EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0328/2002

4 October 2002

*

REPORT

on the Commission proposal for a Council framework decision on attacks against information systems
(COM(2002)0173 – C5-0271/2002 – 2002/0086(CNS))

Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

Rapporteur: Charlotte Cederschiöld

Symbols for procedures

*	Consultation procedure *majority of the votes cast*
**I	Cooperation procedure (first reading) *majority of the votes cast*
**II	Cooperation procedure (second reading) *majority of the votes cast, to approve the common position* *majority of Parliament's component Members, to reject or amend the common position*
***	Assent procedure *majority of Parliament's component Members except in cases covered by Articles 105, 107, 161 and 300 of the EC Treaty and Article 7 of the EU Treaty*
***I	Codecision procedure (first reading) *majority of the votes cast*
***II	Codecision procedure (second reading) *majority of the votes cast, to approve the common position* *majority of Parliament's component Members, to reject or amend the common position*
***III	Codecision procedure (third reading) *majority of the votes cast, to approve the joint text*

(The type of procedure depends on the legal basis proposed by the Commission)

Amendments to a legislative text

In amendments by Parliament, amended text is highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the legislative text for which a correction is proposed, to assist preparation of the final text (for instance, obvious errors or omissions in a given language version). These suggested corrections are subject to the agreement of the departments concerned.

CONTENTS

Page

PROCEDURAL PAGE

By letter of 12 June 2002 the Council consulted Parliament, pursuant to Article 39(1) of the EU Treaty, on the Commission proposal for a Council framework decision on attacks against information systems (COM(2002)0173 – 2002/0086(CNS)).

At the sitting of 13 June 2002 the President of Parliament announced that he had referred the proposal to the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs as the committee responsible and the Committee on Legal Affairs and the Internal Market and the Committee on Industry, External Trade, Research and Energy for their opinions (C5-0271/2002).

The Committee on Citizens' Freedoms and Rights, Justice and Home Affairs had appointed Charlotte Cederschiöld rapporteur at its meeting of 23 May 2002.

The committee considered the Commission proposal and the draft report at its meeting of 17 June 2002, 11 September 2002 and 3 October 2002.

At the last meeting it adopted the draft legislative resolution by 27 votes to 5, with 2 abstentions.

The following were present for the vote: Jorge Salvador Hernández Mollar (chairman), Giacomo Santini. (vice-chairman), Charlotte Cederschiöld (rapporteur), Giuseppe Brienza, Marco Cappato (for Maurizio Turco), Ozan Ceyhun, Carlos Coelho, Gérard M.J. Deprez, Giuseppe Di Lello Finuoli, Enrico Ferri (for Bernd Posselt), Adeline Hazan, Pierre Jonckheer, Timothy Kirkhope, Eva Klamt, Ole Krarup, Jean Lambert (for Alima Boumediene-Thiery), Baroness Sarah Ludford, Lucio Manisco (for Fodé Sylla), Bill Newton Dunn, Marcelino Oreja Arburúa, Elena Ornella Paciotti, Paolo Pastorelli (for Marcello Dell'Utri),Hubert Pirker, Martine Roure, Heide Rühle, Olle Schmidt (for Lousewies van der Laan), Ilka Schröder, Miet Smet (for Mary Elizabeth Banotti), Ole Sørensen (for Francesco Rutelli), Patsy Sörensen, The Earl of Stockton (for The Lord Bethell), Anna Terrón i Cusí, Christian Ulrik von Boetticher and Christos Zacharakis (for Thierry Cornillet).

The opinion of the Committee on Industry, External Trade, Research and Energy is attached. The Committee on Legal Affairs and the Internal Market decided on 28 May 2002 not to draw up an opinion.

The report was tabled on 4 October 2002.

The deadline for tabling amendments will be indicated in the draft agenda for the relevant part-session.

