



**COUNCIL OF
THE EUROPEAN UNION**

**Brussels, 17 January 2005
(OR. en)**

15010/04

**Interinstitutional File:
2002/0086 (CNS)**

**DROIPEN 64
TELECOM 170**

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject : Council Framework Decision on attacks against information systems

COUNCIL FRAMEWORK DECISION 2005/ /JHA
of

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(1)(e) and 34(2)(b) thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Parliament ¹,

¹ OJ C 300 E, 11.12.2003, p. 26.

Whereas:

- (1) The objective of this Framework Decision is to improve cooperation 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.
- (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.
- (3) An effective response to those threats requires a comprehensive approach to network and information security, as underlined in the *eEurope* Action Plan, in the Communication by the Commission "Network and Information Security: Proposal for a European Policy Approach" and in the Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security ¹.
- (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.

¹ OJ C 43, 16.2.2002, p. 2.

- (5) Significant gaps and differences in Member States' laws in this area may hamper the fight against organised crime and terrorism, and may complicate effective police and judicial cooperation in the area of attacks against information systems. The trans-national and borderless character of modern information systems means that attacks against such systems are often trans-border 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 ¹, 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" and the European Parliament in its Resolution of 19 May 2000 indicate or call for legislative action against high technology crime, including common definitions, incriminations and sanctions.
- (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 cooperation 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 OJ C 19, 23.1.1999, p. 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 cooperation in the area of criminal offences related to attacks against information systems, and to contribute to the fight against organised crime and terrorism.
- (9) 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 should be protected in accordance with the principles of the said Convention.
- (10) 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.
- (11) There is a need to achieve a common approach to the constituent elements of criminal offences by providing for common offences of illegal access to an information system, illegal system interference and illegal data interference.
- (12) In the interest of combating computer-related crime, each Member State should ensure effective judicial cooperation in respect of offences based on the types of conduct referred to in Articles 2, 3, 4 and 5.

- (13) There is a need to avoid over-criminalisation, particularly of minor cases, as well as a need to avoid criminalising right-holders and authorised persons.
- (14) There is a need for Member States to provide for penalties for attacks against information systems. The penalties thus provided for shall be effective, proportionate and dissuasive.
- (15) It is appropriate to provide for more severe penalties when an attack against an information system is committed within the framework of a criminal organisation, as defined in the Joint Action 98/733 JHA of 21 December 1998 on making it a criminal offence to participate in a criminal organisation in the Member State of the European Union ¹. It is also appropriate to provide for more severe penalties where such an attack has caused serious damages or has affected essential interests.
- (16) Measures should also be foreseen for the purposes of cooperation 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 referred to in the Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime ², for the exchange of information.

¹ OJ L 351, 29.12.1998, p. 1.

² OJ C 187, 3.7.2001, p. 5.

- (17) Since the objectives of this Framework Decision, ensuring that attacks against information systems be sanctioned in all Member States by effective, proportionate and dissuasive criminal penalties and improving and encouraging judicial cooperation by removing potential complications, cannot be sufficiently achieved by the Member States, 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 set out in Article 5 of the EC Treaty. In accordance with the principle of proportionality, as set out in that Article, this Framework Decision does not go beyond what is necessary in order to achieve those objectives.
- (18) This Framework Decision respects the fundamental rights and observes the principles recognised by Article 6 of the Treaty on European Union and reflected in 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 national 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 conduct referred to in paragraph 1 is 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 as a criminal offence.
2. Each Member State shall ensure that the attempt to commit the offences referred to in Articles 2, 3 and 4 is punishable as a criminal offence.
3. Each Member State may decide not to apply paragraph 2 for the offences referred to in Article 2.

Article 6

Penalties

1. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 2, 3, 4 and 5 are punishable by effective, proportional and dissuasive criminal penalties.
2. Each Member State shall take the necessary measures to ensure that the offences referred to in Articles 3 and 4 are punishable by criminal penalties 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 offence referred to in Article 2(2) and the offence referred to in Articles 3 and 4 are 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 apart from the penalty level referred to therein.
2. A Member State may also take the measures referred to in paragraph 1 when the offence 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 offences 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 commission of the offences referred to in Articles 2, 3, 4 and 5.

Article 9

Penalties 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 penalties, which shall include criminal or non-criminal fines and may include other penalties, 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 penalties or measures.

Article 10
Jurisdiction

1. Each Member State shall establish its jurisdiction with regard to the offences referred to in Articles 2, 3, 4 and 5 where the offence 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 its jurisdiction in accordance with paragraph (1)(a), each Member State shall ensure that the jurisdiction 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 law, 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 offences referred to in Articles 2, 3, 4 and 5, when 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 cooperate 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 cooperation between their judicial authorities and the coordination of their action. Sequential account may be taken of the following factors:

- the Member State shall be that in the territory of which the offences have been committed according to 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 rules set out in paragraphs 1(b) and 1(c).

6. Member States shall inform the General Secretariat of the Council and the Commission 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 forward that information to the other Member States.

Article 12

Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision by *

* Two years after the date of entry into force of this Framework Decision.

2. By * Member States shall transmit to the General Secretariat of the Council and to the Commission the text of any provisions transposing into their national law the obligations imposed on them under this Framework Decision. By **, on the basis of a report established on the basis of information and a written report by the Commission, the Council shall assess the extent to which Member States have complied with the provisions of this Framework Decision.

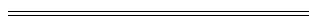
Article 13

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



* Two years after the date of entry into force of this Framework Decision.

** Thirty months after the date of entry into force of this Framework Decision.