COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 20.10.2004
COM(2004) 702 final

COMMUNICATION DE LA COMMISSION AU CONSEIL ET AU PARLEMENT EUROPÉEN

Protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme

TABLE DES MATIÈRES

1. INTRODUCTION

Lors de sa réunion de juin 2004, le Conseil européen avait demandé à la Commission et au Haut Représentant d'élaborer une stratégie globale visant à renforcer la protection des infrastructures critiques.

La présente communication donne un aperçu des actions entreprises par la Commission en matière de protection des infrastructures critiques et propose des mesures supplémentaires visant à renforcer les instruments existants et à donner suite aux mandats conférés par le Conseil européen.

2. LA MENACE TERRORISTE

Le risque d'attentats terroristes catastrophiques susceptibles de toucher des infrastructures critiques s'accroît. Les conséquences d'une attaque visant les systèmes de contrôle des infrastructures critiques seraient très variables. On estime généralement qu'un cyber-attentat réussi ferait peu ou pas de victimes, mais pourrait interrompre le fonctionnement d'infrastructures vitales. Ainsi par exemple, un cyber-attentat réussi contre le réseau de téléphonie publique priverait les usagers des services téléphoniques jusqu'à ce que les techniciens réparent et rétablissent le réseau. Une attaque visant les systèmes de commande d'installations chimiques ou de gaz liquide pourrait occasionner un plus grand nombre de victimes et des dégâts matériels significatifs.

La défaillance d'une partie des infrastructures pourrait également entraîner des défaillances dans d'autres secteurs, produisant des effets en cascade. Pareil scénario pourrait résulter de la synergie qui existe entre les différentes infrastructures. Ainsi, un attentat visant des installations électriques pourrait entraîner une interruption de la distribution d'électricité mais également paralyser les installations d'épuration et de distribution d'eau si les turbines et les autres appareils électriques de ces installations ne sont plus alimentés.

Les réactions en cascade peuvent également entraîner beaucoup de dégâts en raison de l'interruption d'un grand nombre de services de base. Les pannes d'électricité survenues en Amérique du Nord et en Europe au cours des deux dernières années ont montré la vulnérabilité des infrastructures dans le domaine de l'énergie et partant, la nécessité de prendre des mesures efficaces afin de prévenir et/ou de limiter les conséquences découlant de graves perturbations dans la distribution. Cette utilisation du cyber-terrorisme pourrait également amplifier les effets d'une attaque physique, comme un attentat à la bombe dans un bâtiment combiné à une interruption provisoire de la distribution d'électricité ou des services téléphoniques. Dans ce cas, les difficultés d'intervention des services de secours en attendant le rétablissement de l'alimentation électrique ou des systèmes de communication pourraient augmenter le nombre de victimes et accroître la panique.

3. INFRASTRUCTURES CRITIQUES EN EUROPE

3.1. Définition des infrastructures critiques

Les infrastructures critiques sont les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction,

peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris le secteur bancaire et des finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base. Certains éléments critiques de ces secteurs ne peuvent être considérés comme des infrastructures au sens strict, puisqu'il s'agit plutôt de réseaux ou de chaînes d'approvisionnement qui sous-tendent la fourniture d'un produit ou d'un service essentiel. Par exemple, l'approvisionnement en denrées alimentaires ou en eau de nos grandes zones urbaines dépend de certaines installations clés, mais également d'un réseau complexe constitué de producteurs, de transformateurs, de fabricants, de distributeurs et de détaillants.

Les infrastructures critiques englobent:

- Les installations et les réseaux dans le secteur de l'énergie (notamment les installations de production d'électricité, de pétrole et de gaz, les installations de stockage et les raffineries, le système de transport et de distribution).

- Les technologies des communications et de l'information (les télécommunications, les systèmes de radiodiffusion, les logiciels, le matériel informatique et les réseaux, y compris l'internet, etc.)

- Les finances (le secteur bancaire, les marchés des valeurs et les investissements)

- Le secteur des soins de santé (hôpitaux, installations offrant des soins de santé et banques de sang, laboratoires et produits pharmaceutiques, services d'urgence, de recherche et de sauvetage)

- Alimentation (sécurité, moyens de production, distribution et industrie agroalimentaire)

- Eau (réserves, stockage, traitement et réseaux)

- Transports (aéroports, ports, installations intermodales, chemins de fer et réseaux de transit de masse, systèmes de contrôle du trafic)

- Production, stockage et transport de produits dangereux (matériaux chimiques, biologiques, radiologiques et nucléaires)

- Administration (services de base, installations, réseaux d'information, actifs et principaux sites et monuments nationaux)

Ces infrastructures appartiennent ou sont exploitées par le secteur public et le secteur privé. Toutefois, dans sa communication 574/2001 du 10 octobre 2001, la Commission a déclaré: «le renforcement de certaines de ces mesures (de sûreté) par les pouvoirs publics, à la suite d'attaques dirigées contre la société entière et non pas les acteurs impliqués dans le transport aérien…..doit être assumé par l'autorité publique». Le secteur public est donc appelé à jouer un rôle fondamental.

