COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 17.11.2005
COM(2005) 576 definitivo

LIBRO VERDE

RELATIVO A UN PROGRAMMA EUROPEO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

(presentato dalla Commissione)

LIBRO VERDE

RELATIVO A UN PROGRAMMA EUROPEO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE

1. BACKGROUND

Le infrastrutture critiche (IC) possono essere danneggiate, distrutte o manomesse a causa di atti deliberati di terrorismo, calamità naturali, negligenza, incidenti, pirateria informatica, attività criminose e comportamenti dolosi. Per tutelare la vita e i beni dei cittadini dell'UE dai rischi legati al terrorismo, alle calamità naturali e agli incidenti, bisogna fare in modo che gli eventuali danni alle infrastrutture critiche o la loro manomissione siano, nella misura del possibile, di breve durata, poco frequenti, gestibili, geograficamente isolati e il meno nocivi possibile per il benessere degli Stati membri, dei loro cittadini e dell'Unione europea. I recenti attentati terroristici di Madrid e Londra hanno evidenziato i rischi degli attentati terroristici contro le infrastrutture europee. Le reazioni a livello dell'UE devono essere rapide, coordinate ed efficaci.

Il Consiglio europeo del giugno 2004 ha chiesto alla Commissione di preparare una strategia globale per la protezione delle infrastrutture critiche. La Commissione ha risposto adottando, il 20 ottobre 2004, una comunicazione intitolata "La protezione delle infrastrutture critiche nella lotta contro il terrorismo" che presenta una serie di proposte chiare per incrementare la prevenzione, la preparazione e la risposta in caso di attentati terroristici che coinvolgono le infrastrutture critiche.

Le conclusioni del Consiglio sulla prevenzione, la preparazione e la risposta in caso di attentati terroristici e il programma di solidarietà dell'Unione europea sulle conseguenze delle minacce e degli attentati terroristici adottato dal Consiglio nel dicembre 2004 hanno appoggiato l'intenzione della Commissione di proporre un programma europeo per la protezione delle infrastrutture critiche (EPCIP) ed espresso il proprio accordo sulla costituzione, ad opera della Commissione, di una rete informativa di allarme sulle infrastrutture critiche (CIWIN).

La Commissione ha organizzato due seminari e ha invitato gli Stati membri a presentare idee e osservazioni. Il I seminario dell'UE sulla protezione delle infrastrutture critiche si è svolto il 6 e 7 giugno 2005 con la partecipazione degli Stati membri. Dopo il seminario, gli Stati membri hanno consegnato alla Commissione la documentazione relativa al loro approccio in materia di protezione delle infrastrutture critiche e hanno commentato le idee discusse nel corso del seminario. I contributi pervenuti in giugno e in luglio hanno costituito la base per gli sviluppi successivi della protezione delle infrastrutture critiche. Per portare avanti il dibattito sui problemi in materia di protezione delle infrastrutture critiche il 12 e 13 settembre si è svolto il II seminario dell'UE sulla protezione delle infrastrutture critiche. Al seminario hanno partecipato sia gli Stati membri che le associazioni industriali. La Commissione ha pertanto deciso di presentare il presente libro verde per illustrare le diverse alternative esistenti in materia di EPCIP.

2. OBIETTIVO DEL LIBRO VERDE

L'obiettivo principale del libro verde è di raccogliere indicazioni utili sulle diverse alternative strategiche possibili in materia di EPCIP coinvolgendo una gran parte di coloro che operano in tale settore. Una efficace protezione delle infrastrutture critiche richiede che vi siano comunicazione, coordinamento e cooperazione a livello nazionale e dell'UE tra tutte le parti interessate – i proprietari e i gestori delle infrastrutture critiche, le autorità di regolamentazione, le associazioni professionali e industriali in cooperazione con i diversi livelli del settore pubblico e con il settore privato.

Il libro verde fornisce alternative sul modo in cui la Commissione può rispondere alla richiesta del Consiglio di istituire un programma europeo per la protezione delle infrastrutture critiche e la CIWIN e costituisce la seconda fase di un processo di consultazione relativo all'istituzione di un programma europeo per la protezione delle infrastrutture critiche. La Commissione si aspetta di ricevere, a seguito di questo libro verde, concrete indicazioni circa le alternative strategiche esposte. Sulla base dei risultati del processo di consultazione sarà messo a punto nel corso del 2006 un pacchetto sulla politica in materia di EPCIP.

3. OBIETTIVI E PORTATA DELL'EPCIP

3.1. L'obiettivo globale dell'EPCIP

L'obiettivo dell'EPCIP consiste nel garantire che vi siano livelli adeguati e omogenei di sicurezza nella protezione delle infrastrutture critiche, punti deboli individuali minimi e sistemi di reazione rapida già sperimentati in tutta l'Unione. Il livello di protezione può non essere uguale per tutte le infrastrutture critiche e può essere legato all'impatto dell'interruzione del funzionamento di una infrastruttura critica. L'EPCIP sarà un processo in continua evoluzione e necessiterà di un riesame periodico per restare al passo con i nuovi problemi e preoccupazioni.

L'EPCIP deve cercare di ridurre al minimo le conseguenze negative che maggiori investimenti nella sicurezza potrebbero avere sulla competitività di una determinata impresa. Nel calcolare la proporzionalità dei costi non si deve perdere di vista la necessità di mantenere la stabilità dei mercati che è fondamentale per gli investimenti a lungo termine, le ripercussioni della sicurezza sui mercati azionari e sulla dimensione macroeconomica.

Domanda

Ritenete che tale obiettivo globale sia appropriato per un programma europeo finalizzato alla protezione delle infrastrutture critiche? In caso contrario, quale dovrebbe esserne l'obiettivo?

3.2. Da cosa deve proteggere il programma europeo per la protezione delle infrastrutture critiche

Sebbene le misure per la gestione delle conseguenze siano identiche o simili per la maggior parte dei danni, le misure di protezione possono variare in funzione del tipo di minaccia. Tra le minacce che incidono significativamente sulla capacità di provvedere alle esigenze fondamentali e alla sicurezza della popolazione, di mantenere l'ordine e di fornire i servizi pubblici minimi essenziali e il regolare funzionamento dell'economia rientrano gli attentati intenzionali e le calamità naturali. Le alternative sono:

a) **un approccio generale relativo a tutti i tipi di rischio** – Un approccio globale di questo tipo terrebbe conto sia delle minacce derivate da attentati intenzionali che di quelle legate alle calamità naturali e darebbe la possibilità di utilizzare al massimo le sinergie tra le misure di protezione, ma non si concentrerebbe in particolare sul terrorismo;

b) **un approccio relativo a tutti i rischi incentrato principalmente sul terrorismo** – Si tratta di un approccio flessibile che permette la connessione con altri tipi di fenomeni come la minacce derivanti da attentati intenzionali e da calamità naturali ma fa del terrorismo la sua priorità. Se il livello delle misure di protezione di un particolare settore dell'industria risultasse adeguato, gli operatori del settore potrebbero concentrarsi sulle minacce alle quali sono ancora vulnerabili.

c) **un approccio ai rischi incentrato sul terrorismo** - Si tratterebbe di un approccio incentrato sul terrorismo che non si occuperebbe di altri tipi più comuni di minaccia.