DRAFT LEGISLATIVE RESOLUTION

European Parliament legislative resolution on the Commission proposal for a Council framework decision on attacks against information systems (COM(2002)0173 – C5-0271/2002 – 2002/0086(CNS))

(Consultation procedure)

The European Parliament,

– having regard to the Commission proposal (COM(2002)0173[1]),

– having regard to Article 34(2)(b) of the EU Treaty,

– having been consulted by the Council pursuant to Article 39(1) of the EU Treaty (C5-0271/2002),

– having regard to Rules 106 and 67 of its Rules of Procedure,

– having regard to the report of the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs and the opinion of the Committee on Industry, External Trade, Research and Energy (A5-0328/2002),

1. Approves the Commission proposal as amended;

2. Calls on the Council to notify Parliament should it intend to depart from the text approved by Parliament;

3. Asks to be consulted again if the Council intends to amend the Commission proposal substantially;

4. Instructs its President to forward its position to the Council and Commission.

Text proposed by the Commission	Amendments by Parliament
Amendment 1 Recital 5 a (new)	
	(5 a) This framework decision and the definitions it employs, set out in Article 2, must be in agreement with, and where necessary extended to include, the new OECD Guidelines for the Security of Information Systems and Networks, adopted on 25 July 2002.

[1] OJ C

Justification

Self-explanatory.

Amendment 2
Recital 9

(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.	(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. ***At European level there is still at present a lack of adequate data protection provisions in the area of the third pillar. Hence an EU third pillar instrument for the protection of personal data, specifically in the context of law enforcement, is urgently needed.***

Justification

The existing Council of Europe Convention is no substitute for a data protection instrument at European level and in no way affects the need to introduce such an instrument. Parliament has repeatedly drawn attention to the need for a data protection instrument for the third pillar.

Amendment 3
Recital 13a (new)

	(13a) 1. The protection of information systems is a factor of fundamental importance for creating an area of freedom, security and justice, but the potential abuse of such systems must also be taken into account. National

legislation must therefore closely monitor attacks against and unlawful disruption of information systems used to achieve objectives which are contrary to fundamental freedoms and rights until such time as European human rights issues come under Community law and can then be dealt with more democratically by being taken into consideration when adopting European positions.

2. Likewise, conduct which is considered in national law to be of minor significance shall be exempt from the obligation to impose penalties under criminal law and is thus excluded from the scope of this framework decision.

Justification

Since respect for human rights does not have the same democratic protection in the EU as respect for the internal market, democratic responsibility for these issues must be clarified. There should be a possibility of greater leniency in respect of minor offences as a complement to the report's proposal to take account of the youth of offenders, which also exists at national level in most Member States' criminal law. The explanatory memorandum to the Commission's proposal also provides for the possibility of excluding minor offences from the scope of the framework decision.

Amendment 4
Recital 16

(16) 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. Operational contact points should be established for the exchange of information.	(16) 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. Operational contact points should be established for the exchange of information ***and should be activated as soon as there is an appropriate data protection instrument in the area of the third pillar at European level.***

Justification

Parliament has repeatedly drawn attention to the need for a data protection instrument for the third pillar. Only when such a data protection instrument exists, should data exchange in the area of criminal law be enforced at European level.

Amendment 5
Recital 19

(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.	(19) This Framework Decision respects the fundamental rights ***and freedoms*** and observes the principles recognised in particular by ***the European Convention for the Protection of Human Rights and Fundamental Freedoms and the case law of the European Court of Human Rights,*** the Charter of Fundamental Rights of the European Union, and notably Chapters II and VI thereof, ***and by national and international law on human rights and fundamental freedoms. Consequently, this framework decision and the national implementing measures cannot be used to suppress, in particular, freedom of opinion, expression, demonstration and association.***

Justification

Self-explanatory.

Amendment 6
Article 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.	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. ***This Framework Decision will respect fundamental rights and freedoms and will observe the principles of the European Convention on Human Rights and the fundamental freedoms established by the case law of the European Court of Human Rights, in the European Union's Charter of Fundamental Rights and in national and international law concerning human rights and fundamental freedoms.***

Justification

Since respect for human rights does not have the same democratic protection in the EU as respect for the internal market, democratic responsibility for these issues must be clarified.

Amendment 7
Article 1 a (new)

	(1 a) 1. In addition to the creation of offences covering the actions referred to in Articles 3, 4 and 5, prevention should also not be neglected, and Member States should help encourage participants in the Information Society increasingly to promote a culture of security, particularly by holding information campaigns, together with the affected employers, organisations and other actors, to raise awareness of security risks on information networks.
	2. The Commission shall take the initiative with a view to raising awareness among citizens, businesses and the public sector

	concerning security risks on electronic communication networks, and shall play a role in coordinating and harmonising the content of information campaigns in the Member States on the security aspects and risks involved in electronic communications networks.

