breach against personal privacy and protection of personal data)?

1.5. What are the legal duties of operators to guarantee privacy of individual data? (E-mails, favourite sites, PIN number, etc…)

1.6. Are the victims (users, telecom operators, service providers, banks) bound by law to denounce the deeds?

1.7. Is there a legal duty for Internet service providers to store the connection data? If yes, for how long?

1.8. How can the law enforcement agencies have access to these data

1.9. Is your legislation relative to lawful interception of communications applicable to new information technologies? (i.e. S-PCS Satellites, Internet)

1.10. What are the rights and duties (or restrictions) of service providers and/or telecommunication operators when intercepting communications or identifying offenders?

2. Statistics of offences related to information technologies

2.1. What are the services or bodies in charge of collecting and centralising such statistical data?

2.2. In view of the future analysis of collected data, could you precise the criterias taken into account for your statistics when listing the offences mentioned under point 1.2

- Assessing complaint?
- Assessing judicial/police procedure?
- Assessing the number of identified victims?

3. National figures for 1997, 1998 and 1999:

3.1. Computers used as a device for committing offences:

3.1.a. forged means of payment

3.1.b. forged money

3.1.c. falsified administrative documents

3.1.d. other false documents

3.1.e. swindling

3.1.f. others

3.2. Use of communication networks for unlawful reasons:

3.2.a. paedophilia

3.2.b. child prostitution

3.2.c. credit card fraud

3.2.d. incitement to racial hatred

3.2.e. incitement to/propaganda for terrorism

3.2.f. incitement to drug usage

3.2.g. drug trafficking

3.2.h. other types of smuggling

3.2.i. money laundering

3.2.j. others

4. Relations with telephone operators and service providers

4.1 Apart from legal obligations, what are the main problems, detectives have to face in their investigations: identification and localisation of offenders, access to connection data, interception, variety and diversity of protocols used, sorting and exploiting data.

4.2 Who (or which institution) has the forensic responsibility for the analysis of seized soft and/or hardware or for the authenticity of seized Internet data?

5. Perspectives

5.1. Which aspects -technical, legal and/or co-ordination of investigation services- should be highlighted by the EU to guarantee security of data exchange and to avoid uprise in crime eased by the advent of new technologies? (please enumerate by priority order)

5.2. Which public or private players, including EU bodies and working groups, have to be associated to such measures? (please specify, for each of them, the purpose of their alliance)

6. Are there any governmental projects or initiatives regarding protection, warning and response to cyber attacks in your country?