Domanda

Quale approccio dovrebbe scegliere l'EPCIP? Perché?

4. PROPOSTA SUI PRINCIPI FONDAMENTALI

Ci si propone di basare l'EPCIP sui seguenti principi fondamentali:

- **Sussidiarietà** – La sussidiarietà dovrebbe costituire il nucleo fondamentale dell'EPCIP anche se la protezione delle infrastrutture critiche è prima di tutto e soprattutto una responsabilità nazionale. La responsabilità primaria della protezione delle infrastrutture critiche dovrebbe spettare agli Stati membri e ai proprietari/gestori i quali agiscono all'interno di un quadro comune. A sua volta, la Commissione si concentrerebbe sugli aspetti relativi alla protezione delle infrastrutture critiche che hanno ripercussioni sulle frontiere dell'UE. Non dovrebbe cambiare nulla per quanto riguarda la responsabilità dei proprietari e dei gestori di prendere decisioni e di formulare piani per proteggere le proprietà.

- **Complementarietà** – Il quadro comune dell'EPCIP sarebbe complementare alle misure esistenti. Qualora vi siano già dei meccanismi comunitari, essi devono continuare ad essere utilizzati per garantire l'attuazione globale dell'EPCIP.

- **Riservatezza** – La condivisione delle informazioni sulla protezione delle infrastrutture critiche dovrebbe avvenire in un clima di fiducia e di riservatezza. Non si deve dimenticare che la conoscenza di fatti specifici su una infrastruttura critica può essere utilizzata per causare danni o conseguenze inaccettabili per gli impianti di infrastrutture critiche. Sia a livello dell'UE che a livello degli Stati membri, le informazioni relative alla protezione delle infrastrutture critiche saranno classificate e ne sarà dato l'accesso solo a chi ha bisogno di conoscerle.

- **Cooperazione tra gli operatori del settore** - Tutti gli operatori del settore, tra cui gli Stati membri, la Commissione, le associazioni professionali e industriali, gli organismi di regolamentazione e i proprietari, gestori e utilizzatori (intendendo per "utilizzatori" le organizzazioni che utilizzano le infrastrutture ai fini del commercio o della fornitura di servizi) hanno un ruolo da svolgere nella protezione delle infrastrutture critiche. Tutti gli

operatori devono cooperare e contribuire allo sviluppo e all'attuazione dell'EPCIP in funzione dei loro ruoli e responsabilità specifiche. Le autorità degli Stati membri provvedono a dirigere e coordinare l'elaborazione e l'attuazione di un approccio nazionale coerente alla protezione delle infrastrutture critiche nell'ambito delle loro giurisdizioni. I proprietari, i gestori e gli utilizzatori partecipano attivamente sia a livello nazionale che dell'UE. Nei casi in cui non esistano norme settoriali o non siano ancora state istituite norme internazionali, gli organismi di regolamentazione adottano norme adeguate, ove opportuno.

- **Proporzionalità** – Le strategie e le misure per la protezione devono essere commisurate al livello di rischio dal momento che non tutte le infrastrutture critiche possono essere protette da tutti i tipi di rischio (per esempio, le reti di trasmissione di elettricità sono troppo estese perché si possa recintarle o sorvegliarle). Applicando tecniche adeguate di gestione dei rischi, si può concentrare l'attenzione sui settori esposti ai rischi maggiori, tenendo conto dei pericoli, della vulnerabilità, del rapporto costi-efficacia, del livello di protezione e dell'efficacia delle strategie contenitive esistenti.

Domanda

Tali principi fondamentali sono accettabili? Ve ne sono di superflui? Vi sono altri principi di cui occorrerebbe tener conto?

Siete d'accordo sul fatto che le misure per la protezione devono essere commisurate al livello di rischio dal momento che non tutte le infrastrutture critiche possono essere protette da tutti i tipi di rischio?

5. UN QUADRO COMUNE PER L'EPCIP

Il danneggiamento o la perdita di un elemento di un'infrastruttura in uno Stato membro può avere effetti negativi su diversi altri paesi e sull'economia europea nel suo complesso. Un'eventualità di questo tipo diventa sempre più probabile dal momento che le nuove tecnologie (come Internet) e la liberalizzazione dei mercati (per esempio nel settore dell'elettricità e della fornitura di gas) fanno sì che molte infrastrutture siano parte di una rete più ampia. In una situazione di questo tipo le misure di protezione non possono essere superiori a quelle dell'elemento più debole. Ciò significa che può rendersi necessario un livello comune di protezione.

Perché la protezione sia efficace è necessario che vi siano comunicazione, coordinamento e cooperazione a livello nazionale, dell'UE (se del caso) e internazionale tra tutti gli operatori del settore. Potrebbe essere istituito un quadro comune a livello dell'UE per la protezione delle infrastrutture critiche in Europa per assicurare che ciascuno Stato membro provveda a livelli di protezione adeguati e uguali per le infrastrutture critiche e che le norme della concorrenza nel mercato interno non vengano falsate. Al fine di sostenere le attività degli Stati membri la Commissione agevolerà l'individuazione, lo scambio e la diffusione delle migliori pratiche in materia di protezione delle infrastrutture critiche creando un quadro comune per la protezione delle infrastrutture critiche. La portata di tale quadro generale deve essere esaminata.

Il quadro comune EPCIP conterrebbe misure orizzontali che definiscono la competenza e le responsabilità di tutti gli operatori del settore della protezione delle infrastrutture critiche e porrebbe le basi per approcci settoriali specifici. Il quadro comune intende integrare le misure settoriali esistenti a livello comunitario e negli Stati membri per fornire il massimo livello possibile di sicurezza delle infrastrutture critiche che si trovano nell'Unione europea. Dovrebbe essere considerato prioritario l'impegno per raggiungere un accordo su un elenco comune di definizioni e di settori di infrastrutture critiche.

