# Identification and designation of European critical infrastructures and assessment of the need to improve their protection

2006/0276(CNS) - 27/06/2007

The Committee on Civil Liberties, Justice and Home Affairs adopted by a large majority the report by Jeanine **HENNIS-PLASSCHAERT** (ALDE, NL) amending, under the consultation procedure, 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.

The main amendments are as follows:

- the title of the proposal is amended to underline that it concerns “priority sectors” as opposed to “all” sectors;

- structurally conditioned threats should also be identified, but the **threat of terrorism** should be given priority;

- reinforce the principle according to which the directive strengthens **public safety** through a consistent and efficient system that is not at cross-purposes with itself;

- there are a number of critical infrastructures in the Community, the disruption of which would affect **three or more Member States or at least two other 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 infrastructure should be identified by means of a common procedure. On the basis of common criteria a **list of priority sectors with European critical infrastructure** should be drawn up. A common action framework should be laid down for the protection of such European critical infrastructures that puts Member States in a position to reduce the potential danger to critical infrastructure on their territory by taking appropriate measures. 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;

- 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;

- Critical infrastructure should be designed in a way that minimises any links with and localisation in third countries. The localisation of elements of critical infrastructures outside the European Union 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. The recent SWIFT case showed that critical data needs to be protected against illegal use by foreign authorities or private actors;

- each owner/operator of European critical infrastructure should establish an **Operator Security Plan** identifying critical assets and laying down relevant security solutions for their protection. It should take into account vulnerability, threat and risk assessments, as well as other relevant information provided by Member State authorities;

- these Operator Security Plans should be forwarded to the CIP Contact Point in the Member States. Compliance with existing sector-based protection measures could satisfy the requirement to establish and update an Operator Security Plan as well as designate a **Security Liaison Officer**;

- this Directive complements existing sectoral measures at Community level and in the Member States. Where Community mechanisms and legislation are already in place, they should be implemented and applied so as to contribute to the improvement of public safety. In so doing, overlaps and contradictions with this Directive and the imposition of additional costs without an additional gain in security are to be avoided;

- as regards proportionality, particular attention should be paid to financial acceptability for owners or operators and for the Member States;

- "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;

- the cross-cutting and sectoral criteria to be used to identify European Critical Infrastructures shall be built on existing protection criteria and be adopted and amended in accordance with Article 308 of the EC Treaty and Article 203 of the Euratom Treaty;

- where Community mechanisms are already in place, they shall continue to be used. Duplications of, or contradictions between, different acts or provisions shall be avoided at all costs;

- each Member State shall identify the priority sectors within its territory, as well as those outside its territory that may have an impact on it;

- each Member State shall notify the Commission of the priority sectors thus identified at the latest one year after the adoption of the relevant criteria and thereafter on an on-going basis;

- the list of priority sectors with critical infrastructure shall be adopted and amended by the Council;

- Data protection: the processing of personal data carried out directly or through an intermediary by, and necessary for the activities of, European Critical Infrastructures shall be carried out in accordance with the provisions of Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and of the applicable principles with regard to data protection. The data processing shall be carried out within the EU and any mirroring of data shall not be allowed in third countries for reasons of security;

- the Commission and the Council shall adopt a list of existing protection measures applicable to specific sectors listed in Annex I. Compliance with one or more of the listed protection measures satisfies the requirement to establish and update an Operator Security Plan;

- each Member State shall report to the Commission on a summary basis on the types of structural vulnerabilities, threats and risks encountered in European Critical Infrastructures within **12 months** (as opposed to 18 months) following the adoption of the list and thereafter on an ongoing basis every 2 years;

- a common template for these reports shall be developed by the Commission and approved by the Council;

- **extension of the transposition deadline is essential** since transposition by the end of 2007 is unrealistic therefore Member States shall bring into force the laws, regulations and administrative provisions

necessary to comply with this Directive by **31 December 2008** at the latest. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.

Lastly, MEPs have decided to make a **list of "possible" critical infrastructure sectors** to be taken into account when setting up the definitive list. Radio communication and navigation Radio communication, navigation and radio-frequency identification (RFID) spectres; Payment and securities clearing and settlement infrastructures and systems and their service providers and banking and insurance.