EUROPEAN PARLIAMENT

2004 *2009*

Committee on Economic and Monetary Affairs

2006/0276(CNS)

6.6.2007

OPINION

of the Committee on Economic and Monetary Affairs

for the Committee on Civil Liberties, Justice and Home Affairs

on the proposal for a Council directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection
(COM(2006)0787 – C6-0053/2007 – 2006/0276(CNS))

Draftsman: Harald Ettl

SHORT JUSTIFICATION

The Commission submitted a proposal on measures to improve European crisis management based on the Hague Programme of 5 November 2005, which covers both the efficient management of crises affecting two or more Member States, improved civil protection in the event of disasters and critical infrastructure protection (CIP) in the fight against terrorism, and on the preparatory work of the Commission in connection with the Green Paper of 17 November 2005.

Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services.

Together with internal security, CIP in the EU constitutes a central issue for the European social system. The destruction of critical infrastructure could, from a psychological standpoint, lead to a total loss of public confidence in the EU. At the moment, the provisions made for crisis management in the individual EU Member States vary greatly. For this reason in particular, the Commission proposal provides for critical infrastructure in Europe to be identified and designated according to a common procedure.

A precondition for active crisis management is the preservation of all necessary IT and telecommunication systems. These sectors have a transversal infrastructure and at the same time constitute a critical infrastructure for other critical infrastructures such as the monetary, financial and insurance sectors. A targeted attack on the computer network of the ECB, of a major bank or of the Frankfurt stock exchange must be rapidly countered both on a technical and an institutional level.

Major corporations have no choice but to work on an international level. A European survey in the year 2000 indicated that more than half of all undertakings concerned did not carry out security audits. The potential abuse of web servers facilitates actions by radical groupings and constitutes an essential element in the use of information technology by terrorist groups.

Infrastructures of an international nature and those for which scant alternatives exist are particularly vulnerable in the event of a disaster. The power cut of 4 November 2006 affecting the European transmission grid threw this weakness into sharp relief. Despite the existence of national water supply systems, problems not confined to one country may also arise with the supply of water from aquifers, springs and rivers.

Similarly, international rail transport links and airport and air traffic control installations must be able to rely on European logistics and countermeasures in the event of a crisis.

In view of the very nature of their business, insurance and reinsurance companies have for many years had to deal with the issue of risk management. Previous directives such as that on the "Solvency I" package have already had to consider risk management issues for insurance companies, both as regards data and material cover, and these provisions will have to be

brought up to date to take account of the increased risk for the "Solvency II" package. As far as insurance is concerned, the need for proportionality notwithstanding, consideration should also be given to the possibility of an additional liability risk, possibly to be borne by the state.

The draftsman welcomes and supports the Commission's intention to coordinate CIP measures at European level. However, care must be taken to avoid double regulation of existing sectoral measures, for instance with regard to the recommendations for securities settlement systems, standards for securities clearing and settlement in the EU and standards for the use of EU securities settlement systems in ESCB credit operations.

A combination of binding and non-binding measures must result in a realistic cost-benefit ratio for European added value.

AMENDMENTS

The Committee on Economic and Monetary Affairs calls on the Committee on Civil Liberties, Justice and Home Affairs, as the committee responsible, to incorporate the following amendments in its report:

Text proposed by the Commission	Amendments by Parliament
Amendment 1 Recital 3	
(3) In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection (EPCIP) and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, manmade, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority. If the level of protection measures against a particular high level threat is found to be adequate in a critical infrastructure sector, stakeholders should concentrate on other threats to which they are still vulnerable.	(3) In December 2005 the Justice and Home Affairs Council called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection (EPCIP) and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, manmade, technological threats and natural disasters should be taken into account in the critical infrastructure protection process***.*** ***Structurally conditioned threats should also be identified***, but the threat of terrorism should be given priority. If the level of protection measures against a particular high level threat is found to be adequate in a critical infrastructure sector, stakeholders should concentrate on other threats to which they are still vulnerable.

Justification

Necessary addition.

Amendment 2
Recital 4

(4) The primary responsibility for protecting critical infrastructures ***currently*** falls on the Member States and the owners/operators of critical infrastructures. This ***should*** not change.	(4) The primary responsibility for protecting critical infrastructures falls on the Member States and the owners/operators of critical infrastructures. This ***must*** not change ***in the future***.

Justification

Clarification of national responsibility.

