COUNCIL OF THE EUROPEAN UNION

Brussels, 28 February 2003

6946/03

LIMITE

DROIPEN 12
TELECOM 31

Interinstitutional File: 2002/0086 (CNS)

OUTCOME OF PROCEEDINGS

of :	Council
on :	27 and 28 February 2003
No. prev. doc. :	6671/1/03 REV 1 DROIPEN 11 TELECOM 25
No. Cion prop. :	8586/02 DROIPEN 29 ECO 143 (COM (2002) 173 final)
Subject :	Proposal for a Council Framework Decision on attacks against information systems

During its meeting on 28 February 2003, the JAI Council examined the above proposal on the basis of 6671/1/03 REV 1 DROIPEN 11 TELECOM 25.

The JAI Council reached a general approach on the text in Annex I, subject to the following:

- The lifting by the Irish, French, Swedish, Danish and Netherlands delegations of their parliamentary reservations;
- The examination of the opinion of the European Parliament in the light of the general approach reached by the Council;
- The examination of the recitals on the basis of the text in Annex I which will be carried out in conformity with the interinstitutional agreement on the drafting of legislative texts.

Annex II of this document contains a declaration made by the Commission concerning Article 6.
Changes to the text are underlined as compared to 6671/1/03 REV 1 DROIPEN 11 TELECOM 25.

ANNEX I

Proposal for a
COUNCIL FRAMEWORK DECISION
on attacks against information systems

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Articles 29, 30(1)(a), 31 and 34(2)(b) thereof,

Having regard to the proposal of the Commission[1],

Having regard to the opinion of the European Parliament[2],

Whereas:

(1) The objective of this Framework Decision is to improve co-operation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems.[3]

(2) There is evidence of attacks against information systems, in particular as a result of the threat from organised crime, and increasing concern at the potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States. This constitutes a threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, and therefore requires a response at the level of the European Union.

---

1 OJ C . . p .
2 OJ C . . p.
3 See footnote to Article 1.

(3) An effective response to those threats requires a comprehensive approach to network and information security, as underlined in the Europe Action Plan, in the Communication by the Commission "Network and Information Security: Proposal for a European Policy Approach"[1] and in the Council Resolution of 6 December 2001 on a common approach and specific actions in the area of network and information security.

(4) The need to further increase awareness of the problems related to information security and provide practical assistance has also been stressed in the European Parliament Resolution of 5 September 2001[2].

(5) Significant gaps and differences in Member States' laws in this area hamper the fight against organised crime and terrorism, and act as a barrier to effective police and judicial co-operation in the area of attacks against information systems. The trans-national and borderless character of modern electronic communication networks means that attacks against information systems are often international in nature, thus underlining the urgent need for further action to approximate criminal laws in this area.

(6) The Action Plan of the Council and the Commission on how to best implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice[3], the Tampere European Council on 15-16 October 1999, the Santa Maria da Feira European Council on 19-20 June 2000, the Commission in the Scoreboard[4] and the European Parliament in its Resolution of 19 May 2000[5] indicate or call for legislative action against high technology crime, including common definitions, incriminations and sanctions.

---

1 COM (2001) 298.
2 [2001/2098(INI)].
3 OJ C 19, 23.1.1999.
4 COM (2001) 278 final.
5 A5-0127/2000.

(7) It is necessary to complement the work performed by international organisations, in particular the Council of Europe's work on approximating criminal law and the G8's work on transnational co-operation in the area of high tech crime, by providing a common approach in the European Union in this area. This call was further elaborated by the Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions on "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime"[1].

(8) Criminal law in the area of attacks against information systems should be approximated in order to ensure the greatest possible police and judicial co-operation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism.

(9) The Framework Decision on the European Arrest Warrant[2], the Annex to the Europol Convention and the Council Decision setting up Eurojust contain references to computer-related crime which needs to be defined more precisely. For the purposes of such instruments, computer-related crime should be understood as including attacks against information systems as defined in this Framework Decision which provides a much greater level of approximation of the constituent elements of such offences. This Framework Decision also complements the Framework Decision on combating terrorism[3] which covers terrorist actions causing extensive destruction of an infrastructure facility, including an information system, likely to endanger human life or result in major economic loss.

