MEMO/06/477

Brussels, 12 December 2006

The European Programme for Critical Infrastructure Protection (EPCIP)

The security and economy of the European Union as well as the well-being of its citizens depends on certain infrastructure and the services they provide. The destruction or disruption of infrastructure providing key services could entail the loss of lives, the loss of property, a collapse of public confidence and moral in the EU. Any such disruptions or manipulations of critical infrastructure should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union. The recent terrorist attacks in Madrid and London have highlighted the risk of terrorist attacks against European infrastructure.

In order to counteract these potential vulnerabilities the European Council requested in 2004 the development of a European Programme for Critical Infrastructure Protection. Since then, a comprehensive preparatory work has been undertaken, which has included the organisation of relevant seminars, the publication of a Green Paper and discussions with both public and private stakeholders.

With this in mind, an EPCIP Communication has been developed establishing a horizontal framework concerning the protection of critical infrastructures in Europe.

The Communication sets out the issues which need to be addressed and how:

- Measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of Critical Infrastructure Protection (CIP) expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies
- Support for Member States concerning National Critical Infrastructures (NCI) which could optionally be used by the Member States
- Contingency planning
- An external dimension
- Accompanying financial measures and in particular the proposed EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013, which will provide funding opportunities for CIP related measures having a potential for EU transferability.

As part of the EPCIP framework dealing specifically with European Critical Infrastructures, it is necessary to include a proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. The proposed Directive establishes the necessary procedure for the identification and designation of European Critical Infrastructure (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructure.

What is the nature of the problem we are trying to address?

The issue at hand which requires action is the vulnerability of critical infrastructures in Europe and the ensuing vulnerability of the services they provide. This applies to all critical infrastructures in Europe regardless of whether they can be considered as having EU or national importance.

Taking into account the principles of subsidiarity and proportionality, EU level action should concentrate on those critical infrastructures having an EU importance. With this in mind, EPCIP will develop into a process leading over time to an assessment of vulnerabilities of particular CI sectors and the preparation of proposals on how to best address these vulnerabilities. These key activities and especially the development of specific protection measures will concentrate on European critical infrastructure, with the Member States however being encouraged to adopt similar approaches concerning their national critical infrastructure.

Why is EU level action needed?

Firstly, the Commission has been asked to develop work on protecting critical infrastructure by European Councils in March and June 2004. This has been backed by the Justice and Home Affairs Council in December 2005.

Secondly, given its role in promoting the internal market, the Commission is interested in ensuring that it is not impeded by protection measures, nor is it damaged by their absence.

A growing number of Member States are preparing their own approaches to critical infrastructure protection and are waiting for the Commission to put forward a general European CIP programme, so that they can take into account the common EU approach. Delaying the adoption of a common framework would increase the chance that various incompatible approaches to CIP would be developed by the Member States.

Weak links have to be eliminated especially where transboundary effects came into play. The risk of one Member State suffering because another has failed to adequately protect infrastructure on their territory needs to be minimised.

Additional costs for companies operating in more than one Member State resulting from differing security measures need to be minimised.

Some infrastructure are becoming increasingly European, which means that a purely national approach is insufficient e.g. the energy pipelines and transmission network.

Some of the work concerning the details of how to better protection critical infrastructure in Europe (especially on such issues as the identification of interdependencies) can reasonably be expected to take a long time. Such work should start as quickly as possible and needs to be based on a common approach.

Stakeholder consultations have been ongoing since 2004 and have included three EU CIP Seminars, the adoption of a Green Paper, the holding of two informal CIP contact points meetings and numerous bilateral meetings with government and private sector representatives.

Criminal and terrorist threats are not diminishing and that there is an interest, and potentially synergies, in Member States and the Commission cooperating to protect against them.

Does the proposal satisfy the subsidiarity principle?