Dal momento che i settori cui appartengono le infrastrutture critiche sono molto diversi, sarebbe difficile prescrivere esattamente quali criteri utilizzare per individuarle e proteggerle tutte in un quadro orizzontale; pertanto tali criteri devono essere indicati settore per settore. È tuttavia necessario che vi sia un approccio comune per alcune questioni trasversali.

Si propone, pertanto, che il potenziamento delle infrastrutture critiche nell'UE sia raggiunto mediante l'istituzione di un quadro comune EPCIP (obiettivi comuni, metodologie per quanto riguarda, ad esempio, i raffronti e le interdipendenze), lo scambio di migliori pratiche e la conformità dei meccanismi di monitoraggio. Tra gli elementi che faranno parte del quadro comune vi sono:

- i principi comuni relativi alla protezione delle infrastrutture critiche;
- i codici/norme stabiliti congiuntamente;
- le definizioni comuni sulla cui base possano essere stabilite specifiche definizioni settoriali (un elenco indicativo delle definizioni è incluso nell'allegato 1);
- un elenco comune dei settori di infrastrutture critiche (un elenco indicativo dei settori è incluso nell'allegato 2);
- i settori prioritari della protezione delle infrastrutture critiche;
- la descrizione delle responsabilità degli operatori del settore;
- punti di riferimento concordati;
- le metodologie per comparare e indicare quali siano le infrastrutture prioritarie nei diversi settori.

Tale quadro comune ridurrebbe gli eventuali effetti di distorsione sul mercato interno.

Il quadro comune dell'EPCIP potrebbe essere facoltativo o obbligatorio oppure avere un carattere misto in funzione degli aspetti considerati. Entrambi i tipi di quadro potrebbero integrare le misure settoriali e orizzontali esistenti a livello comunitario e degli Stati membri; tuttavia, solo un quadro giuridico fornirebbe una base giuridica sufficientemente solida e vincolante per permettere un'attuazione coerente e uniforme delle misure per proteggere le infrastrutture critiche dell'UE e per definire chiaramente le responsabilità rispettive degli Stati membri e della Commissione. Delle misure facoltative di natura non vincolante, certamente più flessibili, non servirebbero a chiarire i compiti di ciascuno.

Sulla base dei risultati di un'analisi approfondita e tenendo il debito conto della proporzionalità delle misure proposte, la Commissione potrebbe utilizzare un certo numero di strumenti, segnatamente legislativi, nella sua proposta di EPCIP. Se del caso, alcune misure specifiche saranno corredate da valutazioni d'impatto.

Domande

Un quadro comune sarebbe uno strumento efficace per potenziare l'EPCIP?

Qualora fosse necessario un quadro giuridico quali elementi dovrebbero farne parte?

Siete d'accordo sul fatto che occorre determinare settore per settore i criteri per individuare i diversi tipi di infrastrutture critiche dell'UE e le misure considerate necessarie?

Un quadro comune sarebbe utile per chiarire le responsabilità degli operatori del settore? In quale misura tale quadro comune dovrebbe essere obbligatorio e in quale misura facoltativo?

Quale dovrebbe essere il campo di applicazione del quadro comune? Siete d'accordo con l'elenco dei termini e delle definizioni indicativi dell'allegato I che possono servire, ove opportuno, da base per definizioni settoriali specifiche? Siete d'accordo con l'elenco dei settori indicativi delle infrastrutture critiche dell'allegato II?

6. INFRASTRUTTURE CRITICHE DELL'UE

6.1. Definizione di un'infrastruttura critica dell'UE

L'elemento determinante per la definizione di un'infrastruttura critica dell'UE sarebbe stabilire l'esistenza o meno di un effetto transfrontaliero, vale a dire stabilire se un incidente potrebbe avere o meno un impatto grave al di là delle frontiere dello Stato membro in cui è situato l'impianto. Un altro elemento di cui occorre tener conto è il fatto che i sistemi bilaterali di cooperazione tra Stati membri in materia di protezione delle infrastrutture critiche costituiscono uno strumento consolidato ed efficace per la gestione delle infrastrutture critiche che si trovano al confine tra due Stati membri. Tale cooperazione sarebbe complementare a quella prevista nell'ambito dell'EPCIP.

Le infrastrutture critiche dell'UE potrebbero consistere nelle infrastrutture materiali e di tecnologia dell'informazione, reti, servizi e beni il cui danneggiamento o distruzione avrebbero gravi ripercussioni sulla salute, la sicurezza e il benessere economico o sociale dei cittadini di

(a) due o più Stati membri – **in questo caso sarebbero incluse alcune infrastrutture critiche bilaterali (ove opportuno);**

(b) tre o più Stati membri – **in questo caso sarebbero escluse tutte le infrastrutture critiche bilaterali.**

Nell'esaminare i rispettivi vantaggi di tali due opzioni è importante ricordare quanto segue:

– il fatto che un'infrastruttura sia considerata infrastruttura critica dell'UE non significa che si rendono automaticamente necessarie misure supplementari di protezione. Le misure di protezione esistenti, che possono comprendere accordi bilaterali tra Stati membri, possono essere perfettamente adeguate e quindi rimanere immutate quando l'impianto viene classificato come infrastruttura critica dell'UE;

– l'opzione (a) può comportare che un maggior numero di impianti siano classificati come infrastrutture critiche;

– l'opzione (b) può significare che nel caso in cui un'infrastruttura interessi solo due Stati membri, la Comunità europea non svolgerebbe alcun ruolo anche se il livello di protezione fosse giudicato insufficiente da uno dei due Stati membri e se gli altri Stati membri rifiutassero di prendere delle misure. L'opzione (b) potrebbe portare a numerosi accordi bilaterali o disaccordi tra Stati membri. Le imprese, che spesso operano a un livello paneuropeo, potrebbero trovarsi a dover operare con un mosaico di accordi diversi, il che comporterebbe dei costi aggiuntivi.

Inoltre, non bisognerebbe dimenticare di prendere in considerazione le infrastrutture critiche che hanno origine o si trovano in un paese terzo, ma sono interconnesse o hanno potenzialmente un effetto diretto sugli Stati membri dell'UE.

Domanda

Devono essere considerate infrastrutture critiche dell'UE le infrastrutture che hanno potenzialmente un forte impatto transfrontaliero su due o più Stati membri o tre e più Stati membri? Perché?