(10) All Member States have ratified the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data. The personal data processed in the context of the implementation of this Framework Decision will be protected in accordance with the principles of the said Convention.

---

1 COM (2000) 890.
2 OJ C . . p.
3 OJ C . . p.

(11) Common definitions in this area, particularly of information systems and computer data, are important to ensure a consistent approach in Member States in the application of this Framework Decision.

(12) There is a need to achieve a common approach to the constituent elements of criminal offences by providing for a common offence of illegal access to an information system, and illegal interference with an information system.

(13) This Framework Decision requires Member States to establish the criminal offence of illegal access to information systems. However, it does not require Member States to establish the criminal offence *per se* of unauthorised viewing of television and cable broadcasts.

(14) In the interest of combating cybercrime, each Member State should ensure effective judicial cooperation in respect of offences based on the types of behaviour referred to Articles 2, 3, 4 and 5.

(15) There is a need to avoid over-criminalisation, particularly of trivial or minor conduct, as well as the need to avoid criminalizing right-holders and authorised persons such as legitimate private or business users, managers, controllers and operators of networks and systems, legitimate scientific researchers, and authorised persons testing a system, whether a person within the company or a person appointed externally and given permission to test the security of a system.

(16) There is a need for Member States to provide penalties for attacks against information systems which are effective, proportionate and dissuasive, including custodial sentences in serious cases;

(17) It is necessary to provide for more severe penalties when certain circumstances accompanying an attack against an information system make it an even greater threat to society.

In such cases, sanctions on perpetrators should be sufficient to allow for attacks against information systems to be included within the scope of instruments already adopted for the purpose of combating organised crime such as the 98/733/JHA Joint Action of 21 December 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union[1].

(18) Measures should be taken to enable legal persons to be held liable for the criminal offences referred to by this act which are committed for their benefit, and to ensure that each Member State has jurisdiction over offences committed against information systems in situations where the offender is physically present on its territory or where the information system is on its territory.

(19) Measures should also be foreseen for the purposes of co-operation between Member States with a view to ensuring effective action against attacks against information systems. Member States should therefore make use of the existing network of operational contact points for the exchange of information.

(20) Since the objectives of ensuring that attacks against information systems be sanctioned in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial co-operation by removing potential obstacles, cannot be sufficiently achieved by the Member States individually, as rules have to be common and compatible, and can therefore be better achieved at the level of the Union, the Union may adopt measures, in accordance with the principle of subsidiarity as referred to in Article 2 of the EU Treaty and as set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in the latter Article, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.

[1] OJ L 351, 29.12.1998, p. 1.

(21) This Framework Decision is without prejudice to the powers of the European Community.

(22) This Framework Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, and notably Chapters II and VI thereof.

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1

Definitions

For the purposes of this Framework Decision, the following definitions shall apply:

(a) *"Information System"* means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.

(b) *"Computer data"* means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.

(c) *"Legal person"* means any entity having such status under the applicable law, except for States or other public bodies in the exercise of State authority and for public international organisations.

(d) "*Without right*" means access or interference not authorised by the owner, other right holder of the system or part of it, or not permitted under the domestic legislation.

Article 2

Illegal access to Information Systems

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

2. Each Member State may decide that the acts referred to in paragraph 1 are incriminated only where the offence is committed by infringing a security measure.

Article 3

Illegal system interference

Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 4

Illegal data interference

Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

Article 5

Instigation, aiding and abetting and attempt

1. Each Member State shall ensure that the instigation of, aiding and abetting an offence referred to in Articles 2, 3 and 4 is punishable.

2. Each Member State shall ensure that attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable.

3. Each Member State may decide not to enforce paragraph 2 of this Article for the offences referred to in Article 2.

Article 6

Penalties

1. Each Member State shall take the necessary measures to ensure that the conduct referred to in Articles 2, 3, 4 and 5 is punishable by effective, proportionate and dissuasive criminal penalties.

2. Each Member State shall take the necessary measures to ensure that the conduct referred to in Articles 3 and 4 is punishable of a maximum of at least between 1 and 3 years of imprisonment.

Article 7

Aggravating circumstances

1. Each Member State shall take the necessary measures to ensure that the conduct referred to in Articles 2 paragraph 2 , 3 and 4 is punishable by criminal penalties of a maximum of at least between 2 and 5 years of imprisonment when committed within the framework of a criminal organisation as defined in Joint Action 98/733/ JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member States of the European Union, apart from the penalty level referred to therein.

