

Comments to European Green Paper "European Programme for Critical Infrastructure Protection"

1. *Re. item 3.2. What should EPCIP protect against: the EPCIP should only address the threat of terrorism (option c). Existing legislation and operators' contingency plans already cover other types of hazard.*
2. *Item 4. Subsidiarity: While we fully agree that "The responsibility and accountability of owners and operators to make their own decisions and plans for protecting their own assets should not change" it is also imperative that the protection of installations from external threats remains a police or military function, ref. Comment 9. below.*
3. *Item 4. Confidentiality: Confidentiality of information must be guaranteed by all parties. Lists of Critical Infrastructure (CI) in the public domain could in themselves be a security liability, through the attracting of undesirable attention.*
4. *Re items 6.3 and 7.4: Protection of CI requires a cooperative partnership between owners/operators and the appropriate authorities with clearly defined responsibilities. Owners/operators must be involved from the start; in identifying CI, in determining the criteria to be used and in drafting protection measures.*
5. *Item 8.1. A general comment: It is part of upcoming Danish legislation (Offshore Sikkerhedsloven) that owners/operators are required to prepare necessary security measures, thereby being expected to incur "limited cost increases". This has been accepted by operators as a general principle. However, it would in contrast be unacceptable if the costs of any extended measures - including those involving police or military - ref. Comment 9. below - should be borne by owners/operators, since such measures would primarily aim at protecting energy supplies for society in general.*
6. *Item 8.1. Responsibilities of CI owners/operators:*
 - *the Operator Security Plan (OSP) has merit, but the issues of approval authority and disclosure need to be addressed.*
7. *Item 8.1. Questions:*
 - *it is not possible to provide a quantified response to questions one and three, re. also Comment 5. above.*
 - *re. question two: notification of whether or not infrastructure is critical should not be an obligation on the operator but a dialogue between operator and MS.*
 - *re. question four: operators must be able to determine and implement their own internal security measures.*
8. *Item 9.1. CI warning information network (CIWIN): CIWIN should also alert operators in real time of threats and alerts.*
9. *As a general comment, member states would be expected to analyse regularly external threats and take steps to lower the threat level that an installation may be exposed to. The protection of installations from external threats remains a police or military function.*