COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 17.11.2005
COM(2005) 576 final

LIVRE VERT

SUR UN PROGRAMME EUROPEEN DE PROTECTION DES INFRASTRUCTURES CRITIQUES

(présenté par la Commission)

LIVRE VERT

SUR UN PROGRAMME EUROPEEN DE PROTECTION DES INFRASTRUCTURES CRITIQUES

1. CONSIDÉRATIONS GÉNÉRALES

Les infrastructures critiques (IC) peuvent subir des dommages ou des interruptions ou encore être détruites par des actes terroristes délibérés ou par des catastrophes naturelles, par négligence, accident ou piratage informatique, du fait d'activités criminelles ou d'actes de malveillance. Pour préserver la vie et les biens des personnes exposées, dans l'UE, aux risques d'actes terroristes, de catastrophes naturelles et d'accidents, toute interruption ou manipulation des IC devrait, dans toute la mesure du possible, être courte, exceptionnelle, relativement facile à gérer, géographiquement isolée et ne porter atteinte que dans une mesure très limitée au bien-être des États membres, de leurs citoyens et de l'Union européenne. Les récents attentats terroristes de Madrid et de Londres ont mis en évidence les risques que font peser les attaques terroristes sur les infrastructures européennes. La réaction de l'UE se doit d'être rapide, coordonnée et efficace.

Le Conseil européen de juin 2004 a invité la Commission à préparer une stratégie globale visant à renforcer la protection des infrastructures critiques (PIC). En réponse, la Commission a adopté, le 20 octobre 2004, une communication intitulée «Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme», dans laquelle elle propose des mesures précises en vue de renforcer la prévention, la préparation et la réponse de l'UE face aux attaques terroristes contre des infrastructures critiques.

Dans ses conclusions relatives à la prévention, la préparation et la réaction en cas d'attentats terroristes et dans son «Programme de solidarité de l'UE face aux conséquences des menaces et des attentats terroristes», qu'il a adopté en décembre 2004, le Conseil s'est félicité de l'intention de la Commission de proposer un programme européen de protection des infrastructures critiques (EPCIP) et a approuvé la création par celle-ci d'un réseau d'alerte concernant les infrastructures critiques (CIWIN).

La Commission a organisé deux séminaires et a invité les États membres à proposer des idées et présenter leurs observations. Le premier séminaire sur la protection des infrastructures critiques de l'UE, auquel participaient les États membres, s'est tenu les 6 et 7 juin 2005. À la suite de ce séminaire, les États membres ont communiqué à la Commission des documents d'information exposant leur approche de la PIC et lui ont transmis leurs observations sur les questions abordées lors du séminaire. La Commission a reçu, en juin et juillet de cette année, des contributions qui ont permis de faire avancer les travaux sur la PIC. Le second séminaire sur la protection des infrastructures critiques de l'UE, qui s'est tenu les 12 et 13 septembre, visait à faire avancer la discussion. Tant les États membres que les associations représentatives du secteur ont participé à ce séminaire. À l'issue de ce séminaire, la Commission a décidé de publier le présent livre vert, dans lequel elle décrit les différents scénarios envisageables pour l'EPCIP.

2. OBJECTIF DU LIVRE VERT

L'objectif premier du livre vert est d'obtenir des réactions aux différents scénarios envisageables pour l'EPCIP en associant à la discussion un grand nombre d'acteurs concernés. La protection efficace des infrastructures critiques passe par la communication, la coordination et la coopération, tant au niveau national qu'au niveau de l'UE, entre toutes les parties intéressées, qu'il s'agisse des propriétaires et des exploitants d'infrastructures, des organes de réglementation, des organisations professionnelles et associations sectorielles, de tous les niveaux de l'administration ou du public en général.

Le livre vert présente différents scénarios en réponse à la demande du Conseil visant à mettre en place l'EPCIP et le CIWIN et marque la deuxième phase d'un processus de consultation sur l'établissement d'un programme européen de protection des infrastructures critiques. La Commission espère, en publiant ce livre vert, obtenir en réponse des contributions concrètes sur les options qu'il décrit. En fonction des résultats de ce processus de consultation, la Commission pourrait présenter en 2006 un train de mesures sur l'EPCIP.

3. OBJET ET CHAMP D'APPLICATION DE L'EPCIP

3.1. L'objectif général de l'EPCIP

L'objectif de l'EPCIP serait de garantir des niveaux de sûreté suffisants et uniformes des infrastructures critiques, de réduire au minimum les défaillances et de fournir, pour l'ensemble de l'Union européenne, des moyens de réaction rapide ayant fait leurs preuves. Le niveau de protection pourrait ne pas être identique pour toutes les IC et dépendre des effets que pourrait causer la défaillance d'une IC. Le programme sera évolutif et sera réexaminé régulièrement de manière à s'adapter aux nouveaux problèmes qui pourraient surgir et aux nouvelles préoccupations.

L'EPCIP devrait réduire au minimum les effets négatifs que les investissements accrus au service de la sûreté pourraient avoir sur la compétitivité d'un secteur d'activité donné. Dans le calcul de la proportionnalité des coûts, il ne faut pas perdre de vue la nécessité de préserver la stabilité des marchés, essentielle pour les investissements à long terme, ni l'influence qu'exerce la sûreté sur l'évolution des marchés boursiers et sur la dimension macroéconomique.

Question

Cet objectif de l'EPCIP vous paraît-il approprié? Dans la négative, quel devrait être cet objectif?