Amendment 3
Recital 5

(5) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would affect ***two*** or more Member States or ***a*** Member ***State*** other than that in which the critical infrastructure is located. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructure. Such European critical infrastructures should be identified and designated by means of a common procedure. The need to improve the protection of such critical infrastructures should be assessed under a common framework. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well established and efficient means of dealing with transboundary critical infrastructure. EPCIP should build on such cooperation.	(5) There are a certain number of critical infrastructures in the Community, the disruption or destruction of which would affect ***three*** or more Member States or ***two*** Member ***States*** other than that in which the critical infrastructure is located. This may include transboundary cross-sector effects resulting from interdependencies between interconnected infrastructure. Such European critical infrastructures should be identified and designated by means of a common procedure. The need to improve the protection of such critical infrastructures should be assessed under a common framework. Bilateral schemes for cooperation between Member States in the field of critical infrastructure protection constitute a well established and efficient means of dealing with transboundary critical infrastructure. EPCIP should build on such cooperation.

Justification

Subsidiarity principle.

Amendment 4
Recital 5 a (new)

(5a) A series of measures governing the identification, designation and protection of critical infrastructures already exists for some sectors. Any future Community-wide regulation should not result in duplicate regulation in these sectors in the absence of added security.

Amendment 5
Recital 6 a (new)

(6a) Critical infrastructure should be designed in such a way so as to minimise any links with and localisation in third countries. The localisation of elements of critical infrastructures outside the Europen Unon increases the risk of terrorist attacks with spill-over effects on the whole infrastructure, access by terrorists to data stored outside the European Union, as well as risks of non-compliance with Community legislation, thus rendering the entire infrastructure more vulnerable.

Justification

The recent SWIFT case showed that critical data needs to be protected against illegal use by foreign authorities or private actors.

Amendment 6
Recital 10

(10) In order to facilitate improvements in the protection of European critical infrastructures, common methodologies should be developed for the identification and classification of ***vulnerabilities,*** threats and risks to infrastructure assets.	(10) In order to facilitate improvements in the protection of European critical infrastructures, common methodologies should be developed for the identification and classification of threats and risks to***, and structural vulnerabilities of,*** infrastructure assets.

Justification

Need to be more specific.

Amendment 7
Recital 14

(14) Information sharing regarding Critical Infrastructure should take place in an	(14) Information sharing regarding Critical Infrastructure should take place in an

environment of trust and security. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive data will be sufficiently protected. ***To encourage information sharing, it should be clear for the industry that the benefits of providing Critical Infrastructure related information outweigh the costs for the industry and society in general. Critical Infrastructure Protection information exchange should therefore be encouraged.***	environment of trust and security. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive data will be sufficiently protected.

Justification

Subsidiarity principle.

Amendment 8
Recital 15

(15) This Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive.	(15) This Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive***, without additional costs arising due to the duplication of requirements that carry no added security.***

Justification

Avoiding unnecessary bureaucratic burdens without any security benefit.

Amendment 9
Recital 15 a (new)

	(15a) This Directive does not address the particular significance of the external dimension of critical infrastructure that is a feature of, for example, the financial or energy sectors.

Justification

Clarification, pointing out that critical infrastructures outside the European Union can have a massive impact, particularly in the areas of finance and energy, and that action is needed to increase security.

Amendment 10
Article 1

This directive establishes a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures.	This directive establishes a procedure for the identification and designation of European Critical Infrastructures, and a common approach to the assessment of the needs to improve the protection of such infrastructures ***against all manner of risks***.

Justification

The strategy should seek to cover all manner of risks which may result in lasting damage to the functioning and integrity of infrastructure, including those which are not the result of terrorism or natural disasters. Such risks include, inter alia, human error, inadequate training of staff, outsourcing of undertakings' essential infrastructures, epidemics, increasing dependency on IT, world-wide interconnection of IT systems, political unrest, etc..

Amendment 11
Article 2, point (b)

b) "European Critical Infrastructure" means critical infrastructures the disruption or destruction of which would significantly affect ***two*** or more Member States, or ***a single Member State*** if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure;	b) "European Critical Infrastructure" means critical infrastructures the disruption or destruction of which would significantly affect ***three*** or more Member States, or ***at least two Member States*** if the critical infrastructure is located in another Member State. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

Amendment 12
Article 2, point (c), indent 1

• ***public*** effect ***(number of*** members of the population ***affected)***;	• effect ***on*** members of the population;

Justification

Need to be more specific.

Amendment 13
Article 2, point (c), indent 2

• ***economic*** effect (significance of economic loss and/or degradation of products or services);	• effect ***on the internal market*** (significance of economic loss and/or degradation of products or services);

Justification

Need to be more specific.