Yes, the subsidiarity principle is satisfied as the measures proposed in the Directive cannot be achieved by any single Member State on its own. Although it is the responsibility of each Member State to protect the critical infrastructures present under its jurisdiction, it is crucial for the security of the European Union to make sure that the most important infrastructures having an impact on the entire Community or on two or more Member States are protected to a satisfying degree and that particular Member States are not made vulnerable because of the existence of lower security standards in other Member States. The identification and protection of infrastructures having an importance for the EU (ECI) cannot be done below EU level as an EU perspective is needed in order to assess interdependencies and develop common minimum protection measures. Such measures are needed in order to make sure that a minimum level of security exists in the EU and weak links cannot be exploited. In general:

- It is clear that the protection of critical infrastructures is first and foremost a national responsibility.
- All stakeholders acknowledge that due to interdependencies and the general nature of today's economy, there exists in the EU a certain number of critical infrastructures which if disrupted or destroyed would have a serious impact on the entire Community or on a number of Member States.
- There is therefore a need to identify and designate in a coherent fashion (using the same sector-based criteria in the entire EU) the above mentioned critical infrastructures and assess whether they require additional protection measures.

Does the proposal satisfy the proportionality principle?

Yes. The draft proposal does not go beyond what is necessary in order to achieve the underlying objectives of improving the protection of critical infrastructures in Europe. No other approach would allow the EU to achieve the required objective within a reasonable period of time. At the same time, common rules in the CIP field will be of benefit to businesses, which are currently subjected to various regimes in the MS. The proposal puts forward a minimal number of measures needed to improve the protection of critical infrastructures. The underlying objective cannot be sufficiently achieved through other measures, namely by adopting a guideline approach to EPCIP, as this would not guarantee similar levels of protection across the entire EU and weak links could be exploited.

What type of infrastructure is the Commission concentrating on?

The Commission's actions will focus on European Critical Infrastructure – that is critical infrastructure that, if disrupted or destroyed, would significantly affect two or more Member States or a single Member State if the critical infrastructure is located in another Member State. With due regard to existing Community competences, the responsibility for protecting National Critical Infrastructures falls on the NCI owners/operators and on the Member States. The Commission will support the Member States in these efforts only where requested to do so. (EPCIP) will therefore also include the possibility for Member States to take action themselves on their national critical infrastructure.

Why two or more Member States and not three or more?

Once an event involves two Member States there is a transboundary dimension. If one Member State decides to take insufficient action to protect this type of infrastructure then the other Member State can suffer.

Some stakeholders did feel that European Critical Infrastructure need only consider infrastructure where the impact will affect three or more Member States, arguing that existing bilateral arrangements were sufficient to cover infrastructure involving only two Member States. The Commission considered this carefully but concluded that, legally, three or more Member States was not in-line with the concept of transboundary that runs throughout the EU treaties. It also realised that while some bilateral agreements did exist for what might be termed European Critical Infrastructure, this was certainly not the case for all of it. Finally, the use of the three or more Member States approach to EPCIP would eliminate certain Member States from the scope of EPCIP (e.g. in several sectors Portugal could only be impacted by infrastructures located in Spain).

Won't European Critical Infrastructure just be the same as National Critical Infrastructure?

No, but they could be similar. For example, if an airport is European Critical Infrastructure, it is likely to be critical for the Member State it is situated in as well; however, the reverse does not necessarily apply; an airport critical for one Member State may not have a serious transboundary impact if disrupted or destroyed and hence will not be European Critical Infrastructure.

Why is the approach all-hazards and not just terrorism?

When considering the seriousness of the impacts of an event, it is (from the disruption point of view) largely irrelevant what caused it. When considering whether something is or is not European Critical Infrastructure, there is no need to make a distinction here as it is the impact of the disruption that is of importance. Clearly when considering protection measures the nature of the threat and the vulnerability needs to be considered in more detail. Given the greater experience of dealing with natural hazards, component failure and criminal threats, the protection measures are likely to focus on terrorism.

What approach is the Commission taking?

The Commission is in the process of proposing:

- a Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection; and
- a Communication on the European Programme for Critical Infrastructure Protection (EPCIP) which contains an action plan.