3.2. Contre quoi l'EPCIP devrait-il nous protéger?

Alors que les mesures de gestion des conséquences sont identiques ou similaires pour résoudre la plupart des perturbations, les mesures de protection peuvent différer en fonction de la nature de la menace. Les attaques intentionnelles ou les catastrophes naturelles figurent parmi les menaces capables de diminuer sensiblement notre capacité d'assurer les besoins essentiels et la sécurité de la population, de maintenir l'ordre et de fournir les services publics essentiels minimums, ou encore susceptibles de porter atteinte au bon fonctionnement de l'économie. Les scénarios envisageables sont les suivants:

a) **l'approche tous risques** – cette approche globale tiendrait compte de la menace provenant à la fois des attaques intentionnelles et des catastrophes naturelles. Elle permettrait d'exploiter au maximum les synergies entre les mesures de protection, mais le terrorisme ne serait pas sa priorité;

b) **l'approche tous risques conjuguée avec la priorité donnée au risque terroriste** – cette approche souple tiendrait compte d'autres types de risques, tels que la menace que représentent les attaques intentionnelles et les catastrophes naturelles, mais donne la priorité au risque terroriste. Si le niveau des mesures de protection dans un secteur d'activité donné s'avérait suffisant, les acteurs concernés se concentreraient sur les menaces face auxquelles ils sont encore vulnérables;

c) **l'approche axée sur le risque terroriste** – cette approche serait focalisée sur le terrorisme, mais ne se préoccuperait pas des menaces plus courantes.

Question

Quelle approche devrait être adoptée pour l'EPCIP? Pour quelle(s) raison(s)?

4. PRINCIPES CLÉS PROPOSÉS

L'EPCIP pourrait reposer sur les principes clés suivants:

- **Subsidiarité** - La subsidiarité serait au cœur de l'EPCIP, la PIC étant avant tout une responsabilité nationale. La responsabilité première en matière de PIC incomberait aux États membres et aux propriétaires/exploitants, leur action étant guidée par un cadre commun. La Commission se concentrerait, quant à elle, sur les aspects relatifs à la protection des infrastructures critiques de l'UE ayant une dimension transfrontalière. La responsabilité des propriétaires et des exploitants, qui doivent prendre leurs propres décisions et adopter leurs propres plans de protection de leurs infrastructures, resterait inchangée.

- **Complémentarité** - Le cadre commun de l'EPCIP serait un complément des mesures existantes. Dans les cas où des mécanismes communautaires sont déjà en place, ces derniers devraient continuer à être utilisés et contribueraient à la mise en œuvre globale de l'EPCIP.

- **Confidentialité** – Le partage des informations concernant la PIC s'effectuerait dans un climat de confiance et dans le respect de la confidentialité, d'autant plus nécessaire qu'il existe un risque que des informations factuelles sur une infrastructure critique donnée puissent être utilisées de manière à provoquer une défaillance des installations concernées ou à commettre des actes aux conséquences inacceptables pour celles-ci. Tant au niveau de l'UE qu'à celui des États membres, les informations sur la PIC seraient classifiées et leur accès serait fondé sur le principe du «besoin d'en connaître».

- **Coopération des acteurs concernés** – Tous les acteurs concernés, à savoir les États membres, la Commission, les associations professionnelles et sectorielles, les organismes de normalisation, ainsi que les propriétaires, les exploitants et les utilisateurs (par «utilisateurs», il faut entendre les organisations qui exploitent et utilisent les infrastructures à des fins professionnelles et pour des prestations de services) ont un rôle à jouer dans la

PIC. Ils devraient tous coopérer et contribuer à la conception et à la mise en œuvre de l'EPCIP en fonction de leurs rôles respectifs et des responsabilités qui leur incombent. Les autorités des États membres seraient chargées de diriger et de coordonner les travaux de définition et de mise en œuvre d'une approche nationale cohérente de la protection des infrastructures critiques se trouvant sur leur territoire. Les propriétaires, les exploitants et les utilisateurs seraient activement associés tant au niveau national qu'à celui de l'UE. Dans les cas où il n'existe pas de normes sectorielles ou de normes internationales, les organismes de normalisation pourraient adopter, le cas échéant, des normes communes.

- **Proportionnalité** - Les stratégies et les mesures de protection seraient proportionnées au niveau de risque, étant donné que les infrastructures ne peuvent pas toutes être protégées contre toutes les menaces (par exemple, les réseaux de transport de l'électricité sont trop étendus pour être clôturés ou surveillés). En appliquant des techniques appropriées de gestion des risques, on se concentrerait sur les points qui sont les plus exposés, compte tenu de la menace, de la criticité relative des infrastructures, du rapport coûts-avantages, du niveau actuel de sûreté et de l'efficacité des stratégies d'atténuation existantes.

Question

Ces principes clés vous paraissent-ils acceptables? Certains de ces principes sont-ils superflus? D'autres principes devraient-ils être ajoutés?

Estimez-vous, vous aussi, que les mesures de protection devraient être proportionnées au niveau de risque en cause, étant donné que les infrastructures ne peuvent pas toutes être protégées contre toutes les menaces?

5. UN CADRE COMMUN POUR L'EPCIP

Tout dommage que pourrait subir une infrastructure dans un État membre ou toute perte d'une telle infrastructure pourrait entraîner un préjudice pour plusieurs autres États membres et pour l'économie européenne dans son ensemble. La probabilité d'un tel préjudice s'accroît parce que, avec les nouvelles technologies (par exemple, l'internet) et la libéralisation des marchés (par exemple, ceux du gaz et de l'électricité), un grand nombre d'infrastructures font partie d'un réseau plus large. Dans ces conditions, les mesures de protection ne peuvent être supérieures à celles du maillon le plus faible. Un niveau de protection commun pourrait donc s'avérer nécessaire.

La protection efficace passe par la communication, la coordination et la coopération, tant au niveau national et international qu'au niveau de l'UE (selon le cas), entre toutes les parties intéressées. Un cadre commun, au niveau de l'UE, pour la protection des infrastructures critiques en Europe pourrait être mis en place afin de s'assurer que tous les États membres offrent des niveaux de protection suffisants et uniformes de leurs infrastructures critiques et que la concurrence dans le marché intérieur n'est pas faussée. En vue de soutenir l'action des États membres, la Commission faciliterait le recensement, l'échange et la diffusion des meilleures pratiques en matière de PIC en définissant un cadre commun pour la protection de ces infrastructures. Il reste encore à déterminer l'étendue de ce cadre général.

Le cadre commun de l'EPCIP comprendrait des mesures horizontales qui préciseraient les compétences et les responsabilités de tous les acteurs concernés par la PIC et jetteraient les bases d'approches sectorielles. Le cadre commun serait censé compléter les mesures

sectorielles déjà adoptées au niveau communautaire et dans les États membres afin d'assurer un niveau de sûreté maximal aux IC installées dans l'Union européenne. La priorité devrait être donnée à la recherche d'un accord sur une liste commune de définitions et de secteurs d'infrastructures critiques.