Les infrastructures critiques doivent être définies au niveau des États membres et au niveau européen, et ces listes devraient être établies avant la fin de 2005.

Les infrastructures critiques européennes sont étroitement liées et dépendantes les unes des autres. La concentration des entreprises, la rationalisation industrielle, les pratiques telles que la fabrication à flux tendus et la concentration de la population dans les zones urbaines sont autant de facteurs qui ont contribué à cette situation. Les infrastructures critiques d'Europe dépendent aujourd'hui davantage des technologies communes d'information, y compris l'internet, ainsi que des communications et de la radionavigation par satellite. Les problèmes peuvent se succéder en cascade au travers de ces infrastructures liées, et entraîner des défaillances inattendues et de plus en plus graves dans des services essentiels. Ces liens étroits et cette forte dépendance entre les infrastructures les rendent plus vulnérables face aux menaces d'interruption des services ou de destruction des installations.

Il convient d'étudier les critères sur la base desquels on considère que des infrastructures ou des éléments d'infrastructures sont critiques. Ces critères devraient également reposer sur des compétences sectorielles et collectives. On pourrait suggérer trois critères pour l'identification d'infrastructures critiques potentielles:

- L'étendue – la perte d'infrastructures critiques est mesurée en fonction de l'étendue de la région géographique susceptible d'être touchée – de dimension internationale, nationale, provinciale/territoriale ou locale.

- Le degré de gravité – l'incidence ou la perte peut être nulle, minimum, modérée ou élevée. Les critères suivants pourraient être utilisés pour mesurer le degré de gravité:

    (a) incidence sur le public (nombre de personnes touchées, décès, maladies, dommages corporels graves, évacuation);

    (b) incidence économique (effet sur le PIB, importance de la perte économique et/ou de la dégradation de produits ou services);

    (c) incidence environnementale (impact sur le public et sur l'environnement);

    (d) dépendance (à l'égard d'autres infrastructures critiques) ;

    (e) politique (confiance dans les capacités du gouvernement).

- L'effet dans le temps – ce critère détermine à quel moment la perte d'un élément pourrait avoir une incidence grave (immédiatement, après 24-48 heures, une semaine, autre).

Toutefois, dans de nombreux cas, des effets psychologiques peuvent aggraver des événements par ailleurs d'importance mineure.

L'annexe technique donne un aperçu des développements en matière de protection des infrastructures critiques, et dresse un bilan sectoriel des résultats obtenus à ce jour par la Commission. Il montre que la Commission a acquis une expérience considérable dans ce domaine.

3.2. Gestion de la sécurité

Pour analyser les infrastructures critiques des États membres et les éléments qui en dépendent face à la menace terroriste et pour déterminer leur vulnérabilité, il convient de récolter des informations auprès d'un certain nombre de sources. Chaque secteur et chaque État membre

devra identifier les infrastructures qu'il considère critiques sur son territoire, selon une formule harmonisée au niveau de l'UE et avec les organisations ou les personnes chargées de la sécurité.

Il est impossible de protéger toutes les infrastructures contre toutes les menaces terroristes. Ainsi, les réseaux de transport de l'électricité sont trop longs pour être protégés par des grillages ou pour être surveillés. Si l'on applique des techniques de gestion des risques, on peut se concentrer sur les points qui présentent le risque le plus élevé, en tenant compte de la menace, de la mesure dans laquelle les infrastructures sont critiques, du niveau actuel de protection et de l'efficacité des stratégies existantes pour limiter les incidences et assurer la continuité de l'activité.

La gestion de la sécurité est un processus délibéré visant à déterminer le risque et à définir et mettre en oeuvre des actions destinées à le ramener à un niveau déterminé et acceptable avec un coût acceptable. Cette approche consiste à identifier, mesurer et contrôler les risques pour les maintenir à un niveau correspondant à celui qui a été fixé.

La protection des infrastructures critiques (PIC) implique un partenariat cohérent, basé sur la collaboration entre les propriétaires et les exploitants des infrastructures critiques et les autorités des États membres. Les propriétaires et les exploitants demeurent les premiers responsables de la gestion du risque au niveau des installations physiques, des chaînes d'approvisionnement, des technologies de l'information et des réseaux de communication.