6.2. Interdipendenze

Si propone che la graduale individuazione di tutte le infrastrutture critiche dell'UE tenga particolarmente conto delle interdipendenze. Lo studio delle interdipendenze potrebbe contribuire alla valutazione dell'impatto potenziale delle minacce contro specifiche infrastrutture critiche e soprattutto all'individuazione degli Stati membri che sarebbero colpiti in caso di gravi incidenti connessi alle infrastrutture critiche.

Dovrebbero essere pienamente prese in considerazione le interdipendenze all'interno e tra le imprese, i settori industriali, le giurisdizioni geografiche e le autorità degli Stati membri e segnatamente quelle create dalle tecnologie dell'informazione e delle comunicazioni. La Commissione, gli Stati membri e i proprietari/gestori delle infrastrutture critiche dovrebbero cooperare per individuare tali interdipendenze e adottare strategie adeguate per ridurre i rischi, ove possibile.

Domande

Come si può fare per tener conto delle interdipendenze?

Conoscete delle metodologie che siano adeguate per analizzare tali interdipendenze?

A che livello dovrebbe avvenire l'individuazione delle interdipendenze: a livello dell'UE o degli Stati membri?

6.3. Misure di attuazione per le infrastrutture critiche dell'UE

La Commissione proporrebbe le seguenti misure di attuazione per le infrastrutture critiche dell'UE:

(1) La Commissione e gli Stati membri definiscono criteri specifici da utilizzare per individuare le infrastrutture critiche dell'UE sulla base dei settori specifici;

(2) La Commissione e gli Stati membri individuano e verificano le infrastrutture critiche dell'UE sulla base degli specifici settori. La decisione di classificare determinate infrastrutture critiche come infrastrutture critiche dell'UE viene presa a livello europeo[1] in considerazione della natura transfrontaliera dell'infrastruttura in questione;

(3) Gli Stati membri e la Commissione esaminano sulla base dei settori le lacune esistenti in materia di sicurezza per quanto riguarda le infrastrutture critiche dell'UE;

(4) Gli Stati membri e la Commissione si accordano su quali siano i settori/ le infrastrutture prioritarie per i quali s'impone un'azione, tenendo conto delle interdipendenze;

(5) Ove opportuno, per ciascun settore, i responsabili in materia della Commissione e degli Stati membri concordano delle proposte per misure minime di protezione come norme;

(6) Dopo l'adozione delle proposte del Consiglio, tali misure vengono attuate;

(7) La Commissione e gli Stati membri assicurano un regolare monitoraggio. Ove e quando opportuno, vengono effettuate modifiche per quanto riguarda le misure e l'individuazione delle infrastrutture critiche dell'UE.

Domande

Ritenete accettabile l'elenco delle misure di attuazione per le infrastrutture critiche dell'UE?

In che modo, secondo voi, dovrebbero procedere la Commissione e gli Stati membri per una classificazione comune delle infrastrutture critiche dell'UE dal momento che gli Stati membri dispongono delle competenze necessarie e che la Commissione ha il quadro d'insieme dell'interesse europeo? Dovrebbe trattarsi di una decisione giuridica?

È necessario un meccanismo arbitrale se un singolo Stato membro non è d'accordo sulla classificazione di un'infrastruttura che appartiene alla sua giurisdizione come infrastruttura critica dell'UE?

Occorre fare una verifica delle classificazioni? Chi deve esserne responsabile?

Gli Stati membri dovrebbero avere la possibilità di classificare come infrastrutture critiche per loro delle infrastrutture di altri Stati membri o di paesi terzi? Cosa occorrerebbe fare nei casi in cui uno Stato membro, un paese terzo o un'impresa ritenga che una determinata infrastruttura di uno Stato membro sia per quanto lo riguarda un'infrastruttura critica?

[1] Ad eccezione delle infrastrutture della difesa.

Cosa occorrerebbe fare qualora tale Stato membro non la considerasse come tale? È necessario prevedere un meccanismo di ricorso? In caso affermativo, quale?

Dovrebbe essere data agli operatori la possibilità di presentare un ricorso qualora non siano d'accordo con la classificazione o la mancata classificazione come infrastruttura critica dell'UE? In caso affermativo, in quale sede?

Quali metodologie dovrebbero essere sviluppate per stabilire quali siano i settori e le infrastrutture prioritari per i quali s'impone un'azione? Esistono già metodologie adeguate che possono essere adattate a livello europeo?

In che modo la Commissione può essere coinvolta nell'analisi delle lacune in materia di sicurezza per quanto riguarda le infrastrutture critiche dell'UE?

7. INFRASTRUTTURE CRITICHE NAZIONALI

7.1. Il ruolo delle infrastrutture critiche nazionali nell'EPCIP

Molte imprese europee operano al di là delle frontiere e pertanto sono soggette a obblighi diversi per quanto riguarda le infrastrutture critiche nazionali. Si propone quindi, nell'interesse degli Stati membri e dell'UE nel suo complesso, che ogni Stato membro protegga le proprie infrastrutture critiche nazionali sulla base di un quadro comune in modo che i proprietari e gli operatori di tutta l'Europa si avvantaggino del fatto di non doversi rifare a un mosaico di quadri normativi che comporterebbe il ricorso a innumerevoli metodologie e costi aggiuntivi. Pertanto, la Commissione ritiene che l'EPCIP – pur concentrandosi principalmente sulle infrastrutture critiche dell'UE – non possa trascurare completamente le infrastrutture critiche nazionali. Si delineano tre possibili opzioni:

a) Le infrastrutture critiche nazionali vengono integrate pienamente nell'EPCIP

b) Le infrastrutture critiche nazionali sono fuori dal campo di applicazione dell'EPCIP

c) Gli Stati membri possono utilizzare, quando lo desiderano, alcune parti dell'EPCIP in relazione alle infrastrutture critiche nazionali ma non sono obbligati a farlo.

Domande

Una protezione efficace delle infrastrutture critiche dell'UE sembra richiedere che vengano individuate le infrastrutture critiche dell'UE e le infrastrutture critiche nazionali. Siete d'accordo sul fatto che, pur essendo incentrato sulle infrastrutture critiche dell'UE, l'EPCIP non debba trascurare completamente le infrastrutture critiche nazionali?

Quale delle tre opzioni ritenete più adeguata per l'EPCIP?