Étant donné que les différents secteurs d'infrastructures critiques sont très divers, il serait difficile de définir exactement les critères à appliquer pour recenser et protéger tous ces secteurs dans un cadre horizontal. Il faudrait procéder secteur par secteur. Il conviendrait néanmoins de s'entendre sur une conception commune de certains aspects intersectoriels.

C'est la raison pour laquelle il est suggéré de renforcer les infrastructures critiques de l'UE en instaurant un cadre commun de l'EPCIP (avec des objectifs communs, des méthodologies communes, par exemple pour les comparaisons ou les interdépendances) pour l'échange d'informations sur les meilleures pratiques et sur les mécanismes de contrôle du respect de ces pratiques. Parmi les composantes de ce cadre commun, on peut citer:

- des principes communs en matière de PIC;
- des codes/normes arrêtés en commun;
- des définitions communes sur la base desquelles des définitions sectorielles pourraient être arrêtées (une liste indicative de définitions est reproduite à l'annexe 1);
- une liste commune des secteurs d'infrastructures critiques (une liste indicative est reproduite à l'annexe 2);
- des domaines d'action prioritaires en matière de PIC;
- une description des responsabilités des acteurs concernés.
- des points de référence convenus;
- des méthodes pour comparer les différents secteurs d'infrastructures et pour établir entre eux un ordre de priorité.

Un cadre commun ainsi défini permettrait aussi de réduire au minimum les distorsions potentielles dans le marché intérieur.

Le cadre commun de l'EPCIP pourrait être facultatif ou obligatoire, ou avoir un caractère hybride en fonction des aspects considérés. Ces deux types de cadre pourraient compléter des mesures sectorielles et horizontales déjà prises au niveau communautaire et au niveau des États membres. Cependant, seul un cadre juridique fournirait une base juridique suffisamment solide et contraignante pour permettre une mise en œuvre cohérente et uniforme des mesures de protection des infrastructures critiques de l'Union européenne et pour délimiter clairement les responsabilités respectives des États membres et de la Commission. Avec des mesures facultatives à caractère non contraignant, offrant certes plus de souplesse, ce partage des responsabilités ne serait pas clair.

Suivant les résultats d'une analyse approfondie et en tenant dûment compte de la proportionnalité des mesures proposées, la Commission pourrait utiliser un certain nombre d'instruments, notamment législatifs, dans sa proposition d'EPCIP. Une analyse d'impact devra être jointe à toute proposition de mesures sectorielles, le cas échéant.

Questions

Un cadre commun serait-il un moyen efficace de renforcer la PIC?

Si un cadre législatif s'avérait nécessaire, quels éléments devrait-il comporter?

Êtes-vous d'accord avec l'idée selon laquelle les critères de recensement des différents types d'infrastructures critiques de l'Union européenne et les mesures de protection considérées comme nécessaires devraient être définis secteur par secteur?

Un cadre commun aiderait-il à clarifier les responsabilités des acteurs concernés? Quels volets de ce cadre commun devraient être obligatoires et quels volets devraient être facultatifs?

Quelle devrait être l'étendue de ce cadre commun? Êtes-vous d'accord avec la liste indicative de termes et de définitions reproduite à l'annexe I, qui pourrait servir de base (le cas échéant) à des définitions sectorielles? Êtes-vous d'accord avec la liste indicative des secteurs d'infrastructures critiques reproduite à l'annexe II?

6. INFRASTRUCTURES CRITIQUES DE L'UE (ICE)

6.1. Définition des infrastructures critiques de l'UE

L'élément déterminant de la définition comme infrastructure critique de l'UE serait l'existence ou non d'un effet transfrontalier, selon qu'un incident pourrait avoir ou non un impact grave par-delà les frontières de l'État membre où l'installation est située. L'autre élément à prendre en considération tient au fait que les systèmes bilatéraux de coopération entre États membres en matière de PIC constituent un instrument éprouvé et efficace de gestion des IC lorsque celles-ci sont situées dans une zone frontalière entre deux États membres. Cette coopération compléterait l'EPCIP.

Les ICE pourraient comprendre les ressources physiques, les services, les technologies de l'information, les réseaux et les actifs dont l'arrêt ou la destruction aurait de graves incidences sur la santé, la sécurité, la sûreté ou le bien-être économique ou social des citoyens:

a) soit de deux États membres ou plus – **de sorte qu'elles incluraient certaines IC bilatérales (selon le cas)**;

b) soit de trois États membres ou plus – **de sorte qu'en seraient excluent toutes les IC bilatérales**.

Pour mesurer les avantages respectifs de ces deux options, il importe de garder présent à l'esprit le fait que:

– le classement d'une infrastructure comme ICE ne signifie pas que des mesures de protection supplémentaires soient automatiquement nécessaires. Les mesures de protection existantes, qui peuvent être prévues dans le cadre d'accords bilatéraux entre les États membres, peuvent très bien suffire pour protéger cette infrastructure et, partant, ne pas exiger de changement du fait du classement comme ICE;

– l'option a) peut avoir pour effet qu'un plus grand nombre d'infrastructures seraient classées comme ICE;

– l'option b) peut impliquer que, dans le cas où une infrastructure n'intéresse que deux États membres, la Communauté européenne ne jouerait aucun rôle, même si le niveau de protection était jugé insuffisant par l'un de ces deux États membres et si les autres États membres refusaient de prendre des mesures. L'option b) pourrait aussi déboucher sur une multitude d'accords, ou de désaccords, bilatéraux entre les États membres. Les entreprises, qui doivent souvent exercer leurs activités à un niveau paneuropéen, risqueraient d'être soumises à une mosaïque d'accords différents, ce qui pourrait se traduire pour elles par des surcoûts.

En outre, il ne faudrait pas oublier de prendre en considération les IC qui ont leur point de départ ou qui se trouvent dans un pays tiers mais qui sont interconnectées ou ont un effet direct potentiel sur les États membres de l'UE.

