COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 20.10.2004
COM(2004) 702 definitivo

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO

La protezione delle infrastrutture critiche nella lotta contro il terrorismo

INDICE

1. INTRODUZIONE

Il Consiglio europeo del giugno 2004 ha chiesto alla Commissione e all'Alto Rappresentante di preparare una strategia globale per la protezione delle infrastrutture critiche.

La presente comunicazione fornisce una panoramica delle iniziative che la Commissione sta adottando per la protezione delle infrastrutture critiche e propone alcune misure supplementari per potenziare gli strumenti esistenti e soddisfare la richiesta formulata dal Consiglio europeo.

2. I PERICOLI

Il rischio che si verifichino attentati terroristici catastrofici ai danni delle infrastrutture critiche è in continuo aumento. Le conseguenze di un attentato ai sistemi di controllo industriali delle infrastrutture critiche possono essere le più varie. Si ritiene comunemente che un attentato di tipo informatico riuscito causerebbe poche o nessuna vittima ma potrebbe determinare gravi danni a infrastrutture vitali. Per esempio, un attentato informatico riuscito alla rete telefonica pubblica priverebbe gli utenti di tale servizio per tutto il tempo necessario alla riparazione della rete. Un attentato ai sistemi di controllo di impianti chimici o di gas naturale liquido può comportare un numero maggiore di vittime e gravi danni materiali.

Altri danni dalle conseguenze catastrofiche per le infrastrutture critiche possono verificarsi quando l'interruzione del funzionamento di una parte di un'infrastruttura è causa di interruzioni del funzionamento di altre parti con un effetto a catena. Un problema di questo tipo può verificarsi a causa delle sinergie esistenti tra le diverse industrie. Per esempio, nel caso di un attentato a una centrale elettrica, l'interruzione del servizio di fornitura elettrica può portare al blocco delle turbine e di altri apparati elettrici e quindi all'interruzione del funzionamento degli impianti per il trattamento delle acque reflue e del sistema idrico.

A loro volta, le reazioni a catena possono generare molti danni a causa dell'interruzione di una vasta gamma di servizi. I blackout nell'America del Nord e in Europa degli ultimi due anni hanno messo a nudo la vulnerabilità delle infrastrutture energetiche e, di conseguenza, la necessità di individuare misure efficaci per prevenire o mitigare le gravi conseguenze derivate da un'interruzione della fornitura. Il ricorso ad atti di ciberterrorismo può anch'esso determinare un'amplificazione delle conseguenze materiali degli attentati. Un esempio potrebbe essere la combinazione di un normale bombardamento ad un edificio con una temporanea interruzione dei servizi di fornitura elettrica o telefonica. Le difficoltà che ne deriverebbero per i servizi di soccorso, fino al ripristino dei sistemi di elettricità e delle comunicazioni, potrebbero determinare un incremento del numero di vittime e seminare il panico tra i cittadini.

3. LE INFRASTRUTTURE CRITICHE EUROPEE

3.1. Che cos'è un'infrastruttura critica

Le infrastrutture critiche consistono in infrastrutture materiali e di tecnologia dell'informazione, reti, servizi e beni il cui danneggiamento o distruzione avrebbe gravi ripercussioni sulla salute, la sicurezza e il benessere dei cittadini oppure sul valido funzionamento delle amministrazioni pubbliche degli Stati membri. Le infrastrutture critiche

sono presenti in molti settori dell'economia, compreso quello delle banche e della finanza, dei trasporti e della distribuzione, dell'energia, dei servizi, della sanità, dell'approvvigionamento alimentare e delle comunicazioni nonché nei servizi pubblici fondamentali. Per alcuni di questi elementi critici non si può parlare in senso stretto di 'infrastruttura', ma si tratta comunque di reti o catene di distribuzione che forniscono un prodotto o un servizio di importanza capitale. Per esempio, l'approvvigionamento alimentare o idrico nelle principali aree urbane dipende da alcune strutture chiave ma anche da una complessa rete di produttori, trasformatori, distributori e venditori al dettaglio.

