

Proposal for a Council Framework Decision on attacks against information systems

(2002/C 203 E/16)

COM(2002) 173 final — 2002/0086(CNS)

(Submitted by the Commission on 19 April 2002)

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,

Having regard to the opinion of the European Parliament,

Whereas:

(1) 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.

(2) 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' ⁽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.

(3) 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 5th September 2001 ⁽²⁾.

(4) 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 cooperation 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.

(5) 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.

(6) 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' ⁽⁶⁾.

(7) 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.

⁽¹⁾ COM(2001) 298.

⁽²⁾ (2001/2098(INI)).

⁽³⁾ OJ C 19, 23.1.1999.

⁽⁴⁾ COM(2001) 278 final.

⁽⁵⁾ A5-0127/2000.

⁽⁶⁾ COM(2000) 890.

- (8) The Framework Decision on the European Arrest Warrant, 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 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.
- (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 will 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 a common offence of illegal access to an information system, and illegal interference with an information system.
- (12) There is a need to avoid over-criminalisation, particularly of trivial or minor conduct, as well as the need to avoid criminalising 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.
- (13) 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;
- (14) 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⁾.
- (15) 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.
- (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. Operational contact points should be established for the exchange of information.
- (17) 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 cooperation 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.
- (18) This Framework Decision is without prejudice to the powers of the European Community.
- (19) 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

Scope and objective of the Framework Decision

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.

⁽¹⁾ OJ L 351, 29.12.1998, p. 1.

*Article 2***Definitions**

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

- (a) 'Electronic communications network' means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable TV networks, irrespective of the type of information conveyed
- (b) 'Computer' 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.
- (c) 'Computer data' means any representation of facts, information or concepts which has been created or put into a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function.
- (d) 'Information System' means computers and electronic communication networks, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.
- (e) '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.
- (f) 'Authorised person' means any natural or legal person who has the right, by contract or by law, or the lawful permission, to use, manage, control, test, conduct legitimate scientific research or otherwise operate an information system and who is acting in accordance with that right or permission.
- (g) 'Without right' means that conduct by authorised persons or other conduct recognised as lawful under domestic law is excluded.

*Article 3***Illegal access to Information Systems**

Member States shall ensure that the intentional access, without right, to the whole or any part of an information system is punishable as a criminal offence where it is committed:

- (i) against any part of an information system which is subject to specific protection measures; or
- (ii) with the intent to cause damage to a natural or legal person; or
- (iii) with the intent to result in an economic benefit.

*Article 4***Illegal interference with Information Systems**

Member States shall ensure that the following intentional conduct, without right, is punishable as a criminal offence:

- (a) the serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data;
- (b) the deletion, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system where it is committed with the intention to cause damage to a natural or legal person.

*Article 5***Instigation, aiding, abetting and attempt**

1. Member States shall ensure that the intentional instigation of, aiding or abetting an offence referred to in Articles 3 and 4 is punishable.
2. Member States shall ensure that attempt to commit the offences referred to in Articles 3 and 4 is punishable.

*Article 6***Penalties**

1. Member States shall ensure that offences referred to in Articles 3, 4 and 5 are punishable by effective, proportionate and dissuasive penalties including a custodial sentence with a maximum term of imprisonment of no less than one year in serious cases. Serious cases shall be understood as excluding cases where the conduct resulted in no damage or economic benefit.
2. Member States shall provide for the possibility of imposing fines in addition to or as an alternative to custodial sentences.

*Article 7***Aggravating circumstances**

1. Member States shall ensure that the offences referred to in Articles 3, 4 and 5 are punishable by a custodial sentence with a maximum term of imprisonment of no less than four years when they are committed under the following circumstances:

- (a) the offence has been 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;
- (b) the offence caused, or resulted in, substantial direct or indirect economic loss, physical harm to a natural person or substantial damage to part of the critical infrastructure of the Member State;
- (c) the offence resulted in substantial proceeds; or

2. Member States shall ensure that the offences referred to in Articles 3 and 4 are punishable by custodial sentences greater than those foreseen under Article 6, when the offender has been convicted of such an offence by a final judgement in a Member State.

*Article 8***Particular circumstances**

Notwithstanding Articles 6 and 7, Member States shall ensure the penalties referred to in Articles 6 and 7 can be reduced, where, in the opinion of the competent judicial authority, the offender caused only minor damage.

*Article 9***Liability of legal persons**

1. Member States shall ensure that legal persons can be held liable for conducts referred to in Articles 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 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 commit offences or engage in the conduct referred to in Articles 3, 4 and 5.

*Article 10***Sanctions for legal persons**

1. Member States shall ensure that a legal person held liable pursuant to Article 9(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. Member States shall ensure that a legal person held liable pursuant to Article 9(2) is punishable by effective, proportionate and dissuasive sanctions or measures.

*Article 11***Jurisdiction**

1. Each Member State shall establish its jurisdiction with regard to the offences referred to in Articles 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 and the act affects individuals or groups of that State; 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 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).

4. Each Member State shall take the necessary measures also to establish its jurisdiction over the offences referred to in Articles 3 to 5 in cases where it refuses to hand over or extradite a person suspected or convicted of such an offence to another Member State or to a third country.

5. 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.

6. Member States shall inform the General Secretariat of the Council and the Commission accordingly where they decide to apply paragraph 3, where appropriate with an indication of the specific cases or circumstances in which the decision applies.

Article 12

Exchange of information

1. For the purpose of exchange of information relating to the offences referred to in Articles 3, 4 and 5, and in accordance with data protection rules, Member States shall ensure that they establish 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 13

Implementation

1. Member States shall bring into force the measures necessary to comply with this Framework Decision by 31 December 2003.

2. They shall communicate to the General Secretariat of the Council and to the Commission the text of any provisions they adopt and information on any other measures taken to comply with this Framework Decision.

3. On that basis, the Commission shall, by 31 December 2004, submit a report to the European Parliament and to the Council on the operation of this Framework Decision, accompanied where necessary by legislative proposals.

4. The Council shall assess the extent to which Member States have complied with this Framework Decision.

Article 14

Entry into force

This Framework Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Communities*.