Amendment 14
Article 2, point (d)

(d) "vulnerability" means a characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to disruption or destruction by a threat and includes dependencies on other types of infrastructure;	(d) "***structural*** vulnerability" means a characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to disruption or destruction by a threat and includes dependencies on other types of infrastructure;

Justification

Need to be more specific.

Amendment 15
Article 3, paragraph 1, subparagraph 1

1. The cross-cutting and sectoral criteria to be used to identify European Critical Infrastructures shall be adopted in accordance with the procedure referred to in Article 11(3). They may be amended in accordance with the procedure referred to in Article 11(3).	1. The cross-cutting and sectoral criteria to be used to identify European Critical Infrastructures shall be ***built on existing protection criteria and*** adopted in accordance with the procedure referred to in Article 11(3). They may be amended in accordance with the procedure referred to in Article 11(3).

Amendment 16
Article 3, paragraph 1, subparagraph 2

The cross-cutting criteria having a horizontal application to all critical infrastructure sectors shall be developed taking into account the severity of the effect of the disruption or destruction of a particular infrastructure. They shall be adopted by [***one year*** after the entry into force of this Directive] at the latest.	The cross-cutting criteria having a horizontal application to all ***European*** critical infrastructure sectors shall be developed taking into account the severity of the effect of the disruption or destruction of a particular infrastructure. They shall be adopted by [***six months*** after the entry into force of this Directive] at the latest.

Justification

Shorter procedure.

Amendment 17
Article 3, paragraph 1, subparagraph 3

The sectoral criteria shall be developed for priority sectors ***while*** taking into account the characteristics of individual critical infrastructure sectors and involving***, as appropriate,*** relevant stakeholders. They shall be adopted for each priority sector at the latest one year following the designation as a priority sector.	The sectoral criteria shall be developed for priority sectors ***and built on existing sector-based protection measures,*** taking into account the characteristics of individual critical infrastructure sectors, and involving relevant stakeholders ***as sectors possess particular experience, expertise and requirements concerning the protection of their critical infrastructure.*** They shall be adopted for each priority sector at the latest one year following the designation as a priority sector.

Amendment 18
Article 3, paragraph 1, subparagraph 3 a (new)

	Where Community mechanisms are already in place, they shall continue to be used. Duplication of and conflicts between different acts or provisions shall be avoided at all costs.

Amendment 19
Article 3, paragraph 3, subparagraph 1

3. Each Member State shall identify the critical infrastructures located within its territory as well as critical infrastructures outside its territory that may have an impact on ***it***, which satisfy the criteria adopted pursuant to paragraphs 1 and 2. .	3. Each Member State shall identify the critical infrastructures located within its territory as well as critical infrastructures outside its territory that may have an impact on ***its territory***, which satisfy the criteria adopted pursuant to paragraphs 1 and 2. .

Justification

Need to be more specific.

Amendment 20
Article 4, paragraph 1 a (new)

	1a. European Critical Infrastructures shall be designed so as to minimise any links with and localisation in third countries.

Justification

The recent SWIFT case showed that critical data needs to be protected against illegal use by foreign authorities or private actors

Amendment 21
Article 4, paragraph 2 a (new)

2a. The processing of personal data carried out directly or through an intermediary by, and necessary for the activities of, European Critical Infrastructures is carried out in accordance with the provisions of Directive 95/46/EC and of the applicable principles with regard to data protection. The data processing shall be carried out within the European Union and any mirroring of data is not allowed in third countries for reasons of security.

Justification

The recent SWIFT case showed that critical data needs to be protected against illegal use by foreign authorities or private actors

Amendment 22
Article 5, paragraph 2, subparagraph 1

2. The Operator Security Plan shall identify the assets of the European Critical Infrastructure and establish relevant security solutions for their protection in accordance with Annex II. Sector specific requirements concerning the Operator Security Plan taking into account existing Community measures may be ***adopted*** in accordance with the procedure referred to in Article 11(3).	2. The Operator Security Plan shall identify the assets of the European Critical Infrastructure and establish relevant security solutions for their protection in accordance with Annex II. Sector specific requirements concerning the Operator Security Plan taking into account existing Community measures may be ***fully taken into account*** in accordance with the procedure referred to in Article 11(3).

Justification

Insurance companies and banks belong to some of the sectors which continually invest large sums of money in security measures such as access control or the securing of information systems. State measures must not duplicate existing sectoral measures. For this reason, any future regulation should take full account f existing security plans.