Justification

Prevention is the first priority in increasing the security of our information networks. It is therefore important to promote a culture of security among citizens, businesses, authorities, schools and other institutions, in short among everyone who participates or will participate in the Information Society, by means of information, risk-assessment, reminding everyone who uses an information network of their personal liability, taking precautionary measures, and reacting correctly to attacks on information systems.

Amendment 8
Article 2(f)

(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.	***Deleted.***

Justification

Since the term "authorised person" is not used in the legislative text but only serves to explain the concept of lawfulness, it does not need to be defined separately.

Amendment 9
Article 2(g)

(g) "*Without right*" means that conduct by authorised persons or other conduct recognised as lawful under domestic law is	*(g)* "*Without right*" means that conduct by authorised persons or other conduct recognised as lawful under domestic law is

excluded.	excluded.
	Conduct by natural or legal persons is at all events not unlawful where they have 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 are acting in accordance with that right or permission.

Justification

Since the definition of authorised person proposed by the Commission serves only to determine the concept of lawfulness, it should be included here.

Amendment 10
Article 3, paragraph 1 a (new)

	2. The following are not included within the scope of application of this framework decision and are therefore a matter for the national law of the Member States:
	- minor or trivial behaviour;

Justification

The obligation to regard unlawful interference with information systems as a 'criminal offence' does not extend to minor or trivial behaviour (which would not be punished if it was carried out off line, i.e. without recourse to new technologies). The principle of subsidiarity requires us to avoid the risk of any over-criminalisation at European level with binding force.

Amendment 11
Article 4, paragraph 1 a (new)

	1a. The following are not included within the scope of application of this framework decision and are therefore a matter for the national law of the Member States:
	- minor or trivial behaviour;

Justification

The obligation to regard unlawful interference with information systems as a 'criminal offence' does not extend to minor or trivial behaviour (which would not be punished if it was carried out off line, i.e. without recourse to new technologies.). The principle of subsidiarity requires us to avoid the risk of any over-criminalisation at European level with binding force.

Amendment 12
Article 9, paragraph 2

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.	2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable***, where possible,*** 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.

Justification

The legal person exercises control within the limits of the framework imposed by the legislature, including those relating to liability and respect for privacy.

Amendment 13
Article 10(1), introduction

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:	Member States shall ensure that a legal person held liable pursuant to Article 9(1) is punishable by effective, proportionate and dissuasive sanctions, which ***may*** include criminal or non-criminal fines ***or*** other sanctions, such as:

Justification

The rapporteur considers that, in principle, legal persons should not be held liable under criminal law. The measures proposed in this context, however, are largely of an administrative and financial nature. However, the fundamental and comprehensive threat to the entire social structure which crime in this field represents justifies the proposed sanctions, though with the improvements suggested here.

Amendment 14
Article 11, second paragraph, point (a)

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

Justification

It is possible to imagine cases in which an offender is not present on the territory of a Member State and does not commit an offence against an information system with in a Member State, but makes use of an information system on Member State territory in order to commit an offence outside that territory.

Amendment 15
Article 11, second paragraph, point (b)

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

Justification

It is possible to imagine cases in which an offender is not present on the territory of a Member State and does not commit an offence against an information system within a Member State, but makes use of an information system on Member State territory in order to commit an offence outside that territory.

Amendment 16
Article 11, second paragraph, point (b a) (new)

	(b a) the offence has some other close connection with the territory of a Member State.

Justification

It is possible to imagine cases in which an offender is not present on the territory of a Member State and does not commit an offence against an information system within a Member State, but makes use of an information system on Member State territory in order to commit an offence outside that territory.

Amendment 17
Article 13(1)

1. Member States shall bring into force the measures necessary to ***comply with*** this Framework Decision by 31 December 2003.	1. Member States shall bring into force the measures necessary to ***implement Articles 1-11 of*** this Framework Decision by 31 December 2003 ***and Article 12 within one year of its entry into force.***

Justification

See justification for Amendment 18 on Article 14.