7.2. Programmi nazionali per la protezione delle infrastrutture critiche

Sulla base di un quadro comune dell'EPCIP gli Stati membri potrebbero elaborare programmi nazionali di protezione delle infrastrutture critiche per le proprie infrastrutture critiche

nazionali. Gli Stati membri potrebbero applicare misure più severe di quelle previste nell'ambito dell'EPCIP

Domanda

È auspicabile che ciascuno Stato membro adotti un programma nazionale per la protezione delle infrastrutture critiche basato sull'EPCIP?

7.3. Un organismo unico di sorveglianza

Ai fini dell'efficacia e della coerenza è necessario che ogni Stato membro designi un organismo di sorveglianza unico che si occupi dell'attuazione globale dell'EPCIP. Si possono prevedere due possibilità:

(a) un organismo di sorveglianza unico per la protezione delle infrastrutture critiche;

(b) un punto di contatto nazionale, senza poteri, che lasci che lo Stato membro si organizzi autonomamente.

Tale organismo potrebbe coordinare, monitorare e sorvegliare l'attuazione dell'EPCIP nella propria giurisdizione e servire da principale punto di contatto istituzionale in materia di protezione delle infrastrutture critiche con la Commissione, gli altri Stati membri e i proprietari e gestori delle infrastrutture critiche. L'organismo formerebbe la base della rappresentanza nazionale nei gruppi di esperti in materia di protezione delle infrastrutture critiche e potrebbe essere collegato alla rete informativa di allarme sulle infrastrutture critiche (CIWIN). L'organismo di coordinamento nazionale per la protezione delle infrastrutture critiche potrebbe coordinare le azioni nazionali in materia di protezione delle infrastrutture critiche senza pregiudizio delle azioni eventualmente già intraprese nel settore da altri organismi o enti del suo paese.

La graduale individuazione delle infrastrutture critiche nazionali potrebbe essere realizzata obbligando i proprietari e i gestori a comunicare all'organismo di coordinamento nazionale tutte le attività economiche che abbiano una connessione con la protezione delle infrastrutture critiche.

L'organismo di coordinamento nazionale sarebbe responsabile della decisione giuridica con la quale un'infrastruttura sotto la sua giurisdizione viene classificata come infrastruttura critica nazionale. Tale informazione sarebbe destinata solamente allo Stato membro interessato.

Le competenze specifiche dell'organismo potrebbero comprendere le seguenti attività:

a) coordinare, monitorare e sorvegliare l'attuazione globale dell'EPCIP in uno Stato membro;

b) svolgere il ruolo di principale punto di contatto istituzionale in materia di protezione delle infrastrutture critiche con:

   i. la Commissione

   ii. gli altri Stati membri

   iii. i proprietari e i gestori di infrastrutture critiche;

c) partecipare alla classificazione delle infrastrutture critiche dell'UE;

d) prendere la decisione giuridica di classificare un'infrastruttura che appartiene alla sua giurisdizione come un'infrastruttura critica nazionale;

e) servire da autorità cui i proprietari/gestori che non sono d'accordo sul fatto che la loro infrastruttura sia classificata come "infrastruttura critica" possono presentare legalmente ricorso;

f) partecipare all'elaborazione del programma nazionale di protezione delle infrastrutture critiche e di specifici programmi settoriali per la protezione delle infrastrutture critiche;

g) individuare le interdipendenze tra specifici settori di infrastrutture critiche;

h) contribuire ad approcci settoriali alla protezione delle infrastrutture critiche mediante la partecipazione a gruppi di esperti. I rappresentanti dei proprietari e dei gestori potrebbero essere invitati a contribuire al dibattito. Dovrebbero svolgersi regolari riunioni;

i) sorvegliare il processo dell'elaborazione dei piani di emergenza per le infrastrutture critiche.

Domande

Siete d'accordo sul fatto che gli Stati membri siano gli unici responsabili della classificazione e della gestione delle infrastrutture critiche nazionali nell'ambito di un quadro comune dell'EPCIP?

È auspicabile designare un organismo di coordinamento per la protezione delle infrastrutture critiche in ogni Stato membro che abbia la responsabilità del coordinamento globale per le misure connesse alla protezione delle infrastrutture critiche ma che rispetti le responsabilità settoriali esistenti (autorità dell'aviazione civile, direttiva Seveso, etc.)?

Le competenze che proponiamo di attribuire a tale organismo vi sembrano appropriate? Ce ne sono altre che è necessario aggiungere?

7.4. Misure di attuazione per le infrastrutture critiche nazionali

La Commissione proporrebbe le seguenti misure di attuazione per le infrastrutture critiche nazionali:

(1) Gli Stati membri elaborano, sulla base dell'EPCIP, i criteri specifici da utilizzare per individuare le infrastrutture critiche nazionali;

(2) Gli Stati membri individuano e verificano le infrastrutture critiche nazionali sulla base degli specifici settori;

(3) Gli Stati membri esaminano, sulla base dei settori, le lacune esistenti in materia di sicurezza per quanto riguarda le infrastrutture critiche nazionali;

(4) Gli Stati membri stabiliscono quali siano i settori prioritari di azione, tenendo conto, se del caso, delle interdipendenze;

(5) Gli Stati membri fissano, ove opportuno, misure minime di protezione per ciascun settore;

(6) Gli Stati membri hanno la responsabilità di garantire che i proprietari/gestori sotto la loro giurisdizione applichino le necessarie misure di attuazione;

(7) Gli Stati membri assicurano un regolare monitoraggio. Ove e quando opportuno, vengono effettuate modifiche per quanto riguarda le misure e l'individuazione delle infrastrutture critiche.

Domanda

Ritenete accettabile l'elenco delle misure di attuazione per le infrastrutture critiche nazionali? Ve ne sono di superflue? Occorre aggiungerne di altre?

8. RUOLO DEI PROPRIETARI, DEI GESTORI E DEGLI UTILIZZATORI DELLE INFRASTRUTTURE CRITICHE

8.1. Responsabilità dei proprietari, dei gestori e degli utilizzatori delle infrastrutture critiche

Il fatto che un'infrastruttura venga classificata come infrastruttura critica impone ai proprietari e ai gestori alcune responsabilità. Ai proprietari e ai gestori delle infrastrutture classificate come infrastrutture critiche nazionali o dell'UE potrebbero essere attribuite le seguenti quattro responsabilità:

(1) **comunicare all'organismo competente in materia di protezione delle infrastrutture critiche dello Stato membro il fatto che una determinata infrastruttura potrebbe essere considerata critica;**

(2) **designare uno o più rappresentanti di alto livello che agisca come funzionario di collegamento in materia di sicurezza tra il proprietario/gestore e l'autorità competente in materia di protezione delle infrastrutture critiche dello Stato membro.** Il funzionario di collegamento dovrebbe partecipare all'elaborazione dei piani di sicurezza e di emergenza. Il funzionario di collegamento sarebbe il principale funzionario di collegamento con il competente organismo settoriale per la protezione delle infrastrutture critiche nello Stato membro e, se del caso, con le autorità di contrasto;

(3) **Istituire, attuare ed aggiornare un piano di sicurezza per gli operatori (OSP).** Un modello di OSP viene presentato nell'allegato 3.