Le infrastrutture critiche sono:

- impianti e reti energetiche (per esempio, centrali elettriche, impianti di produzione di gas e petrolio, depositi e raffinerie, sistemi di trasmissione e di distribuzione)

- sistemi di comunicazione e di tecnologia dell'informazione (per esempio, le telecomunicazioni, i servizi radiotelevisivi, il software, l'hardware e le reti tra cui Internet)

- la finanza (per esempio, banche, strumenti finanziari e investimenti)

- il sistema sanitario (per esempio, gli ospedali, i servizi sanitari e di raccolta del sangue, i laboratori, il settore dei prodotti farmaceutici e i servizi di raccolta e salvataggio e di emergenza)

- l'approvvigionamento alimentare (per esempio, l'industria alimentare, i sistemi di sicurezza igienica, la produzione e la distribuzione all'ingrosso)

- l'approvvigionamento idrico (per esempio, i bacini, l'immagazzinamento, il trattamento, gli acquedotti)

- i trasporti (per esempio, i servizi portuali, aeroportuali e intermodali, i sistemi di trasporto collettivo su rotaia, i sistemi di controllo del traffico)

- la produzione, l'immagazzinamento e il trasporto di sostanze pericolose (per esempio, materiali chimici, biologici, radiologici e nucleari)

- l'amministrazione (per esempio, servizi cruciali, strutture, reti di informazione, beni e patrimonio architettonico e naturale).

Tali infrastrutture appartengono o vengono fatte funzionare sia dal settore pubblico che da quello privato. La Commissione, tuttavia, nella comunicazione 574/2001 del 10 ottobre 2001 ha dichiarato: "le pubbliche autorità devono assumersi l'onere delle ulteriori misure di sicurezza che intendono imporre, in quanto adottate in risposta ad un attacco che va considerato diretto contro la società nel suo complesso e non contro il solo settore dell'industria". Il settore pubblico ha, pertanto, un ruolo fondamentale da svolgere.

Le infrastrutture critiche devono essere individuate sia a livello dei singoli Stati membri che a livello europeo e devono esserne stilati degli elenchi entro la fine del 2005.

Le infrastrutture critiche europee sono altamente interconnesse e interdipendenti. È una situazione a cui hanno contribuito le concentrazioni tra imprese, la razionalizzazione dell'industria, pratiche commerciali efficaci come la fabbricazione just-in-time e la

concentrazione della popolazione nelle aree urbane. Le infrastrutture critiche europee sono diventate maggiormente dipendenti dalle comuni tecnologie dell'informazione come Internet, la radionavigazione spaziale e la comunicazione. Possono verificarsi problemi attraverso tali infrastrutture interdipendenti che a loro volta possono essere causa di gravi interruzioni della fornitura di servizi essenziali. L'interconnessione e l'interdipendenza rendono tali infrastrutture più vulnerabili al rischio di danneggiamento o distruzione.

È opportuno esaminare in base a quali criteri un'infrastruttura o un elemento di un'infrastruttura può essere considerato critico. Tali criteri dovrebbero essere scelti anche sulla base delle competenze settoriali e collettive. Si potrebbero suggerire tre fattori per l'individuazione di un'infrastruttura potenzialmente critica:

- l'estensione – il danneggiamento di un elemento critico di un'infrastruttura è valutato in funzione dell'estensione della regione geografica che può subirne le conseguenze: internazionale, nazionale, provinciale/territoriale o locale.

- la portata - il livello dell'impatto o del danno può essere valutato come inesistente, minimo, moderato o grande. Tra i criteri che si possono utilizzare per valutare la portata potenziale del danno vi sono i seguenti:

    (a) impatto pubblico (numero dei cittadini colpiti, decessi, malattie, ferite gravi, evacuazione);

    (b) impatto economico (effetto sul PIL, portata della perdita economica, deterioramento di prodotti o servizi);

    (c) impatto ambientale (impatto sui cittadini e l'ambiente circostante);

    (d) interdipendenza (con altri elementi critici di infrastruttura):

    (e) impatto politico (fiducia nelle capacità del governo);

- conseguenze nel tempo: tale criterio serve ad individuare il periodo di tempo in cui il danneggiamento di un elemento può portare gravi conseguenze (per esempio, subito, per 24-48 ore, per una settimana, ecc.)