Amendment 18
Article 14

This Framework Decision shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Communities.	***Articles 1-11 of t***his Framework Decision shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Communities. ***Article 12 shall enter into force on that day on which a data protection instrument for the third pillar enters into force. A specific reference to this effect shall be made on publication in the relevant Official Journal.***

Justification

Parliament has repeatedly drawn attention to the need for a data protection instrument for the third pillar. Only when such a data protection instrument exists, should data exchange in

the area of the criminal law be enforced at European level. Even though Article 12 of the proposal is concerned solely with the establishment of points of contact and both their activity and the transfer and protection of data are governed by national law, its purpose is nevertheless to implement the Council recommendation on accession to the G8 network of contact points with its accompanying commitments. Uniform European data protection legislation seems unavoidable here.

EXPLANATORY STATEMENT

Introduction

Electronic communications and information networks are gaining increasing importance in everyday life. Yet the increase in use for private and professional purposes has also been accompanied by the increasing misuse of information networks and the number of attacks on them. A particular cause of concern here is the threat represented by international attacks on information systems in the form of illegal access, spread of malicious software and data theft. Those affected are not only electronic communications network operators, service providers and electronic commerce companies but also private individuals not engaged in commerce. Since use is now made of modern communications media in practically all areas, large quantities of personal data are stored in a wide variety of data banks: for example, customer profiles are drawn up on the basis of consumption patterns but also even more personal data such as illnesses, prescribed medicines and medical consultations are recorded. Hacking means therefore not only an economic risk and the risk of loss of confidence in electronic commerce but also poses a threat to individual privacy. Furthermore, proper hacking groups have already emerged by now with the result that hacking is turning into organised crime. It cannot be denied that firm action must be taken against this form of organised crime and, on account of its typical cross-border features, international solutions need to be tried.

Content of proposal

The present proposal seeks to counter the growing danger of hacking at two levels, this also being reflected in the choice of a dual legal basis (Articles 29 and 30 of the EU Treaty). On the one hand, the criminal law provisions of the Member States are to be aligned in order to guarantee the seamless criminality of attacks on information systems and to express the clear, EU-wide, uniform disapproval by society of such attacks on information systems. At the same time, police and judicial cooperation in this area is also to be promoted.

The approximation of substantive criminal law is achieved by the framing of criminal offences, the fixing of minimum/maximum penalties and aggravating circumstances and by regulating the liability of legal persons and the issue of jurisdiction.

Such approximation of criminal laws is also essential for effective police and judicial cooperation since this is the only way of ensuring that Member States can provide one another with appropriate legal assistance. In addition, cooperation in combating Internet crime is to be improved by the Member States setting up contact points that are permanently manned and available around the clock to tackle high-tech crime.

Evaluation

The present proposal takes into account the fact that all Member States, except for Luxembourg and Denmark, have signed the Council of Europe Cybercrime Convention[1] which was formally adopted in November 2001 and is also concerned among other things with the approximation of criminal offences in this field. The present proposal for a

[1] http://conventions.coe.int/treaty/EN/cadreprincipal.htm

framework decision broadly incorporates the offences formulated in Articles 2, 4 and 5 of the Convention as it relates to attacks on information systems, thus expediting its implementation. Nevertheless, the proposal creates a greater degree of approximation by treating as a criminal offence any intentional access without right to information systems either where directed against part of an information system that is subject to specific protection or where carried out with the intent to cause damage or to procure an economic benefit. The Council of Europe Convention, on the other hand, leaves Member States the choice of requiring cumulative evidence of different elements.

Article 4, which regulates illegal interference with information systems, broadly corresponds to Articles 4 and 5 of the Convention. There is no possibility, however, for countries to restrict the criminality of interference with data with the intent to cause damage solely to cases where serious harm actually results.

It can therefore be concluded that the proposal is fully in line with the Cybercrime Convention but, at the same time, creates a somewhat higher degree of approximation of criminal offences than the Cybercrime Convention; this would also extend to all Member States, which is undeniably an advantage.

The rapporteur would emphasise that, in principle, legal persons should not be held liable under criminal law. The measures proposed in this context, however, are largely of an administrative and financial nature. However, the fundamental and comprehensive threat to the entire social structure which crime in this field represents justifies the proposed sanctions, though with the improvements put forward by the rapporteur.