Les alertes, les conseils et les informations doivent être diffusés afin d'aider les partenaires du secteur public et du secteur privé à protéger leurs infrastructures principales. Il arrive que des risques ou des menaces spécifiques d'attentat terroriste exigent une réaction immédiate. Dans ce cas, les gouvernements et l'industrie des États membres doivent réagir de manière ciblée et bien coordonnée d'un point de vue opérationnel. De son côté, l'UE devrait coordonner les réactions politiques nécessaires et des dispositions seront définies avec les partenaires au cas par cas sur cette base.

Les meilleurs plans et les meilleures lois en matière de gestion de la sécurité ne servent à rien s'ils ne sont pas correctement appliqués. L'expérience montre que des inspections indépendantes de la Commission destinées à vérifier leur application constituent le seul instrument efficace permettant de garantir l'application correcte des contraintes en matière de sécurité.

4. PROGRES REALISES DANS LA PROTECTION DES INFRASTRUCTURES CRITIQUES AU NIVEAU COMMUNAUTAIRE

Les Européens s'attendent à ce que les infrastructures critiques continuent à fonctionner, quelle que soit l'organisation propriétaire ou exploitante. Dans ce sens, ils estiment que les gouvernements des États membres et l'UE doivent jouer un rôle prédominant. Ils espèrent que les propriétaires et les exploitants à tous niveaux du secteur public et du secteur privé collaboreront pour garantir la continuité des services dont ils dépendent.

Pour compléter les mesures prises au niveau national, l'Union européenne a déjà adopté un certain nombre de mesures législatives établissant des normes minimales pour la protection des infrastructures dans le cadre de différentes politiques communautaires. C'est notamment le cas pour les transports, les communications, l'énergie, la santé et la sécurité au travail et

tous les secteurs de la santé publique. Un nouvel élan a été donné à ces activités après les attentats perpétrés récemment en Amérique et en Europe. Elles permettront de continuer à améliorer et d'étendre les mesures existantes.

Pendant des décennies, des inspections ont été effectuées dans le cadre du traité EURATOM afin de contrôler la bonne utilisation des matériaux nucléaires. Dans le domaine de la protection contre les radiations, il existe un nombre considérable de lois s'appliquant aux risques liés à l'utilisation des installations et des sources contenant des substances radioactives.

Dans le domaine des transports internationaux, l'Union européenne a adopté des lois qui permettent d'appliquer ou de renforcer les accords intervenus au sein des organismes internationaux de réglementation de l'aviation et des transports maritimes. L'Union européenne continuera à promouvoir leurs activités au niveau international et à y participer. Elle encouragera les pays tiers qui ont des relations économiques avec elle à appliquer ces accords. Elle a accordé une assistance à certains d'entre eux afin de parvenir à un niveau homogène et constant de sécurité à l'intérieur et au-delà des frontières de l'UE.

La création d'agences, comme l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour la sécurité des communications, constitue une autre avancée. De plus, dans des secteurs comme la sécurité des transports aériens et maritimes, des services d'inspection ont été mis sur pied au sein de la Commission pour contrôler l'application de la législation en matière de sécurité dans les États membres. Ces inspections permettent d'établir des points de repère et d'assurer un niveau de mise en oeuvre uniforme dans l'ensemble de l'Union.

L'annexe technique contient des informations relatives aux développements actuels en matière de protection des infrastructures critiques, et comporte un aperçu sectoriel des résultats obtenus jusqu'ici par la Commission. Ils montrent que la Commission a acquis une expérience considérable dans ce domaine.

5. RENFORCER LA CAPACITÉ DE PROTECTION DES INFRASTRUCTURES CRITIQUES DE L'UE

5.1. Un programme européen de protection des infrastructures critiques

Compte tenu du grand nombre d'infrastructures critiques potentielles et de leurs caractéristiques individuelles, il est impossible de les protéger toutes au niveau européen. En appliquant le principe de subsidiarité, l'Europe doit concentrer ses efforts sur la protection des infrastructures qui présentent une dimension transnationale et laisser les autres à la seule responsabilité des États membres, mais dans un cadre commun.

De nombreuses directives et réglementations existent déjà, et imposent des moyens pour la détection d'accidents, l'élaboration de plans d'intervention en collaboration avec la protection civile, des exercices réguliers et des liens clairs entre les différents niveaux d'intervention, les pouvoirs publics, les organisations centrales et les services d'urgence. Par ailleurs, il reste encore beaucoup à faire pour la protection des installations de production d'énergie autre que l'énergie nucléaire. Comme l'indique l'annexe technique, il existe un acquis communautaire en matière de protection des infrastructures critiques à des niveaux de développement divers.