Tuttavia, in molti casi, l'effetto psicologico può aggravare il peso di eventi di per sé non molto rilevanti.

L'allegato tecnico documenta gli attuali sviluppi in materia di protezione delle infrastrutture critiche fornendo una panoramica dei risultati ottenuti finora dalla Commissione, i quali dimostrano come quest'ultima abbia acquisito in questo settore un'esperienza considerevole.

3.2. Gestione della sicurezza

Per effettuare uno studio delle minacce che incombono, degli incidenti che si verificano e degli aspetti vulnerabili che presentano gli elementi critici delle infrastrutture degli Stati membri e per analizzare il rapporto di interdipendenza che si instaura tra tali elementi è necessario raccogliere informazioni da una serie di fonti. Ogni settore e ogni Stato dovranno, all'interno della propria giurisdizione, individuare le infrastrutture critiche - secondo una formula armonizzata a livello dell'UE - e le organizzazioni o le persone responsabili della sicurezza.

Non tutte le infrastrutture possono essere protette da tutti i tipi di minaccia. Per esempio, le reti di trasmissione di elettricità sono troppo estese perché si possa recintarle o sorvegliarle. Applicando le tecniche di gestione dei rischi, si può concentrare l'attenzione sui settori esposti ai rischi maggiori, tenendo conto dei pericoli, della vulnerabilità, del livello esistente di protezione e dell'efficacia delle strategie contenitive esistenti al fine della continuità delle attività.

La gestione della sicurezza è un processo consapevole che mira a comprendere quali siano i rischi, a prendere decisioni e ad attuare azioni per riportare i rischi a un livello accettabile di rischio a un costo accettabile. Tale approccio consiste nell'individuare, valutare e tenere sotto controllo i rischi per far sì che questi non superino il livello considerato accettabile.

La protezione delle infrastrutture critiche (CIP) richiede un'attiva cooperazione tra i proprietari e i gestori delle infrastrutture critiche e le autorità degli Stati membri. Sono innanzitutto i proprietari e i gestori a dover gestire i rischi all'interno degli impianti concreti, delle catene di approvvigionamento, delle tecnologie dell'informazione e delle reti di comunicazione.

È indispensabile redigere e divulgare segnalazioni, istruzioni e note informative per aiutare gli operatori del settore pubblico e privato a proteggere i loro principali sistemi di infrastrutture. Di tanto in tanto, possono emergere rischi specifici o minacce di attentati terroristici che richiedono una risposta immediata. In tali casi, si richiederà alle amministrazioni degli Stati membri e alle industrie un intervento coordinato e concentrato sull'operatività. In circostanze di questo tipo, la UE deve coordinare le necessarie reazioni politiche e su tale base stabilire, caso per caso, disposizioni dettagliate con gli operatori del settore.

Persino i migliori progetti e le migliori leggi per la gestione della sicurezza non servono a nulla se non sono applicati correttamente. L'esperienza dimostra che il ricorso ad ispezioni indipendenti della Commissione al fine di verificarne l'applicazione costituisce l'unico strumento efficace che permette di garantire l'applicazione corretta dei criteri di sicurezza.

4. PROGRESSI REALIZZATI NELLA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE A LIVELLO COMUNITARIO

Gli europei si aspettano che le infrastrutture critiche continuino a funzionare indipendentemente dalle organizzazioni che ne sono proprietarie o che ne gestiscono le diverse componenti e contano sul fatto che i governi degli Stati membri e l'UE svolgano un ruolo di primo piano per garantire che sia così. Auspicano, inoltre, che i proprietari e i gestori a tutti i livelli sia del settore pubblico che di quello privato cooperino tra loro per garantire la continuità dei servizi da cui gli europei dipendono.