The rapporteur also has some misgivings about the offence referred to in Article 3(i). Here, the simple act of breaching security precautions is to be made an offence, even where there was no intent to benefit economically or cause damage and, indeed, no damage was caused. It is a fact that a large number of young computer freaks regard hacking as a kind of sport. It can be argued whether it is right that the knowledge that a young friend or family member has broken into a shop comes as a shock, while breaking into the Pentagon's and Microsoft's data banks on the contrary gives rise, in many cases, to a certain admiration. It is, however, a social reality that the same disapproval does not attach to these two kinds of breaking and entering and that young people's sense of wrong is consequently not very pronounced in the area of hacking.

The rapporteur perceives a certain danger in the proposal not taking account of this reality. At the same time, it would probably be sending out the wrong signal to exclude the breaching of security precautions altogether from the list of offences. The rapporteur accordingly takes the view that this must be accommodated at national level. A comparison may be made with other national criminal law which takes the youth of offenders into consideration. Member States are urged to allow judges the possibility in national legislation to acquit minors who, for the first time, are brought to book for unlawful access to an information system, who did not commit this misdemeanour with the intent of causing damage or procuring an economic benefit or creating prospective profits for a criminal organisation. This is one way of avoiding the criminalisation of a large number of young people, particularly as attempted acts and instigation are also punishable offences.

Since respect for human rights does not have the same democratic protection in the EU as respect for the internal market, democratic responsibility for these issues must be clarified. There should be a possibility of greater leniency in respect of minor offences as a complement to the report's proposal to take account of the youth of offenders, which also exists at national level in most Member States' criminal law.

Critical attention also needs to be paid to the planned establishment of contact points in the Member States for the purpose of exchanging information on the relevant offences.

The G8 meeting of Justice and Interior Ministers of 9-10 December 1997 in Washington DC saw the adoption of the principles of a G8 network of national contact points for combating high-tech crime accompanied by an action plan for setting up a network manned permanently around the clock seven days a week and a list of the commitments entered into by individual states when joining the network. In the action plan G8 also calls on other countries to join this network.

The EU Member States that have not joined the G8 network form part of Interpol's National Central Reference Point system (NCRP), which does not however provide 24-hour readiness. A Council recommendation[1] calls on Member States that have not already done so to join the G8 network of contact points with 24-hour service intended for the combat against high-tech crime. Article 12 of the proposal is intended to make the establishment of such contact points compulsory. The rapporteur acknowledges the advantages of such a worldwide network for efficient police and judicial cooperation but also perceives the dangers inherent in the exchange of information between countries about criminal offences and investigations into them. Particular care must be taken here since data transmission is a very sensitive area that involves risks to the protection of privacy. Precisely because there is a substantial democratic deficit in connection with the third pillar, the EU must exercise the same care in this area as has also been exercised by national parliaments. When enforcing data transfer, it must therefore always ensure that there are appropriate rules for data protection in order to counteract the associated risks.

It could of course be argued that Article 12 of the proposal is after all simply concerned with the establishment of contact points and that their activity and the transfer and protection of data are governed by national law. In fact, however, this article has a hidden agenda – that much is clear from the comments on the proposal - which is the implementation of the Council recommendation on joining the G8 network of contact points with its accompanying commitments.

If the EU champions the Europe-wide introduction of this network through legislative and, hence, compulsory measures, it will bear the responsibility towards the citizens of Europe for coping with its accompanying negative features. The somewhat glib wording in Article 12 that the exchange of information is to take place 'in accordance with data protection rules' obscures the fact that there are no data protection rules at EU level in the area of the third pillar, even though this has repeatedly been demanded by Parliament. The Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic

[1] Council recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime (OJ C 187, 3.7.2001).

processing of personal data is in any case not an adequate substitute even if it has been ratified by all Member States.

The rapporteur urges, therefore, that, in the light of the foregoing, Article 12 should enter into force only when an appropriate data protection instrument has been created for the third pillar at EU level.

On the basis of these two amendments - i.e. the possibility of greater leniency for first hacking offences by minors and if the establishment of an EU G8 network is combined with a fundamental system of data protection - the rapporteur can agree to the proposal.

Minority opinion

Marco Cappato

The rapporteur has markedly improved the text proposed by the Commission, by increasing the number of references to the protection of human rights and fundamental freedoms and to privacy. The Radical Members therefore backed most of the rapporteur's amendments, but voted against a legislative resolution which raises serious problems, in particular as regards freedom of expression and the expression of dissent via the Internet.