Dans la plupart des domaines mentionnés ci-dessus, le travail se poursuit, et une coopération est mise en place avec les experts des États membres et les secteurs économiques concernés en vue d'identifier d'éventuelles lacunes et les mesures correctives à apporter (mesures juridiques ou autres). Un grand nombre de réseaux et de comités de sécurité ont été mis sur pied.

Chaque année, la Commission adressera une communication aux autres institutions pour les informer des progrès réalisés. Elle analysera pour chaque secteur l'évolution du travail communautaire en ce qui concerne l'évaluation du risque, le développement de techniques de protection et les actions juridiques en cours ou envisagées en vue d'obtenir leur avis. Le cas échéant, la Commission proposera également dans cette communication des mises à jour et des mesures d'organisation horizontale impliquant une harmonisation, une coordination ou une collaboration. Cette communication qui englobera toutes les analyses et mesures sectorielles constituera la base d'un programme européen de protection des infrastructures critiques (EPCIP).

Ce programme devra aider l'industrie et les gouvernements des États membres à tous les niveaux dans l'UE, tout en respectant les responsabilités et les mandats individuels. La Commission estime qu'un réseau réunissant les spécialistes des États membres de l'UE en matière de protection des infrastructures critiques pourrait l'aider à élaborer le programme – ce réseau d'alerte concernant les infrastructures critiques (CIWIN – Critical Infrastructure Warning Information Network) devrait être mis sur pied le plus rapidement possible en 2005.

La création du réseau devrait principalement contribuer à encourager l'échange d'informations concernant des menaces et des vulnérabilités communes, et l'échange de mesures et de stratégies adéquates permettant de limiter le risque et de protéger les infrastructures critiques. Les États membres devraient à leur tour s'assurer que les informations sont transmises à tous les départements ministériels et à tous les organismes concernés, y compris les services d'urgence et les secteurs industriels qui seront quant à eux chargés d'informer les propriétaires et les exploitants des infrastructures critiques au travers d'un réseau de contacts mis en place au sein des États membres.

Le programme EPCIP permettrait de constituer un forum permanent en vue de rechercher l'équilibre entre les contraintes de concurrence, de responsabilité et de sensibilité de l'information et les avantages découlant d'infrastructures critiques plus sûres. L'industrie sera étroitement associée à ce processus. Le programme contribuera à transmettre plus d'informations aux partenaires concernant des situations de menace spécifique, pour leur permettre de prendre des mesures et de faire face aux conséquences éventuelles. Rien ne devrait changer en ce qui concerne la responsabilité des propriétaires et des exploitants, qui doivent prendre leurs décisions et adopter des plans pour la protection de leurs actifs.

Lorsqu'il n'existe pas de normes sectorielles ou de normes internationales, le Comité européen de normalisation (CEN) et d'autres organismes de normalisation pourraient aider le réseau et proposer des normes de sécurité sectorielles uniformes et adaptées pour tous les secteurs concernés. De telles normes devraient également être proposées au niveau international par le biais de l'ISO, afin de mettre en place des conditions uniformes.

Les menaces qui pèsent sur les infrastructures critiques doivent être évoquées avec prudence, afin de ne pas susciter d'inquiétudes inutiles au sein de la population de l'UE, ni parmi les touristes et investisseurs potentiels. Le terrorisme est une menace constante, mais les décideurs politiques doivent encourager leurs concitoyens à mener une vie aussi normale que

possible. Il y a lieu également de préserver le droit à la vie privée, à l'intérieur et à l'extérieur de l'Union. Les consommateurs et les acteurs économiques doivent être certains que les informations à caractère confidentiel sont manipulées d'une manière correcte et fiable. Un cadre adéquat doit garantir que les informations classifiées sont gérées correctement et protégées contre toute divulgation ou utilisation non autorisée.

Une partie importante des infrastructures critiques de l'UE et des États membres dépassent les frontières de l'UE. Les oléoducs s'étendent sur des continents entiers, des câbles indispensables au bon fonctionnement des technologies de l'information sont enterrés sous les océans, etc. Par conséquent, la coopération internationale joue un rôle important dans la mise en place de partenariats nationaux et internationaux dynamiques entre les propriétaires et les exploitants d'infrastructures critiques et les gouvernements des pays tiers, en particulier lorsqu'il s'agit de fournisseurs directs de l'Union dans le secteur de l'énergie.