A complemento delle misure prese a livello nazionale, l'Unione europea ha già adottato una serie di misure legislative che istituiscono norme minime per la protezione delle infrastrutture nell'ambito delle diverse politiche dell'UE. È il caso, segnatamente, del settore dei trasporti, della comunicazione, dell'energia, dell'igiene e della sicurezza sul posto di lavoro e della sanità pubblica. Dopo i recenti attentati in America e in Europa, è stato dato un nuovo impulso alle attività che porteranno a un ulteriore miglioramento o a un allargamento delle misure esistenti.

Per decenni, sono state effettuate ispezioni nell'ambito del trattato EURATOM per controllare che i materiali nucleari fossero utilizzati correttamente. Nel settore della protezione dalle radiazioni, esistono numerose norme che si applicano ai rischi connessi all'utilizzazione degli impianti e all'uso di fonti contenenti sostanze radioattive.

Nel settore dei trasporti internazionali, l'Unione europea ha adottato norme che attuano o rafforzano gli accordi conclusi dagli organismi internazionali di regolamentazione nel settore aereo e marittimo. L'Unione europea continuerà a promuovere e partecipare attivamente alle loro attività a livello internazionale e incoraggerà i paesi terzi che hanno relazioni economiche con la UE ad attuare tali accordi. A tal fine ha già fornito assistenza ad alcuni di essi onde raggiungere un livello omogeneo e costante di sicurezza all'interno e all'esterno dei confini dell'UE.

Un ulteriore progresso è rappresentato dall'istituzione di agenzie come l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) per la sicurezza nelle comunicazioni. Inoltre, in settori come la sicurezza aerea e marittima, sono stati istituiti servizi ispettivi all'interno della Commissione per svolgere ispezioni sull'attuazione della legislazione in materia di sicurezza da parte degli Stati membri. Tali ispezioni permettono di stabilire dei punti di riferimento che garantiscono un livello di applicazione uniforme in tutta l'Unione europea.

L'allegato tecnico documenta gli attuali sviluppi in materia di protezione delle infrastrutture critiche fornendo una panoramica dei risultati ottenuti finora dalla Commissione, i quali dimostrano come quest'ultima abbia acquisito in questo settore un'esperienza considerevole.

5. POTENZIARE LA CAPACITÀ DI PROTEZIONE DELLE INFRASTRUTTURE CRITICHE DELL'UE

5.1. Un programma europeo per la protezione delle infrastrutture critiche

Considerato il gran numero delle infrastrutture potenzialmente critiche e le loro peculiarità, è impossibile proteggerle tutte con misure a livello europeo. Nel rispetto del principio della sussidiarietà, l'Europa deve concentrare i suoi sforzi sulla protezione delle infrastrutture di natura transfrontaliera e lasciare le altre sotto la sola responsabilità degli Stati membri, seppure nell'ambito di un quadro comune.

Esistono numerose direttive e regolamenti che impongono strumenti per l'individuazione degli incidenti, la pianificazione degli interventi in cooperazione con la Protezione civile, esercitazioni periodiche e collegamenti chiari tra i diversi livelli delle strutture di intervento: le pubbliche autorità, le organizzazioni centrali e i servizi di emergenza. D'altro canto, molto deve ancora essere fatto per quanto riguarda la protezione delle centrali di energia diversa da quella nucleare. Come è indicato nell'allegato tecnico, esiste un acquis comunitario in materia di protezione delle infrastrutture critiche a diversi livelli di sviluppo.

Nella maggior parte dei settori menzionati si sta lavorando, grazie anche alla cooperazione con gli esperti degli Stati membri e dei settori economici interessati, al fine di individuare le eventuali carenze e le misure correttive da applicare (giuridiche o altre). In tale ottica, sono state create molte reti e comitati di sicurezza.

