Fight against terrorism: protection of critical infrastructures

2005/2044(INI) - 01/12/2005

The Council adopted the following conclusions on the protection of critical infrastructures.

Firstly, it notes that many Member States have existing national and bilateral arrangements providing a high level of protection for their critical national infrastructure. However, the Council considers that action at EU level will add value by supporting and complementing Member States' activities, while respecting the principle of subsidiarity.

The protection afforded to critical infrastructure across Europe will be increased through EPCIP enabling Member States to improve their ability to identify and protect elements of their own infrastructures. The confidential nature of information on identified infrastructure needs to be maintained for security reasons. Access to sensitive information will be granted on a need-to-know basis. Without precluding further discussion, European critical infrastructure could be defined as infrastructure the destruction or disruption of which would have a serious impact on the critical societal functions, including the supply chain, health, safety, security, economic or social well-being or the functions of government, of a number Member States which needs to be further defined.

While recognising the threat from terrorism as a priority, the Council agrees that the protection of critical infrastructure should be based on an all-hazards approach. The form and framework of EU-level work should be based on a comprehensive risk assessment by Member States, and where competent the Commission, and build on existing EU-level work. Where appropriate, use could be made of the Joint Situation Centre's counterterrorism analysis capability. Owner/operators of the infrastructure, including the private sector, must be actively involved at both the national and EU level, and have responsibilities for implementing necessary measures.

The Council invites the Commission to build on the results of its Green Paper consultation process and to continue work to establish EPCIP. EPCIP should, while respecting existing competences, provide support to Member States through an agreed framework for action by the Member States, the Commission and, while respecting existing relationships, the private sector and other relevant actors, in order to raise security standards. This should include, where appropriate, common objectives, methodologies, best practices and the identification of interdependencies. Given the differing characteristics of each sector, a sector-by-sector approach is appropriate, taking into account existing EU-level sectoral arrangements. It equally underlines the important contribution of Community and EU-level research, which should support and complement Member States' activities and those of EPCIP.

The Commission is invited to report back following the consultation period on its Green Paper by March 2006. This would include reporting on a number of issues:

- definitions of key terms, including the definition of protection of critical infrastructure and the finalisation of the definition of EU level critical infrastructure;

- an overall assessment of the costs and benefits of regulatory and voluntary approaches;

- clarity on the respective roles of the Commission (respecting existing Community competences), Member States, and owner/operators;

- development of the concept of operator security plans.

Lastly, following the consultation process and discussion of the issues in the Council, the Commission is invited to make a proposal for an EPCIP by June 2006.