5.2. Mise en œuvre du programme EPCIP

La protection des infrastructures critiques implique la participation active des propriétaires et des exploitants des infrastructures, des organes de réglementation, des organisations professionnelles et industrielles, des États membres et de la Commission. À partir des informations fournies par les États membres et mises sur le réseau, l'objectif du programme EPCIP sera de continuer à identifier les infrastructures critiques, d'analyser leur vulnérabilité et leur dépendance les unes par rapport aux autres, de présenter des solutions en vue de les protéger contre tous les dangers et de les y préparer. Dans ce but, il devrait notamment aider les secteurs industriels à déterminer la menace terroriste et ses conséquences potentielles dans leur analyse du risque. Les organes de répression des États membres et la protection civile devraient intégrer le programme EPCIP dans leurs activités de programmation et de sensibilisation.

En étroite coordination avec le réseau, les services de la Commission prendront d'autres mesures, notamment l'adoption d'une législation et/ou la diffusion de l'information. La task force des chefs de police et Europol devraient contribuer à la diffusion des renseignements et des informations relatives aux niveaux de sécurité auprès des organes de répression des États membres qui, à leur tour, devraient être en contact avec les propriétaires et les exploitants des infrastructures critiques, les conseiller au sujet des informations relatives à la menace terroriste et contribuer à mettre en place des stratégies de protection contre le terrorisme.

Les gouvernements des États membres continueront à développer et à alimenter des bases de données concernant les infrastructures critiques au niveau national et seront chargés de l'élaboration, de la validation et de la vérification des plans appropriés, et d'assurer ainsi la continuité des services sur leur territoire. Lorsqu'elle définira le programme EPCIP, la Commission présentera des suggestions quant au contenu minimum et au format de ces bases de données et la manière de les relier entre elles.

Les gouvernements des États membres devraient continuer à communiquer aux propriétaires et aux exploitants des infrastructures critiques (ainsi qu'aux autres États membres, le cas échéant) les renseignements pertinents et les alertes, et leur faire part du type de réaction défini pour chaque niveau de menace/alerte.

Les propriétaires et les exploitants des infrastructures critiques sécuriseront leurs actifs d'une manière adéquate grâce à la mise en oeuvre de leurs plans en matière de sécurité et à la réalisation d'inspections régulières, d'exercices, d'évaluations et de plans. Les États membres

superviseront le processus de manière générale et la Commission garantira une mise en œuvre uniforme dans toute l'Union au moyen de systèmes d'inspection appropriés.

5.3. Objectifs du programme EPCIP et indicateurs de progrès

L'objectif du programme EPCIP et le rôle de la Commission seraient de garantir des niveaux de protection adéquats 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 qui ont été testés. Le programme sera en évolution constante et sera réexaminé régulièrement en fonction de l'évolution des problèmes et des préoccupations au sein de la Communauté.

Le succès sera mesuré sur la base des éléments suivants:

- L'identification et l'élaboration d'inventaires par les gouvernements des États membres concernant les infrastructures critiques situées sur leur territoire en fonction des priorités établies par le programme EPCIP;

- La collaboration des entreprises au sein de leur secteur et avec leur gouvernement pour partager l'information et pour réduire le risque d'incidents susceptibles d'entraîner des perturbations étendues ou durables des infrastructures critiques;

- La Communauté européenne définit une approche commune pour aborder le problème de la sécurité des infrastructures critiques grâce à la collaboration de tous les acteurs publics et privés.

TECHNICAL ANNEX

GLOSSARY

Critical Infrastructure (CI)

Those physical resources; services; and information technology facilities, networks and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Europeans or the effective functioning of the EU or its Member States governments.

Critical infrastructure Warning Information Network (CIWIN)

A EU network to assist Member States, EU Institutions, owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.

Critical Infrastructure Protection (CIP)

The programs, activities and interactions used by owners and operators to protect their critical infrastructure.

CIP capability

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

European programme for Critical Infrastructure Protection (EPCIP)

A programme to provide enhanced security for critical infrastructure as an ongoing, dynamic, national partnership among EU institutions, critical infrastructure owner/operators and EU Member States to assure the continued functioning of Europe's critical infrastructure

Infrastructure

The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services, the smooth functioning of governments at all levels, and society as a whole.

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.

Risk Assessment

A process of evaluating threats to the vulnerabilities of an asset to give an expert opinion on the probability of loss or damage and its impact, as a guide to taking action.

Risk Management

A deliberate process of understanding risk and deciding upon and implementing actions to reduce risk to a defined level, which is an acceptable level of risk at an acceptable cost. This approach is characterized by identifying, measuring, and controlling risks to a level commensurate with an assigned level.

Threat

Any event that has 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.

Threat Assessment

A standardized and reliable manner to evaluate threats to infrastructure.

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.