The Commission proposal has five main defects: an obsession with ad hoc regulation and over-regulation of the Internet; harmonisation of criminal law obtained by harmonising the number of years of imprisonment which can be imposed; a repressive approach which entails the criminalisation of all forms of behaviour considered as comparable to attacks on information systems; the illusion that the repression of criminal acts can be achieved by making penalties more severe rather than by making checks more effective; stepping up the fight against crime by restricting rights and fundamental freedoms such as freedom of expression and freedom to express dissent via the Internet.

We therefore consider that it would be preferable to tackle the issue of crimes committed on the Internet with the existing instruments of criminal law, rather than by increasing the volume of specific technology-based legislation, which moreover has all the defects referred to earlier.

Minority opinion

Ilke Schröder

I am voting against the report on a Council framework decision on attacks against information systems. The document is inspired by the Cybercrime Convention and hence advocates criminalising Internet users.

The European arrest warrant is also mentioned, which makes it substantially more difficult for defence lawyers to defend cases at European level. This can have serious consequences for fundamental rights if people are convicted under the new anti-terrorism legislation, since both urban violence and non-violent action against government buildings count as terrorism.

The Commission proposal is one in a series of current legislative measures intended to create the European Area of Freedom, Security and Justice. Here security does not mean security for society, but the creation of an authoritarian police state. Here freedom means the freedom of the government to monitor and control everything it deems dangerous. Ultimately EU law will lead to the acceptance of arbitrary police measures.

Furthermore, the proposal is a continuation of earlier initiatives on so-called computer-based crime. The opportunity to restrict fundamental rights after 11 September 2001 without much protest and facilitate the far-reaching persecution of critics and opponents of its policy by means of police action and criminal law provisions is also being exploited for this report.

The Commission itself concludes that the best protection against the attacks on computer systems dealt with in the report consists in education and prevention, which would in actual fact mean structurally disconnecting vulnerable computers from the Internet. However, no further mention of this is made in the proposed measures in the actual report.

The aim of the proposal, exactly like the anti-terrorism legislation in the EU and the Member States after 11 September 2001, is therefore not to protect against attacks on information systems, but to undermine fundamental rights and extend the powers of supervisory authorities.

11 September 2002

OPINION BY THE COMMITTEE ON INDUSTRY, EXTERNAL TRADE, RESEARCH AND ENERGY

for the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs

on the proposal for a Council Framework Decision on attacks against information systems

(COM(2002) 173 – C5-0271/1/2002 – 2002/0086(CNS))

Draftsman: Marco Cappato

PROCEDURE

The Committee on Industry, External Trade, Research and Energy appointed Marco Cappato draftsman at its meeting of 4 June 2002.

It considered the draft opinion at its meetings of 8 July, 26 August and 11 September 2002.

At the last meeting it adopted the following amendments unanimously.

The following were present for the vote: Carlos Westendorp y Cabeza (chairman), Peter Michael Mombaur (vice-chairman), Yves Piétrasanta (vice-chairman), Jaime Valdivielso de Cué (vice-chairman), Marco Cappato (draftsman), Sir Robert Atkins, Guido Bodrato, Gérard Caudron, Giles Bryan Chichester, Nicholas Clegg, Willy C.E.H. De Clercq, Harlem Désir, Concepció Ferrer, Colette Flesch, Christos Folias (for Bashir Khanbhai), Per Gahrton (for Nuala Ahern), Norbert Glante, Alfred Gomolka (for Angelika Niebler), Michel Hansenne, Roger Helmer (for Paul Rübig), Hans Karlsson, Werner Langen, Peter Liese (for Konrad K. Schwaiger), Rolf Linkohr, Caroline Lucas, Hans-Peter Martin (for Massimo Carraro), Eryl Margaret McNally, Elizabeth Montfort, Seán Ó Neachtain, Reino Paasilinna, Paolo Pastorelli, Elly Plooij-van Gorsel, John Purvis, Godelieve Quisthoudt-Rowohl, Imelda Mary Read, Mechtild Rothe, Christian Foldberg Rovsing, Jacques Santer (for Marjo Matikainen-Kallström), Umberto Scapagnini, Esko Olavi Seppänen, Claude Turmes, W.G. van Velzen, Alejo Vidal-Quadras Roca, Dominique Vlasto and Olga Zrihen Zaari.