Ogni anno, la Commissione illustrerà in una comunicazione i progressi alle altre istituzioni chiedendone il parere; esaminerà, per ogni settore, gli sviluppi delle azioni comunitarie per quanto riguarda la valutazione dei rischi, l'elaborazione di tecniche di protezione, i procedimenti legali in corso o previsti. Se del caso, inoltre, la Commissione proporrà, in tale comunicazione, aggiornamenti e misure di organizzazione orizzontale per le quali si richiede di armonizzare, coordinare o cooperare. La comunicazione, che ingloba tutte le analisi e le misure settoriali, costituirà la base di un programma europeo di protezione delle infrastrutture critiche (EPCIP).

L'obiettivo di tale programma sarà assistere l'industria e i governi degli Stati membri a tutti i livelli nell'UE, pur nel rispetto dei mandati e delle responsabilità individuali. La Commissione ritiene che sarebbe utile, ai fini dell'elaborazione di tale programma, avvalersi dell'assistenza di una rete di specialisti degli Stati membri – la rete informativa di allarme sulle infrastrutture critiche (CIWIN) – da creare il più presto possibile nel 2005.

Tale rete, da creare a sostegno della protezione delle infrastrutture critiche, servirebbe principalmente ad incoraggiare lo scambio di informazioni sui pericoli e i punti deboli comuni e sulle misure e le strategie più appropriate per ridurre i rischi. A tal fine, gli Stati membri dovrebbero, dal canto loro, assicurarsi che le informazioni pertinenti vengano trasmesse a tutti i servizi e organismi statali competenti, comprese le organizzazioni di servizi di emergenza e le associazioni di categoria del mondo dell'industria che, a loro volta, dovrebbero informare i proprietari e i gestori delle infrastrutture critiche interessate mediante una rete di contatti istituita all'interno degli Stati membri.

L'obiettivo dell'EPCIP sarà di promuovere un forum permanente in cui i vincoli per quanto riguarda la concorrenza, la responsabilità e la riservatezza delle informazioni siano compensati dai benefici derivanti da infrastrutture critiche più sicure. In tale processo un ruolo di primo piano avrà la consultazione del mondo dell'industria. Il forum contribuirà a fornire maggiori informazioni ai partner su specifiche situazioni di pericolo che permetteranno loro di prendere provvedimenti per far fronte alle potenziali conseguenze, ma non dovrebbe portare cambiamenti per quanto riguarda la responsabilità dei proprietari e dei gestori di prendere decisioni e di formulare piani per proteggere le proprietà.

Nei casi in cui non esistono norme settoriali o in cui non sono ancora state istituite norme internazionali, il comitato europeo di normalizzazione (CEN) e le altre organizzazioni di normalizzazione, possono assistere la rete e proporre norme di sicurezza settoriali uniformi ed adeguate per tutti i settori e i sottosettori interessati. Tali norme dovranno essere proposte anche a livello internazionale mediante ISO al fine di creare un'adeguata piattaforma in materia.

Occorrerà fare attenzione, quando si discute di minacce alla sicurezza nazionale, e nella fattispecie alle infrastrutture critiche, come il terrorismo, ad evitare di alimentare indebite preoccupazioni sia all'interno dell'UE che in eventuali turisti e investitori. Il terrorismo costituisce un pericolo costante ma i responsabili politici devono adoperarsi per incoraggiare i cittadini a vivere le loro vite serenamente. Occorre altresì fare attenzione a garantire il rispetto dei diritti privati, sia all'interno che all'esterno dell'Unione. I consumatori e gli operatori devono sentirsi sicuri che le informazioni saranno trattate con cautela, riservatezza e affidabilità. È necessario che vi sia un quadro adeguato per assicurare che le informazioni archiviate siano gestite in maniera corretta e che ne sia impedita l'utilizzazione o la diffusione non autorizzate.

Molte infrastrutture critiche sia dell'UE che degli Stati membri si estendono oltre i confini dell'UE. Interi continenti sono attraversati da gasdotti, il fondo degli oceani è percorso da cavi di importanza vitale per i servizi di tecnologia dell'informazione e così via. Ciò significa che la cooperazione internazionale è un elemento importante per instaurare relazioni di collaborazione dinamica, a livello sia nazionale che internazionale, tra i proprietari o gestori delle infrastrutture critiche e i governi dei paesi terzi, segnatamente i fornitori diretti di prodotti energetici all'Unione.