Together, these will set out the framework for infrastructure protection in the EU. Most of the implementation, however, will take place at the sector-specific level; and in the proposal for a directive, the Commission has identified eleven sectors of the economy that need to be examined.

What issues does the EPCIP Communication address?

The key elements of EPCIP as set out in the proposed Communication would be:

- A proposed Directive establishing a procedure on the identification and designation of ECI;
- Non-binding measures designed to facilitate the implementation of EPCIP including an EPCIP Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of CIP expert groups at EU level, CIP information sharing processes and the identification and analysis of interdependencies.

- Non-binding measures which may optionally be used by Member States for National Critical Infrastructures (NCI) under their responsibility.
- The identification of the need to enhance work on contingency planning.
- An external dimension
- Accompanying financial measures set out in the EU programme on "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" (financial perspectives for 2007-2013). This programme will provide funding opportunities for CIP related measures having a potential for EU transferability.

How will ECI be identified and designated?

The ECI Directive lays down the procedure on how to identify and designate ECI:

- First, the Commission together with the Member States and relevant stakeholders develop cross-cutting and sectoral criteria for the identification of ECI, which are then adopted through the comitology procedure.
- The cross-cutting criteria are developed on the basis of the severity of the disruption or destruction of the CI. The severity of the consequences of the disruption or destruction of a particular infrastructure should be assessed on the basis, where possible, of:
    a. Public effect (number of population affected);
    b. Economic effect (significance of economic loss and/or degradation of products or services);
    c. Environmental effect;
    d. Political effects;
    e. Psychological effects
- Each Member State then identifies those infrastructures which satisfy the criteria.
- Each Member State then notifies the Commission of the critical infrastructures which satisfy the established criteria.
- Following the identification procedure the Commission prepares a draft list of ECI. The draft list is based on the notifications received from the Member States and other relevant information from the Commission. The list is then adopted through comitology.

How will priority sectors be identified?

Relevant work is undertaken under priority CIP sectors selected by the Commission on an annual basis from among those listed in Annex 1 of the proposed Directive. The list of CIP sectors contained in Annex 1 is composed of 11 critical infrastructure sectors.

What are the critical infrastructure sectors?

The EPCIP Communication underlines that "since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis and implemented following an agreed list of CIP sectors". The ECI Directive puts forward in Annex 1 a list of 11 critical infrastructure sectors. The list of CIP sectors contained in Annex 1 may be amended through the comitology procedure in so far as this does not broaden the scope of the Directive.

Annex 1 identifies the following CI sectors:

1. Energy
2. Nuclear industry
3. Information, Communication Technologies, ICT
4. Water
5. Food
6. Health
7. Financial
8. Transport
9. Chemical industry
10. Space
11. Research facilities

What obligations does the ECI Directive impose on owners/operators?

The ECI Directive only imposes two obligations on the owners/operators of those critical infrastructures, which are designated as European Critical Infrastructures. These include:

1. The establishment of an Operator Security Plan which would identify the ECI owners' and operators' assets and establish relevant security solutions for their protection. Annex 2 of the ECI Directive provides the minimum contents of such OSPs including:

- identification of important assets;
- a risk analysis based on major threat scenarios, vulnerability of each asset, and potential impact shall be conducted.
- identification, selection and prioritisation of counter-measures and procedures with a distinction between:
    - **Permanent security measures**, which identify indispensable security investments and means which cannot be installed by the owner/operator at short notice. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.
    - **Graduated security measures**, which are activated according to varying risk and threat levels.

Once an OSP has been created, each ECI owner/operator should submit it to the relevant Member State authority. Each Member State will setup a supervisory system concerning OSPs which will ensure that sufficient feedback is given to the ECI owner/operator concerning the quality of the OSP and in particular the adequacy of the risk and threat assessment.

2. The designation of a Security Liaison Officer (SLO). Article 6 of the ECI Directive requires all CI owners/operators designated as ECI to appoint an SLO. The SLO would function as the point of contact for security issues between the ECI and the relevant CIP authorities in the Member States. The SLO would therefore receive all relevant CIP related information from the Member State authorities and would be responsible for providing relevant information from the ECI to the Member State.