SHORT JUSTIFICATION

The proposal for a framework decision on attacks against information systems seeks to ensure that such attacks are punishable by penalties including a custodial sentence with a maximum term of imprisonment of no less than one year, so as to bring into play the instruments of European police and judicial cooperation and various forms of extraterritorial jurisdiction.

In the case of such specific measures as these, however, it is necessary to ensure that the approximation of laws does not violate basic legal principles or criminalise individuals' conduct solely by virtue of the use of new technologies. The principle of technological neutrality, which already exists in EU law, should not be interpreted solely as requiring non-discrimination as regards the use of one type of technology as opposed to another, but also as preventing a given activity from being criminalised merely because it involves the use of technology. Care should be taken, therefore, to ensure that the legislation targets the offence (be this a terrorist attack, theft, violation of privacy, vandalism, or some other offence) rather than the means whereby it is committed.

That approach would also make it possible to establish a clear distinction between, on the one hand, forms of 'on-line' political activity, civil disobedience, demonstrations and activities of little or no consequence (some of which might be covered by the term 'hacking') and, on the other hand, 'cracking', violent action directed not only against property, but also against physical persons. To ensure that the legislation can make such distinctions without having to keep up with every technological advance, it must be confined to a few precise rules based as closely as possible on general legal principles and the rules governing 'off-line' activities.

It is not acceptable to oblige Member States to impose criminal penalties on activities which are already adequately regulated (such as violation of privacy) or which are permissible and tolerated in any democratic country, or indeed which deserved to be recognised as contributing to the public good, even if they involve actions which might be covered by the term 'attacks against information systems'. For example, action to combat censorship and disinformation which involves interference in, or sabotage of, the means used to repress individuals or whole nations.

If Member States are to be required to treat attacks against information systems as criminal offences, it is not appropriate to rely on the powers of individual judges to assess the facts, and the specific circumstances, of each case. It is essential to include in the proposed framework decision explicit references to fundamental rights and freedoms, and to reaffirm, in line with the subsidiarity principle, that Member States may include in their own legislation exemption clauses which may be applied without thereby infringing the law of the European Union.

The draftsman considers that, unless the proposed amendments – particularly those to Articles 1, 3 and 4 – are adopted, the proposed framework decision could not be regarded as a positive step in terms of extending into the realm of cyberspace the 'area of freedom, security and justice' which is the objective of the European Union's cooperation in the field of justice and home affairs.

AMENDMENTS

The Committee on Industry, External Trade, Research and Energy calls on the Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Text proposed by the Commission[1]	Amendments by Parliament
Amendment 1 Recital 5 a (new)	
	(5 a) This framework decision and the definitions it employs, set out in Article 2, must be in agreement with, and where necessary extended to include, the new OECD Guidelines for the Security of Information Systems and Networks, adopted on 25 July 2002.
Justification	
Self-explanatory.	
Amendment 2 Article 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.	***Given that the protection of information systems is a key element in the creation of an area of freedom, security and justice, the*** objective of this Framework Decision is to improve co-operation between judicial and other ***relevant*** competent authorities, including the police and other specialised law enforcement ***agencies*** of the Member States, ***by*** approximating rules on criminal law in the Member States in the area of attacks against information systems.

[1] OJ C 203 E, 27.8.2002, p. 109.

Justification

It should also be mentioned that the Framework Decision should seek to preserve the fundamental rights of citizens.

Amendment 3
Article 1 a (new)

(1 a) 1. In addition to the creation of offences covering the actions referred to in Articles 3, 4 and 5, prevention should also not be neglected, and Member States should help encourage participants in the Information Society increasingly to promote a culture of security, particularly by holding information campaigns, together with the affected employers, organisations and other actors, to raise awareness of security risks on information networks.

2. The Commission shall take the initiative with a view to raising awareness among citizens, businesses and the public sector concerning security risks on electronic communication networks, and shall play a role in coordinating and harmonising the content of information campaigns in the Member States on the security aspects and risks involved in electronic communications networks.