Question

Les ICE devraient-elles être des infrastructures pouvant avoir un impact transfrontalier potentiellement grave pour au moins deux États membres ou pour au moins trois États membres? Pour quelle(s) raison(s)?

6.2. Interdépendances

Il est proposé que le recensement progressif de toutes les ICE tienne notamment compte des interdépendances. Les études sur les interdépendances contribueraient à l'analyse de l'impact potentiel des menaces contre certaines IC et permettraient notamment de savoir quels États membres seraient touchés en cas d'incident majeur affectant les IC.

Les interdépendances entre les entreprises, les secteurs industriels, les compétences territoriales et les autorités des États membres, ainsi que les interdépendances au sein même de ces secteurs ou entités, en particulier lorsqu'elles sont créées par les technologies de l'information et des communications, devraient être dûment prises en considération. La Commission, les États membres et les propriétaires/exploitants d'infrastructures critiques collaboreraient afin de recenser ces interdépendances et d'appliquer, si possible, des stratégies appropriées de limitation des risques.

Question

Comment les interdépendances peuvent-elles être prises en compte?

Connaissez-vous de bonnes méthodes d'analyse des interdépendances?

À quel niveau les interdépendances doivent-elles être recensées – au niveau de l'UE et/ou des États membres?

6.3. ICE: Étapes de mise en œuvre

La Commission proposerait, pour les ICE, les étapes de mise en œuvre suivantes:

(1) La Commission et les États membres définissent ensemble les critères spécifiques à appliquer pour recenser les ICE par secteur.

(2) Les États membres et la Commission recensent et vérifient progressivement les différents secteurs des ICE. La décision de classer une infrastructure critique particulière comme ICE est prise au niveau européen1 en raison de la nature transfrontalière de l'infrastructure concernée.

(3) Les États membres et la Commission analysent les failles existantes en matière de sûreté des ICE par secteur.

(4) Les États membres et la Commission se mettent d'accord sur les secteurs/infrastructures prioritaires pour lesquels une action s'impose, en tenant compte des interdépendances.

(5) Le cas échéant, pour chaque secteur, la Commission et les acteurs clés des États membres s'entendent sur des propositions de mesures de protection minimums, par exemple des normes.

(6) Après adoption des propositions par le Conseil, ces mesures sont mises en œuvre.

(7) Une surveillance régulière est assurée par les États membres et par la Commission. Il est procédé, pour autant que de besoin, à des révisions (mesures et recensement d'infrastructures critiques).

Questions

En ce qui concerne les ICE, la liste des étapes de mise en œuvre vous paraît-elle acceptable?

Comment, d'après vous, la Commission et les États membres devraient-ils procéder pour le classement en commun des infrastructures critiques en tant qu'ICE – les États membres ayant le savoir-faire et la Commission ayant une vue d'ensemble de l'intérêt européen? La décision de classement devrait-elle être contraignante?

Est-il nécessaire de prévoir un mécanisme d'arbitrage pour le cas où un État membre ne serait pas d'accord avec le classement en tant qu'ICE d'une infrastructure relevant de sa compétence?

Faut-il prévoir un mécanisme de vérification des classements comme ICE? Qui devrait être chargé de ces vérifications?

Les États membres devraient-ils avoir la possibilité de classer comme infrastructures critiques pour eux-mêmes des infrastructures d'autres États membres ou de pays tiers? Que faudrait-il faire si un État membre, un pays tiers ou un secteur d'activité considérait une infrastructure d'un État membre comme une infrastructure critique en ce qui le concerne?

[1] À l'exception des infrastructures liées à la défense.

Que faudrait-il faire alors si cet État membre ne recensait pas cette infrastructure comme critique? Est-il nécessaire de prévoir un mécanisme de recours? Dans l'affirmative, lequel?

Un exploitant devrait-il avoir la possibilité d'exercer un recours s'il n'est pas d'accord avec le classement ou l'absence de classement comme ICE? Dans l'affirmative, qui devrait être saisi d'un tel recours?

Quelles méthodes devraient être définies afin de déterminer les secteurs/infrastructures prioritaires pour lesquels une action s'impose? Existe-t-il des méthodes satisfaisantes qui pourraient être adaptées de manière à être applicables au niveau européen?

Comment la Commission peut-elle être associée à l'analyse des failles en matière de sûreté des ICE?

7. INFRASTRUCTURES CRITIQUES NATIONALES (ICN)

7.1. Le rôle des ICN dans l'EPCIP

Un grand nombre d'entreprises européennes exercent leurs activités par-delà les frontières et, dès lors, sont soumises à des obligations différentes en ce qui concerne les ICN. Dans l'intérêt des États membres et de l'UE dans son ensemble, il est donc suggéré que chaque État membre protège ses ICN en respectant un cadre commun de manière à éviter que les propriétaires et les exploitants de toute l'Europe soient soumis à une mosaïque de cadres différents et, partant, à une multitude de méthodologies et de surcoûts. À cet effet, la Commission propose que l'EPCIP – tout en étant surtout axé sur les infrastructures critiques de l'UE – ne perde absolument pas de vue les infrastructures critiques nationales. Trois possibilités pourraient néanmoins être envisagées:

a) Intégration totale des ICN dans l'EPCIP

b) Exclusion des ICN du champ d'application de l'EPCIP

c) Utilisation facultative de certains volets de l'EPCIP par les États membres pour leurs propres ICN

Question

Il semblerait que la protection efficace des infrastructures critiques de l'Union européenne passe par le recensement tant des ICE que des ICN. Êtes-vous d'accord avec l'idée que, même si l'EPCIP devait se concentrer sur les ICE, il ne devrait pas perdre de vue les ICN?

Laquelle de ces options vous paraît le mieux convenir pour l'EPCIP?

7.2. Programmes de PIC nationaux

Sur la base du cadre commun de l'EPCIP, les États membres pourraient concevoir des programmes nationaux de PIC pour leurs ICN. Ils pourraient appliquer des mesures plus strictes que celles prévues dans le cadre de l'EPCIP.

Question

Est-il souhaitable que le chaque État membre adopte un programme national de PIC fondé sur l'EPCIP?