Amendment 23
Article 7, paragraph 2, subparagraph 1

2. Each Member State shall report to the Commission on a summary basis on the types of vulnerabilities, threats and risks encountered in each sector referred to in	2. Each Member State shall report to the Commission on a summary basis on the types of vulnerabilities, threats and risks encountered in each sector referred to in

Annex I within ***18*** months following the adoption of the list provided for in Article 4(2) and thereafter on an ongoing basis every two years.	Annex I within ***12*** months following the adoption of the list provided for in Article 4(2) and thereafter on an ongoing basis every two years.

Justification

Shorter procedure.

Amendment 24
Article 7, paragraph 4

4. Common methodologies for carrying out vulnerability, threat and risk assessments in respect of European Critical Infrastructures may be developed on a sectoral basis in accordance with the procedure referred to in Article 11(3).	4. Common methodologies for carrying out vulnerability, threat and risk assessments in respect of European Critical Infrastructures may be developed on a sectoral basis in accordance with the procedure referred to in Article 11(3). ***Such common methodologies shall take into account existing methodologies.***

Amendment 25
Article 8

The Commission shall support the owners/operators of designated European Critical Infrastructures by providing access to available best practices and methodologies related to critical infrastructure protection.	***At the request of the Member States, the*** Commission shall support the owners/operators of designated European Critical Infrastructures by providing access to available best practices and methodologies related to critical infrastructure protection.

Justification

Ensuring Member States' involvement.

Amendment 26
Article 10, paragraph 2

2. Any person handling confidential information pursuant to this Directive on behalf of a Member State shall have ***an appropriate*** level of security vetting by the Member State concerned.	2. Any person handling confidential information pursuant to this Directive on behalf of a Member State shall have ***a best possible*** level of security vetting by the Member State concerned.

Amendment 27
Article 10, paragraph 3

3. Member States shall ensure that Critical Infrastructure Protection Information submitted to the Member States or to the Commission, is not used for any purpose other than the protection of critical infrastructures.	3. Member States shall ensure that Critical Infrastructure Protection Information submitted to the Member States or to the Commission, is not used for any purpose other than the protection of critical infrastructures ***and that due account is taken of the principle of proportionality from a material point of view and of fundamental rights and institutions which should be protected***.

Justification

Fundamental rights and institutions which should be protected include inter alia data protection and telecommunications secrecy.

Amendment 28
Article 11, paragraph 1

1. The Commission shall be assisted by a Committee composed of a representative of each ***CIP Contact Point***.	1. The Commission shall be assisted by a Committee composed of a ***responsible*** representative of each ***Member State***.

Justification

Subsidiarity principle.

Amendment 29
Annex I, Sector III, Sub-sector 9

Radio communication ***and*** navigation	Radio communication***,*** navigation ***and radio-frequency identification (RFID) spectres***

Amendment 30
Annex I, Sector VII, Sub-sector 19

Payment and securities clearing and settlement infrastructures and systems	Payment and securities clearing and settlement infrastructures and systems ***and their service providers***

Amendment 31
Annex I, Sector VII, Sub-sector 9 a (new)

19a Banking and insurance

PROCEDURE

Title	Identification, designation and protection of European Critical Infrastructure
References	COM(2006)0787 - C6-0053/2007 - 2006/0276(CNS)
Committee responsible	LIBE
Opinion by Date announced in plenary	ECON 1.2.2007
Drafts(wo)man Date appointed	Harald Ettl 24.1.2007
Discussed in committee	10.4.2007 8.5.2007
Date adopted	5.6.2007
Result of final vote	+: 37 –: 0 0: 3
Members present for the final vote	Gabriele Albertini, Zsolt László Becsey, Pervenche Berès, Sharon Bowles, Udo Bullmann, David Casa, Manuel António dos Santos, Christian Ehler, Jonathan Evans, José Manuel García-Margallo y Marfil, Jean-Paul Gauzès, Robert Goebbels, Donata Gottardi, Dariusz Maciej Grabowski, Karsten Friedrich Hoppenstedt, Sophia in 't Veld, Piia-Noora Kauppi, Guntars Krasts, Andrea Losco, Astrid Lulling, Cristobal Montoro Romero, Joseph Muscat, Joop Post, John Purvis, Alexander Radwan, Dariusz Rosati, Heide Rühle, Eoin Ryan, Antolín Sánchez Presedo, Cristian Stănescu, Margarita Starkevičiūtė, Ivo Strejček, Ieke van den Burg, Sahra Wagenknecht
Substitute(s) present for the final vote	Harald Ettl, Ján Hudacký, Werner Langen, Maria Petre, Andreas Schwab
Substitute(s) under Rule 178(2) present for the final vote	Anne Ferreira