(4) **Partecipare all'elaborazione di un piano d'emergenza** relativo alle infrastrutture critiche, ove opportuno, con le autorità competenti degli Stati membri (autorità di contrasto e autorità di protezione civile).

L'OSP potrebbe essere presentato per essere approvato all'autorità settoriale competente in materia di protezione delle infrastrutture critiche dello Stato membro con la supervisione

generale dell'organismo di coordinamento nazionale, sia che si tratti di infrastrutture critiche nazionali che di infrastrutture critiche dell'UE. Ciò garantirebbe la coerenza delle misure di sicurezza prese da specifici proprietari/gestori e i settori interessati in generale. Da parte sua, l'organismo nazionale di coordinamento, ed eventualmente la Commissione, potrebbe fornire ai proprietari e gestori informazioni utili e un sostegno per far fronte alle minacce cui sono esposti, per elaborare le migliori pratiche e aiutarli, se del caso, a valutare le interdipendenze e la vulnerabilità.

Ogni Stato membro può stabilire una scadenza per l'elaborazione dell'OSP da parte dei proprietari e gestori delle infrastrutture critiche nazionali e delle infrastrutture critiche dell'UE (nel caso delle infrastrutture critiche dell'UE anche la Commissione può essere coinvolta) e può stabilire delle sanzioni amministrative qualora tali scadenze non siano rispettate.

Si propone che l'OSP identifichi le strutture delle infrastrutture critiche dei proprietari e gestori e suggerisca soluzioni in materia di sicurezza per la loro protezione. L'OSP deve descrivere i metodi e le procedure da seguire per garantire la conformità con l'EPCIP, i programmi nazionali e settoriali di protezione delle infrastrutture critiche. L'OSP potrebbe rappresentare uno strumento per un approccio dal basso a una regolamentazione della protezione delle infrastrutture critiche che dia maggiore libertà d'azione (e anche maggiori responsabilità) al settore privato.

In alcuni casi, quando si tratta di determinate infrastrutture come le reti di elettricità o di informazione, sarebbe poco realistico (da un punto di vista pratico e finanziario) aspettarsi che i proprietari e gestori prevedano livelli di sicurezza uguali per tutte le loro proprietà. In tali casi, si propone che i proprietari e gestori individuino, di concerto con le autorità competenti in materia, i punti critici (nodi) di una rete materiale o di informazione su cui potrebbero concentrarsi le misure di protezione della sicurezza.

Le misure di sicurezza dell'OSP potrebbero essere suddivise come segue:

- **le misure permanenti di sicurezza**, che individuerebbero gli investimenti e gli strumenti necessari in materia di sicurezza che i proprietari e gestori non possono realizzare a breve termine. I proprietari e gestori manterrebbero una vigilanza permanente contro le minacce potenziali che non disturberebbe le normali attività economiche, amministrative e sociali.

- **le misure graduali di sicurezza** che potrebbero essere attivate in funzione dei diversi livelli di minaccia. Pertanto gli OSP dovrebbero prevedere diversi regimi di sicurezza adeguati ai possibili livelli di minacce esistenti negli Stati membri in cui hanno sede le infrastrutture.

Si propone che la mancata adesione da parte dei proprietari e gestori di infrastrutture critiche all'obbligo di elaborare un OSP, di contribuire all'elaborazione di piani d'emergenza e di designare un funzionario di collegamento, possa comportare il pagamento di sanzioni finanziarie.

Domande

Le eventuali responsabilità dei proprietari e gestori di una infrastruttura critica sono accettabili nell'ottica del miglioramento della sicurezza di un'infrastruttura critica? Quale potrebbe esserne il costo?

Ritenete che i proprietari e gestori debbano essere obbligati a comunicare che la loro infrastruttura potrebbe essere critica? Ritenete utile il concetto di OSP? Perché?

Gli obblighi proposti sono proporzionati ai costi che comportano?

Quali diritti potrebbero essere attribuiti dalle autorità della Commissione e dagli Stati membri ai proprietari e gestori di infrastrutture critiche?

8.2. Dialogo con i proprietari, i gestori e gli utilizzatori

L'EPCIP potrebbe incoraggiare i proprietari e gestori a costituire dei partenariati. Il successo di un programma di protezione dipende dalla cooperazione e dal livello di coinvolgimento che può essere raggiunto dai proprietari e gestori. Negli Stati membri i proprietari e gestori di infrastrutture critiche potrebbero partecipare allo sviluppo della protezione delle infrastrutture critiche mediante regolari contatti con gli organismi nazionali di coordinamento.

A livello dell'UE potrebbero essere creati dei forum al fine di agevolare gli scambi di pareri su punti generali e specifici della protezione delle infrastrutture critiche. L'adozione di un approccio comune per quanto riguarda la partecipazione del settore privato alla protezione delle infrastrutture critiche, finalizzato a riunire tutti gli operatori del settore - pubblici e privati- permetterebbe agli Stati membri, alla Commissione e alle imprese di discutere insieme tutti i nuovi problemi che si pongono in materia di protezione delle infrastrutture critiche. I proprietari, gestori e utilizzatori delle infrastrutture critiche potrebbero contribuire all'elaborazione di orientamenti, norme sulle migliori pratiche e, ove opportuno, allo scambio di informazioni. Un dialogo di questo tipo contribuirebbe a delineare le versioni future dell'EPCIP.

Se del caso, la Commissione potrebbe incoraggiare la costituzione di associazioni professionali e di imprese dell'UE in materia di protezione delle infrastrutture critiche. I due obiettivi finali sarebbero di garantire che le imprese europee restino competitive e che la sicurezza dei cittadini dell'UE sia rafforzata.

Domande

In che modo dovrebbe essere strutturato il dialogo con i proprietari, i gestori e gli utilizzatori delle infrastrutture critiche?

Chi dovrebbe rappresentare i proprietari, i gestori e gli utilizzatori nel dialogo tra settore pubblico e privato?