2. A Member State may also take the measures referred to in paragraph 1 when the conduct has caused serious damages or has affected essential interests.

Article 8

Liability of legal persons

1. Each Member State shall take the necessary measures to ensure that legal persons can be held liable for conducts referred to in Articles 2, 3, 4 and 5, committed for their benefit by any person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

   (a) a power of representation of the legal person, or
   (b) an authority to take decisions on behalf of the legal person, or
   (c) an authority to exercise control within the legal person.

2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable where the lack of supervision or control by a person referred to in paragraph 1 has made possible the commission of the offences referred to in Articles 2, 3, 4 and 5 for the benefit of that legal person by a person under its authority.

3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are involved as perpetrators, instigators or accessories in the conduct referred to in Articles 2, 3, 4 and 5.

Article 9

Sanctions for legal persons

1. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(1) is punishable by effective, proportionate and dissuasive sanctions, which shall include criminal or non-criminal fines and may include other sanctions, such as:

a) exclusion from entitlement to public benefits or aid;

b) temporary or permanent disqualification from the practice of commercial activities;

c) placing under judicial supervision; or

d) a judicial winding-up order.

2. Each Member State shall take the necessary measures to ensure that a legal person held liable pursuant to Article 8(2) is punishable by effective, proportionate and dissuasive sanctions or measures.

Article 10

Jurisdiction

1. Each Member State shall establish its jurisdiction with regard to the conduct referred to in Articles 2, 3, 4 and 5 where the conduct has been committed:

(a) in whole or in part within its territory; or

(b) by one of its nationals ; or

(c) for the benefit of a legal person that has its head office in the territory of that Member State.

2. When establishing jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that it includes cases where:

(a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory.

3. A Member State which under its laws, does not as yet extradite or surrender its own nationals shall take the necessary measures to establish its jurisdiction over and to prosecute, where appropriate, the conduct referred to in Articles 2 to 5 in cases when it is committed by one of its nationals outside its territory.

4. Where an offence falls within the jurisdiction of more than one Member State and when any of the States concerned can validly prosecute on the basis of the same facts, the Member States concerned shall co-operate in order to decide which of them will prosecute the offenders with the aim, if possible, of centralising proceedings in a single Member State. To this end, the Member States may have recourse to any body or mechanism established within the European Union in order to facilitate co-operation between their judicial authorities and the co-ordination of their action. Sequential account may be taken of the following factors:

- the Member State shall be that in the territory of which the acts has been committed according to Article 10 paragraph 1 (a) and paragraph 2;
- the Member State shall be that of which the perpetrator is a national;
- the Member State shall be that in which the perpetrator has been found.

5. A Member State may decide not to apply, or to apply only in specific cases or circumstances, the jurisdiction rule set out in paragraphs 1(b) and 1(c).

6. Member States shall inform the General Secretariat of the Council and the Commission accordingly where they decide to apply paragraph 5, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

Article 11

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 2, 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they make use of the existing network of operational points of contact available twenty four hours a day and seven days a week.

2. Each Member State shall inform the General Secretariat of the Council and the Commission of its appointed point of contact for the purpose of exchanging information on offences relating to attacks against information systems. The General Secretariat shall notify that information to the other Member States.

Article 12

Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision by […][1].

2. By the same date Member States shall transmit to the General Secretariat of the Council and to the Commission the text of any provisions transposing into their national legislation the obligations imposed on them under this Framework Decision. By 31 December 2004 at the latest on the basis of a report drawn up on the basis of information and a written report from the Commission, the Council shall assess whether Member States have taken the necessary measures in order to comply with this Framework Decision.

Article 13

Entry into force

This Framework Decision shall enter into force on the date of its publication in the *Official Journal of the European Union*.

Done at Brussels,

For the Council

The President

---

[1] Date to be inserted.

ANNEX II

Declaration for inclusion in the minutes of the Council at the adoption of the draft Framework Decision on attacks against information systems.

The Commission regrets that Article 2 paragraph 2 of the Framework Decision does not provide for a minimum level of penalty for the illegal access offence as defined in Article 2.