5.2. Attuazione dell'EPCIP

La protezione delle infrastrutture critiche richiede la partecipazione attiva dei proprietari e dei gestori delle infrastrutture, delle autorità di regolamentazione, delle associazioni professionali e industriali, degli Stati membri e della Commissione. Sulla base delle informazioni fornite dagli Stati membri e messe in rete, gli obiettivi dell'EPCIP saranno di continuare ad individuare le infrastrutture critiche, analizzare la loro vulnerabilità e interdipendenza e presentare soluzioni per proteggerle e per prepararle a tutte le evenienze. Nell'ambito di tali attività le associazioni dell'industria saranno aiutate a capire quali sono i pericoli e le possibili conseguenze nelle loro valutazioni dei rischi. Gli organismi preposti all'applicazione della legge e la Protezione civile degli Stati membri dovrebbero fare in modo che l'EPCIP diventi parte integrante delle loro attività di pianificazione e sensibilizzazione.

I servizi della Commissione, in stretto coordinamento con la rete, elaboreranno ulteriori azioni che consisteranno nell'adozione di leggi e/o nella divulgazione di informazioni. La Task Force dei Capi di polizia europei e Europol avranno un ruolo da svolgere per la diffusione di informazioni in materia di sicurezza agli organismi preposti all'applicazione della legge degli Stati membri, che, a loro volta, dovranno comunicare le informazioni attinenti alle possibili minacce e svolgere una funzione di collegamento con i proprietari e i gestori di infrastrutture critiche, aiutare a fornire pareri in materia di sicurezza e protezione ed elaborare strategie per combattere il terrorismo.

I governi degli Stati membri dovranno continuare a gestire o, se del caso, creare banche dati sulle infrastrutture critiche importanti a livello nazionale e saranno responsabili dell'elaborazione, della convalida e della verifica dei piani attinenti, assicurando così la continuità dei servizi sotto la loro giurisdizione Quando preparerà l'EPCIP, la Commissione formulerà anche suggerimenti sul contenuto minimo e il formato di tali banche dati e sulle modalità di interconnessione.

I governi degli Stati membri dovrebbero continuare a comunicare ai proprietari e ai gestori di infrastrutture critiche (se del caso, anche degli altri Stati membri) le informazioni pertinenti e i relativi allarmi e metterli al corrente del tipo di reazione prevista per ciascun livello di minaccia/allarme.

I proprietari e i gestori delle infrastrutture critiche provvederanno a un'adeguata sicurezza delle proprietà mediante un'attiva messa in pratica dei piani di sicurezza e realizzando periodiche ispezioni, esercitazioni, valutazioni e piani. Gli Stati membri verificheranno il processo globale mentre la Commissione dovrà garantire un'attuazione omogenea in tutta l'Unione mediante adeguati sistemi di ispezione.

5.3. Obiettivi dell'EPCIP e indicatori di progresso

L'obiettivo dell'EPCIP e il dovere della Commissione consistono 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. L'EPCIP sarà un processo in continua evoluzione e necessiterà di un riesame periodico per restare al passo con i problemi e le preoccupazioni della Comunità.

I progressi saranno valutati nei seguenti modi:

- l'individuazione, da parte dei governi degli Stati membri e per quanto attiene alla loro giurisdizione, delle infrastrutture critiche e la redazione di appositi elenchi conformemente alle priorità indicate dall'EPCIP;

- la collaborazione delle imprese con le loro omologhe del settore e con l'amministrazione al fine di condividere informazioni e ridurre la probabilità di incidenti che causino danni estesi o considerevoli alle infrastrutture critiche;

- la Comunità europea decide di istituire un approccio comune per affrontare il problema della sicurezza delle infrastrutture critiche mediante la cooperazione del settore pubblico e privato.

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.