9. MISURE A SOSTEGNO DELL'EPCIP

9.1. La rete informativa di allarme sulle infrastrutture critiche (CIWIN)

La Commissione ha elaborato una serie di sistemi di allarme rapido che permettono di reagire in maniera concreta, coordinata ed efficace in caso di emergenze, comprese quelle di origine terroristica. Il 20 ottobre 2004 la Commissione ha annunciato la costituzione di una rete centrale all'interno della Commissione che assicura un rapido flusso di informazioni tra tutti i sistemi di allarme rapido della Commissione e i servizi interessati (ARGUS).

La Commissione propone di istituire la CIWIN per incoraggiare l'elaborazione di misure adeguate di protezione. Tale rete agevolerebbe lo scambio di migliori pratiche in condizioni di sicurezza e costituirebbe uno strumento per la trasmissione delle informazioni relative a minacce immediate ed allarmi. Il sistema dovrebbe garantire che le persone giuste ricevano le informazioni giuste al momento giusto.

Per lo sviluppo della CIWIN sono possibili le tre seguenti opzioni:

(1) **CIWIN intesa come uno spazio di discussione limitato allo scambio di idee e di migliori pratiche in materia di protezione delle infrastrutture critiche** e destinata ad assistere i proprietari e i gestori delle infrastrutture. Tale forum potrebbe assumere la forma di una rete di esperti e di una piattaforma elettronica per lo scambio delle informazioni pertinenti in un ambiente sicuro. La Commissione svolgerebbe un importante ruolo nella raccolta e divulgazione delle informazioni. Tale opzione non permetterebbe di trasmettere i necessari allarmi rapidi concernenti minacce immediate ma la portata della CIWIN potrebbe essere estesa successivamente.

(2) **CIWIN intesa come un sistema di allarme rapido che collega gli Stati membri con la Commissione** Tale opzione migliorerebbe la sicurezza delle infrastrutture critiche segnalando gli allarmi relativi a minacce immediate. In questo caso, l'obiettivo sarebbe di agevolare un rapido scambio di informazioni sulle minacce potenziali per i proprietari e gestori delle infrastrutture critiche. Il sistema di allarme rapido non prevederebbe lo scambio di informazioni a lungo termine, ma potrebbe essere utilizzato per lo scambio rapido di informazioni sulle minacce imminenti a una determinata infrastruttura.

(3) CIWIN **intesa come un sistema di allarme e comunicazione a più livelli con due funzioni distinte:** a) un sistema di allarme rapido che colleghi gli Stati membri alla Commissione e b) un forum per lo scambio di idee in materia di protezione delle infrastrutture critiche e di migliori pratiche a sostegno dei proprietari e gestori di infrastrutture critiche, formato da una rete di esperti e da una piattaforma per lo scambio di dati elettronici.

Indipendentemente dall'opzione scelta, CIWIN integrerebbe le reti esistenti e occorrerebbe fare attenzione ad evitare sovrapposizioni. A lungo termine CIWIN sarebbe collegata a tutti i proprietari e gestori di infrastrutture critiche in tutti gli Stati membri per esempio mediante l'organismo di coordinamento nazionale. Gli allarmi e le migliori pratiche potrebbero essere diffusi da tale organismo che sarebbe l'unico servizio connesso direttamente alla Commissione e, di conseguenza, a tutti gli altri Stati membri. Gli Stati membri potrebbero utilizzare i loro sistemi di informazione già esistenti per creare un'unità nazionale della CIWIN che colleghi le autorità ai proprietari e gestori. La cosa più importante è che le reti

nazionali potrebbero essere utilizzate come un sistema di comunicazione a doppio senso di circolazione dagli organismi competenti degli Stati membri in materia di protezione delle infrastrutture critiche e dai proprietari e gestori.

Sarà promosso uno studio per definire la portata e le specifiche tecniche necessarie per il futuro interfaccia di CIWIN con gli Stati membri.

Domande

Quale forma dovrebbe assumere la rete CIWIN per sostenere gli obiettivi dell'EPCIP?

I proprietari e gestori delle infrastrutture critiche dovrebbero essere collegati alla rete CIWIN?

9.2. Metodologie comuni

I diversi Stati membri dispongono di diversi livelli di allarme in funzione delle diverse situazioni. Al momento attuale non c'è modo di sapere se, per esempio, un livello "alto" in uno Stato membro corrisponde al livello "alto" di un altro. Ciò può rendere difficile alle imprese transnazionali stabilire le priorità per quanto riguarda le loro spese per le misure di protezione. Sarebbe utile, pertanto, cercare di armonizzare o calibrare i livelli diversi.

Per ciascun livello di minaccia potrebbe esservi un livello di preparazione che permetta l'adozione di misure comuni generali di sicurezza e, ove opportuno, l'utilizzazione di misure graduali di sicurezza. Gli Stati membri che non intendono adottare una determinata misura potrebbero far fronte a una specifica minaccia con misure alternative di sicurezza.

Potrebbe essere prevista una metodologia comune per individuare e classificare le minacce, le capacità, i rischi e le vulnerabilità e per trarre conclusioni sulla possibilità, le probabilità e il grado di gravità di una minaccia in termini di danneggiamento dell'impianto di un'infrastruttura. Ciò comprenderebbe una valutazione dei rischi e una loro classificazione in ordine di priorità che permetterebbe di definire gli avvenimenti a rischio in termini di probabilità, di impatto e di rapporti con altri settori o processi a rischio.

Domande

In che misura è auspicabile e possibile armonizzare o calibrare i diversi livelli di allarme?

Potrebbe essere prevista una metodologia comune per individuare e classificare le minacce, le capacità, i rischi e le vulnerabilità e per trarre conclusioni sulla possibilità, la probabilità e il livello di gravità di una minaccia?

9.3. Finanziamento

A seguito di un'iniziativa del Parlamento europeo (iscrizione di una nuova linea di bilancio – il progetto pilota "Lotta contro il terrorismo" – nell'esercizio del 2005), il 15 settembre la Commissione ha deciso di stanziare 7 milioni di euro per finanziare una serie di azioni per incrementare la prevenzione, la preparazione e la risposta europea agli attentati terroristici, tra cui rientrano la gestione delle conseguenze e la protezione delle infrastrutture critiche, nonché azioni nel settore del finanziamento del terrorismo, degli esplosivi e della radicalizzazione violenta. Più dei due terzi di tale bilancio sono destinati alla preparazione del futuro programma europeo per la protezione delle infrastrutture critiche, all'integrazione e allo

sviluppo delle capacità richieste per la gestione delle crisi di natura transnazionale determinate da eventuali attentati terroristici e alle misure di emergenza che possono rendersi necessarie per far fronte a una grave minaccia o al verificarsi di un attentato. Si prevede che tale finanziamento continui ad esserci nel 2006.