What would be the costs for ECI owners/operators of implementing the ECI Directive obligations?

The costs would vary among the Member States. Although exact quantification is not possible, the following assumptions can be made concerning the two obligations introduced by the proposed ECI Directive:

3. The owners/operators of European critical infrastructure would incur costs associated with the preparation of Operator Security Plans. The exact costs will vary considerably depending on the sector concerned, the type of activities being undertaken but most notably concerning the level of preparedness already achieved (existing business continuity plans etc). Costs can be expected to be low or non-existent for those owners/operators who:

- Have already prepared business continuity plans.
- Are located in a Member State with an already advanced CIP programme (e.g. in certain Member States an obligation for national critical infrastructure to prepare Operator Security Plans already exists).
- Belong to a sector already possessing certain security/safety obligations (e.g. the Port Security Directive[1] obliges port authorities to develop port security assessments and plans which would most likely already satisfy the obligations imposed through a sector specific Operator Security Plan).

Costs can reasonably be expected to be higher for owners/operators who have not addressed security or business continuity issues at all. It could however be expected, that even without the adoption of EPCIP, certain costs concerning business continuity plans would be incurred at a certain point in the future. The problem would remain however that this would be done in an uncoordinated and incomparable fashion.

[1] DIRECTIVE 2005/65/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on enhancing port security

- The owners/operators of European critical infrastructure would incur costs associated with the designation of Security Liaison Officers. As with the Operator Security Plans however, these costs will vary depending on a number of factors. Costs can be expected to be low or not to exist at all for those owners/operators who:
    - Already possess a security officer. For most owners/operators likely to be designated as ECI, this is most likely the case. In this situation, the designation of an SLO will simply amount to giving particular security officials additional competences.
    - Are located in a Member State with an already advanced CIP programme (e.g. in certain Member States an obligation for national critical infrastructure to designate SLO already exists).
    - Belong to a sector already possessing certain security/safety obligations (e.g. the Port Security Directive[2] already obliges the Member States to appoint port security officers for each port. Although this is not identical to the designation of a SLO, which has to be done by the owners/operator, it can serve as a basis for such a designation).

Costs will of course be higher for those owners/operators which do not possess any security officers. Such a situation would however be relatively unlikely for owners/operators designated as European critical infrastructure.

How will duplication of efforts be avoided in areas where certain security measures already exist?

Each CIP sector may develop sector-specific OSPs based on the minimum requirements of Annex 2 of the ECI Directive. Such sector specific OSPs may be adopted through comitology. For those sectors in which similar obligations already exist, article 5(2) foresees the possibility of being exempted from the OSP obligations based on a decision taken through comitology.

Why has only the port sector been included in the Directive as a sector specifically exempted from the OSP obligation?

DG TREN has requested such an exemption during the Interservice Consultation. Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security already obliges port operators to create Port Security Plans.

When would obligations like the creation of an Operator Security Plan have to be implemented?

The owner/operator obligations contained in the draft Directive would only have to be implemented by those owners/operators who would be designated as European Critical Infrastructures. The process of designation can reasonably be expected to take some time as common ECI identification criteria first need to be developed in the particular sectors and only then would the obligation to adopt an operator security plan enter into force minimum one year from having the aforementioned criteria adopted.

[2] DIRECTIVE 2005/65/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 26 October 2005 on enhancing port security

How does the ECI Directive improve protection?

The ECI Directive establishes a process leading to the identification of security gaps. The Member States should report to the Commission on a generic basis on types of security gaps identified in particular sectors. Based on this information, concrete proposals concerning additional protection measures can be put forward. The underlying idea behind this approach is nevertheless the fact that dialogue between particular owners/operators and the Member States should lead to the implementation of improved security measures.

What protection measures does EPCIP put forward?

EPCIP does not put forward any concrete protection measures. The ECI Directive establishes a procedure leading to the identification of protection gaps. If such gaps are identified the relevant Commission service may put forward binding or non-binding measures to address them. This however is not part of the current initiative.