7.3. Organisme de surveillance unique

Pour parvenir à l'efficacité et à la cohérence recherchées, il faudrait que chaque État membre désigne un organisme de surveillance unique, qui serait chargé de la mise en œuvre globale de l'EPCIP. Deux solutions peuvent être envisagées:

a) un organisme de surveillance unique en matière de PIC;

b) un point de contact national, n'ayant aucun pouvoir, l'organisation étant laissée au choix des États membres.

Cet organisme pourrait coordonner, contrôler et surveiller la mise en œuvre de l'EPCIP sur le territoire relevant de sa compétence et pourrait servir de principal point de contact institutionnel pour les questions de PIC avec la Commission, avec les autres États membres et avec les propriétaires et les exploitants d'infrastructures critiques. Il pourrait assurer une représentation nationale au sein des groupes d'experts traitant des questions de PIC et pourrait être connecté au réseau d'alerte concernant les infrastructures critiques (CIWIN). L'organisme national de coordination de la PIC (ONCPIC) pourrait coordonner les actions nationales en matière de PIC, sans préjudice des actions déjà entreprises en la matière par d'autres organismes ou entités de l'État membre dont il relève.

Le recensement progressif des ICN pourrait s'effectuer en obligeant les propriétaires et les exploitants d'infrastructures à notifier à l'ONCPIC toute activité économique liée à la PIC.

L'ONCPIC pourrait être chargé de prendre la décision formelle de classement d'une infrastructure en tant qu'ICN. Seul l'État membre concerné pourrait avoir accès à cette information.

Cet organisme pourrait avoir les compétences suivantes:

a) coordonner, contrôler et surveiller la mise en œuvre globale de l'EPCIP dans un État membre;

b) servir de principal point de contact institutionnel sur les questions relatives à la PIC avec:

   i. la Commission

   ii. les autres États membres

   iii. les propriétaires et les exploitants d'infrastructures critiques

c) participer au classement en tant qu'infrastructures critiques de l'UE (ICE);

d) prendre la décision formelle de classement en tant qu'infrastructure critique nationale d'une infrastructure relevant de sa compétence;

e) servir d'autorité de recours pour les propriétaires/exploitants qui ne sont pas d'accord avec le classement de leur infrastructure comme «infrastructure critique»;

f) participer à l'élaboration du programme national de protection des infrastructures critiques et des programmes de PIC sectoriels;

g) recenser les interdépendances entre les différents secteurs d'infrastructures critiques;

h) contribuer aux approches de la PIC par secteurs en participant à des groupes d'experts. Les représentants des propriétaires et des exploitants pourraient être invités à contribuer aux discussions. Des réunions régulières pourraient être organisées;

i) surveiller le processus d'élaboration de plans d'intervention pour les IC.

Questions

Partagez-vous l'opinion que les États membres devraient être seuls responsables du classement et de la gestion des ICN mais en respectant le cadre commun de l'EPCIP?

Est-il souhaitable de désigner un organisme de coordination de la PIC dans chaque État membre, qui serait chargé de la coordination globale des mesures relatives à la PIC, mais devrait respecter les responsabilités sectorielles existantes (celles des autorités de l'aviation civile, celles découlant de la directive Seveso, etc.)?

Les compétences proposées pour un tel organisme de coordination vous paraissent-elles convenir? Voyez-vous d'autres compétences qui pourraient être nécessaires?

7.4. ICN: Étapes de mise en œuvre

La Commission proposerait, pour les ICN, les étapes de mise en œuvre suivantes:

(1) Sur la base de l'EPCIP, les États membres définissent les critères spécifiques à utiliser pour recenser les ICN.

(2) Les États membres recensent et vérifient progressivement, secteur par secteur, les ICN.

(3) Les États membres analysent les failles existantes en matière de sûreté des ICN par secteur.

(4) Les États membres déterminent les secteurs prioritaires pour lesquels une action s'impose, en tenant compte des interdépendances et, le cas échéant, des priorités retenues au niveau de l'UE.

(5) Les États membres arrêtent, si nécessaire, des mesures de protection minimums pour chaque secteur.

(6) Les États membres sont chargés de veiller à ce que les propriétaires/exploitants des infrastructures relevant de leur compétence mettent en œuvre les mesures d'application nécessaires.

(7) Une surveillance régulière est assurée par les États membres. Il est procédé, pour autant que de besoin, à des révisions (mesures et recensement d'infrastructures critiques).

Question

En ce qui concerne les ICN, la liste des étapes de mise en œuvre vous paraît-elle adaptée? Certaines de ces étapes sont-elles superflues? Faudrait-il en ajouter d'autres?

8. RÔLE DES PROPRIÉTAIRES, DES EXPLOITANTS ET DES UTILISATEURS D'INFRASTRUCTURES CRITIQUES

8.1. Responsabilités des propriétaires, des exploitants et des utilisateurs d'infrastructures critiques

Le classement en tant qu'infrastructure critique fait peser certaines responsabilités sur les propriétaires et les exploitants. Quatre responsabilités pourraient être envisagées pour les propriétaires et les exploitants d'infrastructures classées comme ICN ou ICE:

(1) **Notification à l'organisme d'un État membre compétent en matière de PIC du fait qu'une infrastructure peut présenter un caractère critique.**

(2) **Désignation d'un ou de plusieurs représentants de haut rang comme officiers de liaison pour la sûreté (OLS) entre le propriétaire/exploitant et l'autorité d'un État membre compétente en matière de PIC**. L'OLS participerait à la conception des plans de sûreté et d'intervention. Il serait l'officier de liaison principal pour les relations avec l'organisme sectoriel compétent en matière de PIC dans les États membres et, le cas échéant, avec les services répressifs.

(3) **Établissement, mise en œuvre et mise à jour d'un plan de sûreté pour les exploitants (PSE)**. Une proposition de modèle de PSE est jointe en tant qu'annexe 3.

(4) **Participation**, avec les autorités des États membres compétentes en matière de protection civile et avec les services répressifs, si nécessaire, **à la conception d'un plan d'intervention pour les IC**.