Dal 2007 al 2013 tale finanziamento passerà al programma quadro relativo alla sicurezza e alla tutela delle libertà in cui rientra un programma specifico relativo alla prevenzione, preparazione e gestione delle conseguenze del terrorismo; la proposta della Commissione ha assegnato un importo di 137,4 milioni di euro al fine di individuare le esigenze in materia e di elaborare norme tecniche comuni per la protezione delle infrastrutture critiche.

Il programma offrirà un finanziamento comunitario ai progetti presentati dalle autorità nazionali, regionali e locali per la protezione delle infrastrutture critiche. Il programma è incentrato sull'individuazione delle esigenze di protezione e sulla fornitura di informazioni al fine di elaborare norme comuni e valutare i rischi e le minacce per proteggere le infrastrutture critiche o elaborare piani di emergenza specifici. La Commissione si servirà delle competenze di cui dispone oppure potrebbe contribuire a finanziare studi sulle interdipendenze in specifici settori. Spetta quindi principalmente agli Stati membri o ai proprietari e gestori migliorare la sicurezza delle loro infrastrutture in funzione delle esigenze individuate. Il programma non finanzia il miglioramento della protezione delle infrastrutture critiche. Possono essere utilizzati prestiti di istituzioni finanziarie per migliorare la sicurezza delle infrastrutture negli Stati membri sulla base delle necessità individuate mediante il programma e per attuare norme comuni. La Commissione sarebbe favorevole a sovvenzionare studi settoriali per valutare l'impatto finanziario che un miglioramento della sicurezza di un'infrastruttura può avere sulle imprese.

La Commissione sta finanziando dei progetti di ricerca a sostegno della protezione delle infrastrutture critiche nell'ambito dell'azione preparatoria per la ricerca in materia di sicurezza[2] (2004-2006) e ha previsto attività più sostanziali nel settore delle ricerche in materia di sicurezza nella proposta di decisione di decisione del Consiglio concernente il Settimo programma quadro della CE (COM(2005)119 def.)[3] e la proposta di decisione del Consiglio concernente il programma specifico "Cooperazione" recante attuazione del Settimo programma quadro (COM(2005)440 def.). Le ricerche mirate, finalizzate a fornire strategie pratiche o strumenti per ridurre i rischi, hanno un'importanza capitale per il miglioramento della sicurezza delle infrastrutture critiche dell'UE a medio e lungo termine. Tutte le ricerche in materia di sicurezza, comprese quelle in questo settore, saranno vagliate dal punto di vista etico per garantirne la compatibilità con la Carta dei diritti fondamentali. La richiesta di ricerche aumenterà solo se aumenterà il numero delle interdipendenze tra le infrastrutture.

Domande

Quali sarebbero, secondo voi, il costo e l'impatto dell'attuazione delle misure presentate nel presente libro verde per le amministrazioni e le imprese? Ritenete che sia proporzionato?

---

2 L'importo totale dei crediti nei bilanci del 2004 e del 2005 ammontava a 30 milioni di euro. Per il 2006 la Commissione ha proposto l'importo di 24 milioni di euro che è attualmente all'esame dell'autorità di bilancio.

3 La proposta di bilancio della Commissione per la sicurezza e le attività di ricerca spaziali nell'ambito del VII programma quadro di ricerca e sviluppo ammonta a 570 milioni di euro (COM(2005)119 def.).

9.4. Valutazione e controllo

Per garantire la valutazione e il controllo dell'attuazione dell'EPCIP, occorrerebbe prevedere un procedimento a più livelli con la partecipazione di tutti gli operatori del settore:

- **a livello dell'UE potrebbe essere istituito un meccanismo di valutazione "tra pari",** in cui gli Stati membri e la Commissione possano procedere insieme a valutare il livello globale di attuazione dell'EPCIP in ciascuno Stato membro. La Commissione potrebbe preparare delle relazioni di attività annuali sull'attuazione dell'EPCIP.

- **ogni anno la Commissione potrebbe informare gli Stati membri e le altre istituzioni dei progressi compiuti** in un documento di lavoro della Commissione.

- **a livello degli Stati membri, l'organismo di coordinamento nazionale per la protezione delle infrastrutture critiche di ciascuno Stato membro potrebbe verificare l'attuazione globale dell'EPCIP sul territorio nell'ambito della sua giurisdizione e assicurare la conformità con il programma/i programmi nazionali di protezione delle infrastrutture critiche e i programmi settoriali di protezione delle infrastrutture critiche,** al fine di garantire la loro effettiva attuazione mediante relazioni annuali al Consiglio e alla Commissione.

L'attuazione dell'EPCIP sarebbe un processo dinamico, in continua evoluzione e da valutare continuativamente per stare al passo con un mondo in continuo mutamento e per trarre utili insegnamenti dall'esperienza acquisita. Le valutazioni tra pari e le relazioni di controllo degli Stati membri potrebbero costituire una parte degli strumenti utilizzati per rivedere l'EPCIP e per proporre nuove misure al fine di rafforzare la protezione delle infrastrutture critiche.

Gli Stati membri potrebbero mettere a disposizione della Commissione le informazioni in materia di protezione delle infrastrutture critiche per elaborare valutazioni comuni in materia di vulnerabilità, piani sulla gestione delle conseguenze, norme comuni per la protezione delle infrastrutture critiche e per stabilire le priorità per quanto riguarda le attività di ricerca, eventualmente al fine di una regolamentazione ed armonizzazione. Tali informazioni saranno classificate e ne sarà garantita la riservatezza.

La Commissione potrebbe monitorare le diverse iniziative degli Stati membri, comprese quelle che prevedono sanzioni finanziarie per i proprietari e gestori che non riescono a ripristinare i servizi essenziali per i cittadini entro i termini stabiliti.

Domande

Quale tipo di meccanismo di valutazione sarebbe necessario per l'EPCIP? Ritenete che i meccanismi sopraindicati siano sufficienti?

Le risposte devono essere inviate per posta elettronica entro il 15 gennaio 2006 al seguente indirizzo e-mail: **JLS-EPCIP@cec.eu.int**. Le risposte saranno considerate riservate a meno che gli interpellati non dichiarino esplicitamente la loro volontà di renderle pubbliche. In quest'ultimo caso le risposte saranno pubblicate sul sito Internet della Commissione.

ALLEGATI

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.