Justification

Prevention is the first priority in increasing the security of our information networks. It is therefore important to promote a culture of security among citizens, businesses, authorities, schools and other institutions, in short among everyone who participates or will participate in the Information Society, by means of information, risk-assessment, reminding everyone who uses an information network of their personal liability, taking precautionary measures, and reacting correctly to attacks on information systems.

Amendment 4
Article 2 (g)

(g) "Without right" means that ***conduct by authorised persons or other conduct recognised as lawful under domestic law is excluded.***	(g) ***To act*** "Without right" means ***to take action without right or justification in order to access information system or to commit acts against information systems within the meaning of this framework decision.***

Justification

The definition is not very clear. It would also be easy to evade criminal penalties by legalising a particular action. Moreover, while individual actions covered by these provisions may themselves be unlawful, the action as a whole may be justified.

Amendment 5
Article 3

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	Member States shall ensure that intentional ***illegal*** access 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 ***appropriate*** specific protection measures ***based on the protection of legitimate rights and interests***; or (ii) with the intent to cause damage to ***the legitimate rights and interests of*** a natural or legal person; or

Justification

The obligation to regard as a criminal offence access 'without right' to information systems should not be extended to activities of little or no consequence (which would not be punished if they were carried out 'off line', i.e without using new technologies) or to activities that could be regarded as a form of self-defence or civil disobedience directed against systems being used to the detriment of fundamental freedoms and rights. The subsidiarity principle demands that we avoid imposing binding, criminalising measures at European level.

Amendment 6
Article 3 (iii)

(iii) with the intent to result in an economic benefit.	***deleted***

Justification

The mere fact that the person committing the act has the intent to achieve an economic benefit is not in itself any more unlawful than the act itself and is in any case too vaguely worded: for whom or on whose behalf is an economic benefit intended to result?

Amendment 7
Article 6, paragraph 2 a (new)

	2 a. The Member States shall ensure that, in setting the level of the penalty, account is taken in an equitable manner of the level of security or precautionary measures taken by the person attacked.

Justification

The level of precautionary measures taken to secure the information system of a body (such as a firm, institution, individual citizen etc.) should be taken into account in determining the level of the penalty. The owner of an information system, for example, will take increasingly powerful precautions in line with the importance of his system, and these should of themselves send a negative signal to unauthorised persons.

Amendment 8
Article 7, paragraph 1, letters (b) and (c)

(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;	(b) the offence caused, or resulted in, 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***	***Deleted***

Justification

The principle that an offence that gives rise to substantial economic loss or substantial proceeds should be regarded as a separate offence (and attract penalties up to four times greater) would be a completely new development in criminal law. Such a novel concept would be as dangerous as it was discriminatory in terms of the economic circumstances of those committing an offence and those against whom it was committed. The question of compensation, which is obviously linked to any economic damage sustained or profit obtained, is a different matter altogether.

Amendment 9
Article 9, paragraph 2

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.	2. Apart from the cases provided for in paragraph 1, Member States shall ensure that a legal person can be held liable***, where possible,*** 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.

Justification

The legal person exercises control within the limits of the framework imposed by the legislature, including those relating to liability and respect for privacy.

Amendment 10
Article 10, paragraph 1, letter (a)

(a) exclusion from entitlement to public benefits or aid;	***Deleted***

Justification

Criminal judges cannot usually impose this kind of sanctions, which are the exclusive prerogative of the administrative courts.

Amendment 11
Article 11, first paragraph, point (c)

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

Justification

It is desirable for establishments as well as head offices to be included, in order to avoid loopholes in the criminal law.

Amendment 12
Article 11, second paragraph, point (a)

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

Justification

It is possible to imagine cases in which an offender is not present on the territory of a Member State and does not commit an offence against an information system with in a Member State, but makes use of an information system on Member State territory in order to commit an offence outside that territory.

Amendment 13
Article 11, second paragraph, point (b)

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

Justification

It is possible to imagine cases in which an offender is not present on the territory of a Member State and does not commit an offence against an information system within a Member State, but makes use of an information system on Member State territory in order to commit an offence outside that territory.

Amendment 14
Article 11, second paragraph, point (b a) (new)

(b a) the offence has some other close connection with the territory of a Member State.

Justification

It is possible to imagine cases in which an offender is not present on the territory of a Member State and does not commit an offence against an information system within a Member State, but makes use of an information system on Member State territory in order to commit an offence outside that territory.