Le PSE pourrait être soumis à l'approbation de l'autorité sectorielle compétente, dans un État membre, en matière de PIC, sous la surveillance globale de l'ONCPIC, qu'il s'agisse d'une ICN ou d'une ICE, de façon à assurer la cohérence des mesures de sûreté prises par les propriétaires et les exploitants ainsi que par les secteurs concernés en général. En contrepartie, l'ONCPIC et, s'il y a lieu, la Commission pourraient fournir aux propriétaires et aux exploitants des informations utiles et leur apporter un soutien approprié quant aux menaces auxquels ils sont exposés et quant à la définition des meilleures pratiques et, le cas échéant, ils pourraient les aider dans l'appréciation des interdépendances et des vulnérabilités.

Chaque État membre pourrait imposer aux propriétaires et aux exploitants d'ICN et d'ICE (dans le cas des ICE, la Commission serait également associée) un délai pour l'élaboration du PSE et pourrait, en cas de non-respect de ce délai, leur infliger des amendes administratives.

Il est proposé que le PSE recense les actifs des infrastructures critiques du propriétaire/de l'exploitant et définisse les mesures de sûreté à mettre en œuvre pour leur protection. Le PSE décrirait les méthodes à appliquer et la procédure à suivre afin d'assurer la conformité avec l'EPCIP et les programmes de PIC nationaux et sectoriels. Le PSE pourrait correspondre à une approche ascendante de la réglementation de la PIC, qui laisse au secteur privé une plus grande liberté d'action (et aussi davantage de responsabilités).

Dans certains cas, lorsque sont en cause des infrastructures telles que les réseaux d'électricité et les réseaux d'information, il serait irréaliste (d'un point de vue pratique et financier) d'attendre des propriétaires et des exploitants qu'ils entourent tous leurs actifs de niveaux de sûreté identiques. En pareil cas, il est suggéré que les propriétaires et les exploitants recensent, avec les autorités compétentes, les points critiques (nœuds) d'un réseau physique ou d'information sur lesquels les mesures de sûreté pourraient être ciblées.

Le PSE pourrait prévoir deux types de mesures de sûreté:

- des **mesures de sûreté permanentes**, qui préciseraient les investissements et les moyens nécessaires en matière de sûreté, mais que le propriétaire/l'exploitant ne peut réaliser ou mobiliser à bref délai. Le propriétaire/l'exploitant maintiendrait une vigilance permanente contre les menaces potentielles, sans que ces mesures ne perturbent ses activités économiques, administratives et sociales courantes;

- des **mesures de sûreté graduelles**, qui pourraient être déclenchées en fonction de différents niveaux de menace. Le PSE prévoirait donc différents régimes de sûreté adaptés à des niveaux de menace potentiels définis pour l'État membre où l'infrastructure est située.

Il est proposé que le non-respect, par un propriétaire ou un exploitant d'infrastructure critique, de l'obligation de concevoir un PSE, de contribuer à l'élaboration de plans d'intervention et de désigner un OLS puisse donner lieu à une sanction financière.

Questions

Les responsabilités potentielles des propriétaires/exploitants d'infrastructures critiques sont-elles acceptables dans l'optique d'un renforcement de la sûreté des infrastructures critiques? Quel en serait le coût prévisible?

Les propriétaires et les exploitants devraient-ils être obligés de notifier le fait que leur infrastructure peut présenter un caractère critique? Pensez-vous que l'idée d'un PSE soit utile? Pour quelle(s) raison(s)?

Les responsabilités proposées sont-elles proportionnées aux coûts qu'elles impliquent?

Quels droits les autorités des États membres et la Commission pourraient-ils accorder aux propriétaires et aux exploitants d'infrastructures critiques?

8.2. Dialogue avec les propriétaires, les exploitants et les utilisateurs d'infrastructures critiques

L'EPCIP pourrait inciter les propriétaires et les exploitants à former des partenariats. Le succès d'un programme de protection dépend du niveau de coopération et de participation qui peut être mis en œuvre avec les propriétaires et les exploitants. Dans les États membres, les propriétaires et les exploitants d'infrastructures critiques pourraient être étroitement associés aux progrès en matière de PIC grâce à des contacts réguliers avec l'ONCPIC.

Au niveau de l'UE, des espaces de discussions pourraient être prévus afin de faciliter les échanges de vues sur les questions de PIC générales et sectorielles. L'adoption d'une approche commune de la participation du secteur privé aux travaux sur la PIC, visant à faire se rencontrer tous les acteurs, publics et privés, concernés permettrait aux États membres, à la Commission et aux entreprises de discuter ensemble de toute nouvelle question qui pourrait se poser en matière de PIC. Les propriétaires, les exploitants et les utilisateurs d'infrastructures critiques pourraient contribuer à la définition d'orientations communes et de meilleures pratiques et, le cas échéant, au partage des informations. Ce dialogue aiderait à déterminer les points à revoir dans le cadre des futures révisions de l'EPCIP.

Le cas échéant, la Commission pourrait encourager la création d'associations professionnelles ou sectorielles de l'UE en matière de PIC. Les deux objectifs ultimes seraient de faire en sorte que les entreprises européennes restent compétitives et que la sécurité des citoyens de l'UE soit renforcée.

Question

Comment le dialogue avec les propriétaires, les exploitants et les utilisateurs d'infrastructures critiques devrait-il être structuré?

Qui devrait représenter les propriétaires, les exploitants et les utilisateurs dans le cadre du dialogue entre le public et le privé?

9. MESURES DE SOUTIEN DE L'EPCIP

9.1. Le réseau d'alerte concernant les infrastructures critiques (CIWIN)

La Commission a mis au point un certain nombre de systèmes d'alerte rapide afin de réagir, par des mesures concrètes, coordonnées et efficaces, aux situations d'urgence, notamment celles d'origine terroriste. Le 20 octobre 2004, la Commission a annoncé la création, au sein de la Commission, d'un réseau central pour la circulation rapide des informations entre tous les systèmes d'alerte rapide de la Commission et les services de la Commission concernés (ARGUS).

La Commission propose de créer le CIWIN, réseau qui pourrait accélérer la définition de mesures de protection appropriées en facilitant l'échange sécurisé des meilleures pratiques et en servant de moyen de transmission des alertes immédiates et des informations sur les menaces immédiates. Grâce à ce système, les bonnes personnes obtiendraient les bonnes informations au bon moment.

Le CIWIN pourrait être conçu selon l'une des trois options suivantes:

(1) **Conception du CIWIN comme un espace de discussion limité à l'échange d'idées et de meilleures pratiques en matière de PIC** et destiné à assister les propriétaires et les exploitants d'infrastructures critiques. Cet espace de discussion pourrait prendre la forme d'un réseau d'experts et d'une plate-forme électronique pour l'échange des informations utiles dans un environnement sécurisé. La Commission jouerait un rôle important en recueillant et en diffusant ces informations. Cette option ne permettrait pas de transmettre les alertes rapides nécessaires en cas de menaces imminentes, mais le CIWIN pourrait être étendu par la suite.

(2) Conception du CIWIN comme un système d'alerte rapide (SAR), reliant les États membres et la Commission: cette option renforcerait la sûreté des infrastructures critiques en signalant exclusivement les menaces et les alertes immédiates. Elle aurait pour objectif de faciliter l'échange rapide d'informations sur des menaces potentielles auxquelles seraient exposés les propriétaires et les exploitants d'infrastructures critiques. Le système d'alerte rapide n'impliquerait pas le partage de renseignements à long terme. Il servirait au partage rapide d'informations sur des menaces imminentes pesant sur certaines infrastructures.

(3) Conception du CIWIN comme un système de communication/d'alerte à plusieurs niveaux assurant deux fonctions distinctes: a) un système d'alerte rapide (SAR) reliant les États membres et la Commission et b) un espace de discussion pour l'échange d'idées et de meilleures pratiques en matière de PIC, destiné à assister les propriétaires et les exploitants d'infrastructures critiques et composé d'un réseau d'experts et d'une plate-forme d'échange de données électronique.

Quelle que soit l'option retenue, le CIWIN compléterait les réseaux existants et des mesures seraient prises afin d'éviter les doubles emplois. À terme, une connexion du CIWIN avec tous les propriétaires et exploitants d'infrastructures critiques concernés, dans tous les États membres, par exemple par l'intermédiaire de l'ONCPIC, pourrait être envisagée. Les alertes et les meilleures pratiques pourraient être diffusées par cet organisme, le seul service à être directement relié à la Commission et, partant, à tous les autres États membres. Les États membres pourraient utiliser leurs systèmes d'information existants pour mettre en place un prolongement national du CIWIN, qui relierait leurs autorités aux propriétaires et aux exploitants d'infrastructures critiques. Qui plus est, ces réseaux nationaux pourraient servir de système de communication dans les deux sens entre les organismes des États membres compétents en matière de PIC et les propriétaires/exploitants.

Une étude sera lancée afin de déterminer l'étendue et les caractéristiques techniques de la future interface entre le CIWIN et les États membres.

Questions

Quelle forme devrait prendre le réseau CIWIN afin de soutenir les objectifs de l'EPCIP?

Les propriétaires et les exploitants d'infrastructures techniques devraient-ils être reliés au CIWIN?

9.2. Méthodologies communes

Les États membres ont prévu des niveaux d'alerte différents en fonction des situations considérées. À l'heure actuelle, il n'y a aucun moyen de savoir si, par exemple, un niveau d'alerte «élevé» dans un État membre est identique à un niveau d'alerte déclaré «élevé» dans un autre État membre. Dès lors, il pourrait être difficile pour les entreprises transnationales de définir un ordre de priorité dans les dépenses à consacrer aux mesures de protection. Il pourrait par conséquent être intéressant de chercher à harmoniser ou à étalonner les niveaux d'alerte.

Pour chaque niveau de menace, on pourrait prévoir un niveau de préparation permettant le déclenchement de mesures de sûreté communes d'une manière générale et, le cas échéant, de mesures de sûreté graduelles. Les États membres qui ne souhaiteraient pas appliquer une mesure donnée pourraient faire face à une menace particulière en recourant à d'autres mesures de sûreté.

Une méthodologie commune pourrait être envisagée afin de recenser et de classer les menaces, les capacités, les risques et les vulnérabilités, et afin de tirer des conclusions sur la possibilité, la probabilité et le degré de gravité d'une menace d'interruption d'une infrastructure. Cette méthodologie comprendrait une évaluation et un classement des risques par ordre de priorité, ce qui permettrait de définir les événements à risque en termes de probabilités, d'impact et de rapports avec d'autres secteurs ou processus à risque.

Questions

Jusqu'à quel point est-il souhaitable et réaliste d'harmoniser ou d'étalonner les différents niveaux d'alerte?

Faudrait-il définir une méthodologie commune afin de recenser et de classer les menaces, les capacités, les risques et les vulnérabilités, et de tirer des conclusions sur la possibilité, la probabilité et le degré de gravité d'une menace?

9.3. Financement

En réponse à une initiative du Parlement européen (création d'une nouvelle ligne budgétaire – projet pilote «Lutte contre le terrorisme» - dans le budget 2005), la Commission a décidé, le 15 septembre 2005, d'accorder une enveloppe de 7 millions d'euros pour le financement d'un train de mesures qui amélioreront la prévention, la préparation et la réponse européennes aux attaques terroristes, y compris la gestion des conséquences, la protection des infrastructures critiques, ainsi que les actions dans le domaine du financement du terrorisme, des explosifs et de la radicalisation violente. Plus des deux tiers de ce budget sont consacrés à la préparation du futur programme européen de protection des infrastructures critiques, à l'intégration et au développement des capacités requises pour gérer les crises de dimension transnationale liées aux menaces d'attaques terroristes, ainsi qu'aux mesures d'urgence qui peuvent se révéler nécessaires pour faire face à une menace sérieuse ou à une attaque. Ce financement devrait se poursuivre en 2006.

De 2007 à 2013, il sera relayé par le programme-cadre «Sécurité et protection des libertés». Ce dernier comprendra un programme spécifique intitulé «Prévention, préparation et gestion des conséquences en matière de terrorisme». La Commission a proposé une enveloppe de 137,4 millions d'euros, destinée au recensement des besoins en la matière et à l'élaboration de normes techniques communes pour la protection des infrastructures critiques.

Ce programme permettra d'accorder un financement communautaire aux projets présentés par les autorités nationales, régionales et locales pour la protection des infrastructures critiques. Il est focalisé sur le recensement des besoins en matière de protection et sur la fourniture d'informations en vue de l'élaboration de normes communes et de l'évaluation des menaces et des risques, afin de protéger les infrastructures critiques, ou de la mise au point de plans d'intervention spécifiques. La Commission utiliserait son savoir-faire existant ou pourrait contribuer au financement d'études sur les interdépendances dans certains secteurs. C'est donc principalement aux États membres, ou aux propriétaires et aux exploitants, qu'il incombe d'améliorer la sûreté de leurs infrastructures en fonction des besoins recensés. Le programme proprement dit ne finance pas l'amélioration de la protection des infrastructures critiques. Les institutions financières pourraient accorder des prêts en vue d'améliorer la sûreté des infrastructures des États membres en fonction des besoins recensés dans le cadre de ce programme, et afin de mettre en œuvre des normes communes. La Commission serait disposée à financer des études sectorielles visant à évaluer les incidences financières que l'amélioration de la sûreté des infrastructures pourrait entraîner pour les entreprises.

La Commission finance des projets de recherche axés sur la PIC dans le cadre de l'action préparatoire en matière de recherche sur la sécurité[2] (2004-2006) et a prévu des actions plus poussées dans le domaine de la recherche en matière de sécurité dans sa proposition de décision du Conseil et du Parlement européen concernant le 7ème programme-cadre de la CE pour des activités de recherche (COM(2005) 119 final)[3] et dans sa proposition de décision du Conseil relative au programme spécifique «Coopération» mettant en œuvre le 7e programme-cadre (COM(2005) 440 final). Des recherches ciblées, visant à nous doter de stratégies pratiques ou d'outils pour l'atténuation des risques, sont d'une importance capitale pour la sécurisation des infrastructures critiques de l'UE à moyen et long terme. Toutes les recherches en matière de sécurité, y compris dans ce domaine, feront l'objet d'un examen éthique afin de s'assurer de leur compatibilité avec la Charte des droits fondamentaux de l'Union européenne. La demande de travaux de recherche ne progressera qu'avec l'augmentation des interdépendances entre les infrastructures.

Questions

Quels seraient, selon vous, le coût et l'impact, pour les administrations et les entreprises, de la mise en œuvre des mesures proposées dans le présent livre vert? D'après vous, seraient-ils proportionnés?

---

2 Le montant total des crédits inscrits aux budgets 2004 et 2005 s'élève à 30 millions d'euros. Pour 2006, la Commission a proposé un montant de 24 millions d'euros, qui est soumis à l'examen de l'autorité budgétaire.

3 Le budget que la Commission a proposé pour les activités de recherche liées à la sécurité et à l'espace au titre du 7e programme-cadre est de 570 millions d'euros (COM(2005) 119 final).

9.4. Évaluation et suivi

Pour assurer l'évaluation et le suivi de la mise en œuvre de l'EPCIP, il faudrait un prévoir un processus à plusieurs niveaux auquel participeraient toutes les parties concernées:

- **au niveau de l'UE, on pourrait mettre en place un mécanisme d'évaluation par les pairs**, dans le cadre duquel les États membres et la Commission travailleraient de concert à l'évaluation du niveau global de mise en œuvre de l'EPCIP dans chaque État membre. La Commission pourrait préparer des rapports d'activité annuels sur la mise en œuvre de l'EPCIP;

- **chaque année civile, la Commission informerait les États membres et les autres institutions des progrès accomplis**, dans un document de travail de ses services;

- **au niveau des EM, l'ONCPIC de chaque État membre pourrait surveiller la mise en œuvre globale de l'EPCIP sur le territoire relevant de sa compétence, en veillant au respect du ou des programmes de PIC nationaux et sectoriels**, afin de vérifier qu'ils sont tous effectivement mis en œuvre, et présenterait des rapports annuels à cet égard au Conseil et à la Commission.

La mise en œuvre de l'EPCIP serait un processus dynamique, évolutif et évalué en continu de manière à suivre le rythme des évolutions et à tirer les enseignements de l'expérience acquise. Les évaluations par les pairs et les rapports de suivi des États membres pourraient faire partie des instruments utilisés pour réviser l'EPCIP et proposer de nouvelles mesures afin de renforcer la protection des infrastructures critiques.

Les informations utiles recueillies par les États membres sur les ICE pourraient être communiquées à la Commission pour la mise sur pied d'évaluations communes des vulnérabilités, de plans de gestion des conséquences, de normes communes pour la protection des infrastructures critiques, ainsi que pour la fixation d'un ordre de priorité dans les recherches et, le cas échéant, en vue d'une réglementation et d'une harmonisation. Ces informations seraient classifiées et resteraient strictement confidentielles.

La Commission pourrait contrôler les différentes initiatives des États membres, notamment celles qui prévoient des sanctions financières pour les propriétaires et les exploitants qui sont dans l'incapacité de rétablir des services essentiels aux citoyens dans le délai imparti.

Question

Quel type de mécanisme d'évaluation faudrait-il envisager pour l'EPCIP? Le mécanisme décrit ci-dessus serait-il suffisant?

Les réponses doivent être envoyées au plus tard le 15 janvier 2006 à l'adresse électronique suivante: **JLS-EPCIP@cec.eu.int**. Ces réponses resteront confidentielles, à moins que leur auteur ne déclare expressément souhaiter qu'elles soient rendues publiques, auquel cas elles seront chargées sur le site internet de la Commission.

ANNEXES

ANNEX 1

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure 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.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  - Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  - Environment (effect on the public and surrounding location);

  - Interdependency (between other critical infrastructure elements).

  - Political effects (confidence in the ability of government);

  - Psychological effects (may escalate otherwise minor events). both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

ANNEX 3

OPERATOR SECURITY PLAN

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

Introduction)

Contains information concerning the pursued objectives and the main organisational and protection principles.

Detailed part *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. 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 may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.